Analysis and Design of Security Framework for Cloud Computing

THESIS

Submitted to
Babasaheb Bhimrao Ambedkar University
(A Central University)
Lucknow

For the Award of the Degree of

Doctor of Philosophy

In

COMPUTER SCIENCE

By

JITENDRA KUMAR SAMRIYA

Under the Supervision of

DR. NARANDER KUMAR

DEPARTMENT OF COMPUTER SCIENCE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
LUCKNOW-226025 (U.P.) INDIA

2020

Dedicated to my Parents...

CANDIDATE'S DECLARATION

I, Jitendra Kumar Samriya, solemnly declare that the research work embodied in this thesis entitled **"ANALYSIS AND DESIGN OF SECURITY FRAMEWORK FOR CLOUD COMPUTING"** carried out by me under the guidance and supervision of **Dr. Narander Kumar, Assistant Professor, Department of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India** is an original work and does not contain part of any work submitted for the award of any degree either in this University or any other University around the globe. It is further undertaken that the thesis is essentially free from all kinds of plagiarism.

Date: 28/12/2020
Place: Lucknow

(Jitendra Kumar Samriya)
Research Scholar
Department of Computer Science
Babasaheb Bhimrao Ambedkar University, Lucknow

CERTIFICATE

This is to certify that the thesis titled "**Analysis and Design of Security Framework for Cloud Computing**" submitted by **Mr Jitendra Kumar Samriya** is an original research work and has not been previously submitted in part or full for the award of any other degree or diploma to this or any other University.

The thesis submitted to Babasaheb Bhimrao Ambedkar University, Lucknow satisfies all the requirements as stipulated in the *Doctor of Philosophy (PhD) regulations-2013* and it is fit for submission and evaluation for the award of the degree of Doctor of Philosophy of the University.

Date: 28/12/2020

Supervisor

28/12/20

Head of the Department

ACKNOWLEDGMENT

First and foremost, I would like to Thank **to My Family.** You have given me the power to believe in myself and pursue my dreams. I could never have done this without the faith I have in you, the Almighty.

The award of degree Doctor of Philosophy is one of the hardest deserving achievements. People struggle for it and achievement not easily found. During the entire research works, some valuable people conceived their enormous positions in my heart. In this regard, I am grateful to the University and express my deep sense of gratitude to its **Hon'ble Vice-Chancellor** for delivering this great opportunity to me.

I would like to extend my hearty thanks to my supervisor **Dr Narander Kumar, Department of Computer Science, Babasaheb Bhimrao Ambedkar (A Central) University, Lucknow**, for support and mending efforts along with the valuable advice and encouragement through each step, for many lessons on how to do research and write research papers, for being very supportive in my work, for guiding into each part of the research work and life in general. His genuine concern inspired me to give my best and his insights helpful in looking at the problem from different viewpoints. Specifically, I am thankful for countless hours he spent with me in explaining each part, sharing his experiences on his research. Also, I am grateful for his insightful suggestions that helped me to make the right strategic choices at many crucial decision points along these years. I can never ever forget his contributions in shaping my life. It is all because of his infinite inspiration and contribution, that I am able to present this piece of work in a set tone and style. I am fortunate and feel pride in having his guidance.

I convey my sincere thanks to **Head & Dean** and all other faculty members of the department for their motivation and support during the research. I would also like to show my gratitude to the Department of Computer Science, for providing a healthy and pleasant environment required for quality research.

I would like to thank all administrative and supporting staffs of the University for providing a comfortable environment and help.

Specially thanks should be given to the supporting financial body, University Grants Commission that provided me with a fellowship for this research work.

I particularly would like to deeply appreciate the generous help of my closed friends Neetish Kumar, Jayveer Singh, Ashwini Kumar and Shubham Sonkar who always kept the healthy research environment and extended their full cooperation during my research. They have given me support and joyful and wonderful university life.

A special thanks to my family, my dearest parents, brothers, sister, wife and Son. Words cannot express how grateful I am to my **PARENTS** for all of the sacrifices that you've made on my behalf. Your prayer for me was what sustained me thus far.

I cannot list the names of all people who I indeed to but thanks to all valuable persons, who have given me enormous support and inspiration directly or indirectly during my research work.

Date: 28/12/2020 Jitendra Kumar Samriya

Place: Lucknow

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

Internet of Things	IoT
Service Level Agreement	SLA
Virtual Private Network	VPN
Personal Identification Number	PIN
Intrusion Detection Systems	IDS
Distributed Denial of Service	DDoS
Denial of Service	DoS
Misuse Detection	MD
Anomaly Detection	AD
Host Based IDS	HIDS
Network Based	NIDS
Burrows-Abadi-Needham	BAN
Spider Monkey Optimisation	SMO
Green Cloud Scheduling Model	GCSM
Particle Swarm Optimization	PSO
Virtual Machines	VMs
Fuzzy Ant Bee Colony	FABC
Service Level Agreement	SLA
International Data Corporation	IDC
Information Technology	IT
Cloud Computing	CC
Cloud Service Provider	CSP
Infrastructure as a Service	IaaS

Efficient Authentication Agreement Mechanism/ Protocol	EAAP
RSA With Character Stuffing	RSA-CS
Key Policy Attribute Based Encryption	KP-ABE
Burrows-Abadi-Needham	BAN
Particle Swarm Optimization-Based Probabilistic Neural Network	PSO-PNN
Elliptical Curve Cryptography	ECC
Host-Based Intrusion Detection System	H-IDS
Fuzzy C Means Clustering	FCM
Support Vector Machine	SVM
Internet Protocol-Wireless Sensor Network	IP-WSN
Internet Communication Machinery	ICM
Dynamic Voltage And Frequency Scaling	DVFS
Private Data Bucket	PDB
Non-Private Data Bucket	NPDB
Advanced-Encryption Standard	AES
Public Infrastructure	PKI
Code Obfuscation Engine	CobE
Automated Turing Test	ATT
Dynamic Clustering League Championship	DCLCA
Artificial Bee Colony	ABC
Iterated Spatial Prisoner's Dilemma	ISPD
Public Key Generation	PKG
Bandwidth-Aware Task-Scheduling	BATS
Adaptive Genetic Algorithm	AGA
Ant Colony Optimization	ACO

Fitness Value	FV
Ant Lion Optimization	ALO
Whale Optimization Algorithm	WOA
Cloud Task Scheduling	IWC
Energy-Oriented Flower Pollination Algorithm	E-FPA
Simulated Annealing	SA
One Time Password	OTP
Artificial Neural Network	ANN
Genetic Algorithm	GL
Key-Policy Attribute-Based Encryption	KP-ABE
First Come First Served	FCFS
Round-Robin	RR
Shortest Job First	SJF

LIST OF PUBLICATIONS

1. Narander Kumar, and Jitendra Kumar Samriya. " Security Issues in Cloud Computing: A Survey," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 6, Issue 4, July - August 2017, pp. 063-067, ISSN 2278-6856. - **(UGC Indexed)**
2. Narander Kumar, and Jitendra Kumar Samriya. "EAAP: Efficient Authentication Agreement Protocol Policy for Cloud Environment." International Conference on Next Generation Computing Technologies. **Springer**, Singapore, 2018.
3. Jitendra Kumar Samriya and Narander Kumar." A Novel Intrusion Detection System using Hybrid clustering-optimization approach in Cloud Computing" Materials Today: Proceedings (ELSEVIER) - **(Scopus Indexed) In Press.**
4. Narander Kumar, and Jitendra Kumar Samriya. "A Cryptographic Mechanism Using Prime Number and Character Stuffing to Prevent Hijacking of Cloud Data". International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6, March 2019. - **(Scopus Indexed)**
5. Narander Kumar, and Jitendra Kumar Samriya." Secure Data Validation and Transmission in Cloud and IoT Through Ban Logic And KP-ABE" International Journal of Sensors, Wireless Communications and Control. - **(Web of Science Indexed) Accepted.**
6. Jitendra Kumar Samriya and Narander Kumar." A QoS Aware FTOPSIS-WOA Based Task Scheduling Algorithm with Load Balancing Technique for the Cloud Computing Environment" Indian Journal of Science and Technology 13(35): 3675-3684. - **(Web of Science Indexed)**
7. Jitendra Kumar Samriya and Narander Kumar." An Optimal SLA Based Task Scheduling Aid of Hybrid Fuzzy TOPSIS-PSO Algorithm in Cloud Environment" Materials Today: Proceedings (ELSEVIER). - **(Scopus Indexed) In Press.**
8. Narander Kumar, and Jitendra Kumar Samriya. "Spider Monkey Optimization Based Energy-Efficient Resource Allocation in Cloud Environment" Walailak Journal of Science and Technology(WJST). - **(Scopus Indexed) Communicated.**

9. Jitendra Kumar Samriya and Narander Kumar, "Fuzzy Ant Bee Colony For Security And Resource Optimization In Cloud Computing," 2020 5th International Conference on Computing, Communication and Security (ICCCS) **IEEE**, Patna, 2020, pp. 1-5. - **(Scopus Indexed)**

10. Narander Kumar, and Jitendra Kumar Samriya. "Blockchain Based Efficient Resource Allocation and Minimum Energy Utilization in Cloud Computing Using SMO"-Book Chapter **(Springer Nature). - (Scopus Indexed) Accepted.**

Summary

SUMMARY

Cloud is a third party maintained offsite storage system which stores the user's data. This state's that instead of storing the user’s data on the hard disk or other storage devices it could be stored to a remotely accessed database where there is a link between the remote database and the user computer. In the cloud, the computers are arranged to work concurrently and the collective computing power is used by several applications intuitively they are functioning on a cloud with the support of the virtualization model. The customers are induced into the cloud in this model to access the IT (information technology) resources which are valued and presented on-demand. The resources of IT are shared and rented essentially for many purposes like apartments or office space which are used by tenants. The data centre of the company or server is fetched by the cloud when transmitted on an internet. To overcome the existing infrastructure of some respective companies certain services of cloud computing (CC) such as Google App Engine and Amazon EC2 are made.

There are three functional units or components using which the CC models function. They are listed beneath.

1. Cloud service provider (CSP): CSP is managed by this entity which has high computation power. This entity preserves the clients' data in considerable storage space.

2. Client/owner: This entity stores a huge sum of data files in the cloud and depends on the cloud for computation and conservation of data; it can either be an organization or a particularized consumer.

3. User: It is a unit disclosed by the holder which uses the owner's data which is warehoused on the cloud. The owner as well can be considered as the user itself.

Cloud security is essential mostly related to the secure, safe data and contents in the cloud systems. Moreover, in all the approaches and platforms in cloud computing security is needed.

The virtualization of IT Infrastructure refers to cloud computing which consists of software, hardware, web systems, network, etc.

Using the consecutive models this may be designed and developed.

- Public Cloud Computing: It is a conception of achieving IT Infrastructure virtually from remote places using proper (internet-based) services.
- Private Cloud Computing: It is the planning, enlargement of personal cloud-based infrastructure without a third party into their zone.
- Hybrid Cloud Computing: It is the merging of both i.e., Private and Public Cloud Computing, and used when essential.

Due to the growing IT usages, the security concept should be provided in all these three models. The offered CCS are Infrastructure-as-a-Service, Platform-as-a-Service, Storage-as-a-Service, Security-as-a-Service, Software-as-a-Service.

However, on occasion, it may be noted that the data management companies due to the necessity of more security are using cloud-based service providers and sometimes the cloud computing security services are used by the cloud service provider to safely store their data with proper procedures while inside the company or local server's vulnerability is an issue. The chapter-wise summary of the research is given below.

CHAPTER I

INTRODUCTION

This chapter gives a cloud computing technology overview using defining its underlying principles and the basics. The challenges identified here that cloud computing is facing and possible solutions.

For an emerging design of service provision, cloud computing refers to the underlying structure that has the merits of minimizing cost with sharing storage and computing resources,

interconnected with an on-demand provisioning appliance relying on a pay-per-use business design. The new features affect privacy, traditional security, and trust mechanisms but they also have a direct impact on information technology (IT) budgeting. Share services in a dynamic situation, store data remotely, and the ability to scale rapidly is the merits of cloud computing and it maintaining an assurance sufficient to tolerate confidence in potential customers is the demerit. Dynamic enough or no longer flexible is some core traditional mechanisms to address privacy, hence, a new scheme wants to be established to fit this new pattern.

CHAPTER II

REVIEW OF LITERATURE

This chapter presents and discusses a review of the literature to provide a theoretical background contribution with a broad introduction to cloud computing, efficient authentication protocols, Secure Data Validation and Transmission with data security challenges and opportunities in the cloud. The allocation and scheduling of resources are significant hurdles regarding cloud computing resources in practice. In cloud computing, researchers have been attracted to studying task scheduling for this reason. In a certain manner, the process of arranging incoming requests (tasks) is known as task scheduling, hence available resources are properly utilized. The workflow scheduling, locality/energy/reliability-aware scheduling, and service delivery model are the key research areas in cloud computing. Hence, with dissimilar aims, the services allocation or scheduling in a cloud system plays an important role. In infrastructure as a service (IaaS) platform the most complex problem is resource management. Therefore, a different approach is required for cloud computing to manage resources effectively. Several reputed journals, e-books, etc. are consulted for understanding the new research problems.

CHAPTER III

HYBRID CLUSTERING OPTIMIZATION APPROACH AND EFFICIENT AUTHENTICATION AGREEMENT PROTOCOL (EAAP) FOR AUTHENTICATION

This chapter is categorized into two sections; An Efficient Authentication Agreement mechanism/ protocol (EAAP) is the first section which includes the Diffie-Hellman key exchange method using ECC to give a good security policy for the cloud atmosphere; a novel hybridization scheme for the intrusion detection scheme is the second section introduced to enhance the total cloud security based computing environment. Besides, on the cloud this scheme supports managing several types of security issues cloud; phishing attacks, fake identity detection, and data leakage. For efficient anomalies clustering, the method uses fuzzy-based ANN while the fuzzy-based clustering is then optimized by an SMO scheme. By spontaneously updating the fitness value, the selection process, and iterative classification of fuzzy clustering scheme solved by the hybridization approach. Besides, the minimized dataset was sent to the neural network and the SMO optimization scheme was the result in dimensionality. When compared with other previous hybridization schemes, the introduced scheme outcomes result in enhanced accuracy and reduced computational time.

The content of this chapter is published in-

1. NGCT 2018, Communications in Computer and Information Science, vol. 922. **Springer**, Singapore. ISBN: 978-981-15-1718-1
2. Materials Today: Proceedings, **Elsevier**, ISSN: 2214-7853. **SCOPUS Indexed.** (In Press)

CHAPTER IV

TRAFFIC HIJACKING PREVENTION THROUGH PRIME NUMBER AND CHARACTER STUFFING MECHANISM

In this chapter to secure Cloud Data Hijacking, a cryptographic scheme is presented, which includes RSA with character stuffing (RSA-CS) by prime numbers. Compared with the existing stuffing approach, the RSA algorithm is modified for a better outcome and used for network security in perspectives of the cloud environment. To prevent unauthenticated access and hijacking as well as to provide better security, the introduced framework is utilized.

The content of this chapter is published in-

1. International Journal of Recent Technology and Engineering (IJRTE), vol. 7(6), pp. 1043-1048, 2019, ISSN 2277-3878, **SCOPUS Indexed.**

CHAPTER V

KP-ABE WITH BAN LOGIC TECHNIQUES FOR ACCESS CONTROL

In this chapter a Secure Data Validation and Transmission in Cloud and IoT through Ban Logic and KPABE is used. Initially, the authentication of user is verified. Then the user data is encrypted with the help of the KP-ABE algorithm. Finally, data validation and privacy preservation are done by Burrows-Abadi-Needham (BAN) logic. This verified, and display that the introduced encryption is correct, efficient, and secure to avoid unauthorized contact and prevention of data leakage so that fewer chances of data/identity, theft of a user is the analysis and performed by KP-ABE, that is access control approach.

The content of this chapter is published in-

1. International Journal of Sensors, Wireless Communications and Control, Bentham Science, ISSN: 2210-3287, **Web of Science Indexed**. (Accepted)

CHAPTER VI

SECURE VIRTUAL MACHINE ALLOCATION USING FTOPSIS-PSO AND WOA BASED TASK SCHEDULING AND ANT-BEE COLONY MECHANISMS

In this chapter, an FTOPSIS approach for effective task scheduling with WOA for load balancing among VMs is proposed. This model controls the admittance of the requests by achieving target QoS in terms of response time. Hence the admittance is controlled so that the requests which are accepted do not face a delay greater than the time limit stated in the SLA.

The content of this chapter is published in-

1. Indian Journal of Science and Technology(IJST), vol. 13(35), pp. 3675-3684, 2020, ISSN 0974-5645. **Web of Science Indexed.**
2. 5th International Conference on Computing, Communication and Security (ICCCS-2020), pp 1-5, **IIT** Patna, India, Available on IEEE xplorer.

CHAPTER VII

MINIMUM ENERGY UTILIZATION THROUGH SPIDER MONKEY OPTIMIZATION TECHNIQUE

In this chapter, two different approaches for minimum energy utilization are presented. In the first approach, the Spider Monkey Optimization (SMO) is used for attaining an optimized resource allocation. The key parameters considered to regulate the performance of SMO are its application time, migration time, and resource utilization. Energy consumption is another key factor in cloud computation, and this work adopted the Green Cloud Scheduling Model (GCSM) for the energy utilization of the resources. This is done by scheduling the heterogeneity tasks with the support of a scheduler unit that schedules and allocates the tasks which are deadline-constrained enclosed to nodes which are only energy-conscious. Assessing these methods is formulated using the cloud simulator programming process.

The second approach offers a blockchain-based resource management framework and an

optimized resource allocation strategy using an SMO algorithm based on energy consumption and makespan optimization models in the cloud domain. The SMO is a novel evolutionary algorithm based on spider monkey's foraging behavior. It is a perfect approach for the optimization of benchmark functions and antenna design complications. The use of SMO in this approach successfully optimizes resource allocation when evaluated with the prevailing resource allocation algorithms. In addition to this, the energy depletion of the resources is minimized by applying a Brownout based Energy model.

The content of this chapter is published in-

1. Walailak Journal of Science and Technology, ISSN: 2228-835X. **SCOPUS Indexed. (Communicated)**
2. Book Chapter of Blockchain for 6G-Enabled Network-based Applications: A Vision, Architectural Elements, and Future Directions, **Springer** Nature, **SCOPUS Indexed**. **(Accepted)**

CHAPTER VIII

QoS AND SERVICE LEVEL AGREEMENT POLICY

This chapter presents two different methods for QoS and Service Level Agreement policy. The first approach utilizes the Fuzzy-TOPSIS and particle swarm optimization (PSO) approach. Initially, the available task and the no. of VMs (virtual machines) are optimized by the PSO algorithm. The multi-objective SLA-based task scheduling problem is solved by the Fuzzy TOPSIS which uses the weighted sum of energy, cost, and execution time as an objective function. Based on these three patterns the experimental results are attained.

In the second approach, a Fuzzy Ant Bee Colony (FABC) algorithm is presented with the intention of QoS aware scheduling with security measures in the cloud domain. Here the proposed metaheuristic algorithm is used for security-aware scheduling. A task is allocated to the ideal VM based on the QoS and security level of the users. The foremost aim of this work

is to offer QoS i.e. cost, makespan, and minimized migration of tasks with security enforcement. The proposed algorithm guarantees that the admitted requests are executed without violating service level agreement (SLA). These objectives are attained by the proposed Fuzzy Ant Bee Colony algorithm.

The content of this chapter is published in-

1. Materials Today: Proceedings, **Elsevier,** ISSN: 2214-7853. **SCOPUS Indexed** (In Press**)**

CHAPTER IX

CONCLUSIONS AND FUTURE PERSPECTIVES

This chapter presents, the essential analysis of the works explained in the previous chapters is concluded. The stored data and information on the cloud are vital to persons with a harmful intention for this reason, the cloud environment needs security. Secure information in a considerable measure is kept on PC's and this data is currently being saved and exchanged to the cloud. So it is essential to realize the security process that the Cloud provider uses. The main factor in dealing, is to confirm the safety that the cloud supplier has set up recently. Some of the important issues in the present research work have been identified and independent solutions to each issue have been proposed. These are

- Authentication
- Traffic Hijacking Prevention
- Data Validation and Transmission
- A QoS Aware Scheduling and Load Balancing
- Resource Optimization
- Energy Efficiency

For each sub-problem, the solutions provided are viable, scalable, and dynamic in nature and are validated by the simulation results.

The people in the future will access and share their software applications online and uses the remote server networks to access information instead of depending on fundamental tools and information present in their personal computers. One of the main research topics is the security issues in Cloud Computing which is always investigated by researchers and developers to find appropriate solutions consistently.

CHAPTER I

Introduction

CHAPTER I

INTRODUCTION

This chapter offers an outline of the basic concepts with the features and historical steps towards cloud computing.

1.1 Cloud Computing

During the 60s, excess space was required by the computers and they consumed a large volume of electricity, emitted very little processing output, and had costly electronic parts. However, these large computers were eventually replaced by smaller ones [1]. Moreover, old-fashioned computing will not be able to handle the upturn of online users on various networking sites [2-3]. Globally due to the rise in internet usage, a new approach is needed for handling the volume, variety, and data availability, as a result, cloud computing is preferred [4, 5]. It has applications over a wide range covering IT, businesses, data storage, and software engineering.

1.2 Cloud Service Delivery Models

The rising number of online activities are interconnected by the following new services. As per the analysis of Cisco, the cloud capabilities are induced by the Internet of Things (IoT) [6-8]. IaaS, PaaS, and SaaS are the significant delivery models confirmed after many types of research. Distinct types of service models are presents in this section which are depicted in figure 1.1. IaaS is the last one of the models and they deal with computer hardware. In IT organizations, IaaS care for the revolution in the business outlay [9].

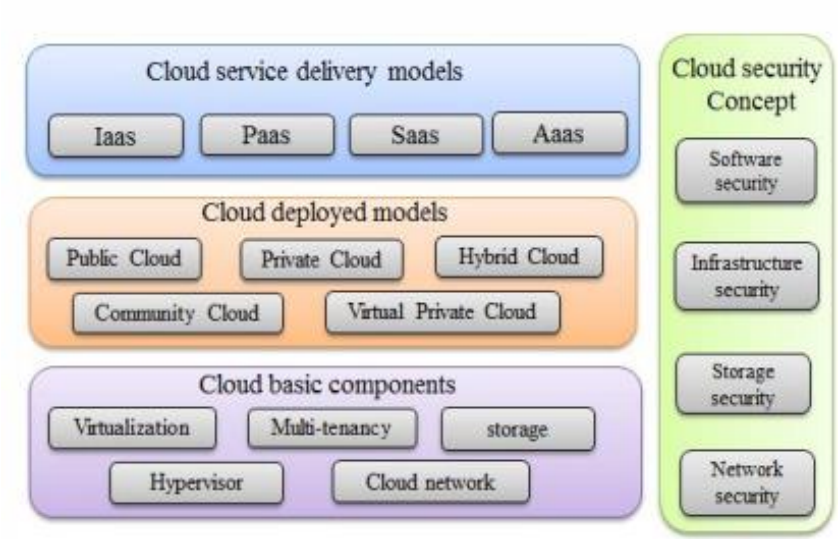

Figure: 1.1. Cloud computing framework

PaaS: This model is a service middleware model. The clients do not have any means to manage the basic structure but can be able to control the applications [10].

SaaS: It is a pool of remote computing facilities. It employs the other dealers and permits the applications to deploy remotely. Some of the examples of SaaS providers are Salesforce and Google App, which is a pool of remote computing facilities. [11-12].

1.3 Cloud Deployed Models

Generally, the cloud framework relies on common resources by individual devices or local servers [13]. As a result, by grabbing the benefit of resource sharing the consistency is achieved.

Private Cloud: The Cloud framework in this section functions and manages within the data center of the organization.

Public Cloud: This model is the proper illustration of cloud hosting, which has a robust Service Level Agreement (SLA) among the customer and provider to maintain the trust. [14].

Community Cloud: The organizations cloud infrastructure share concerns of consumers. Multiple organizations are responsible for sharing and controlling this community cloud [15]. It lessens the expense of the private cloud and lowers security issues.

Hybrid Cloud: Two or more clouds (public, private, community) are combined to form the hybrid cloud. This model presents the benefits of several cloud deployment models.

Virtual Private Cloud: This model comprises a virtual private network (VPN) and is a semi-private one having very few resources.

1.4. Basic Components of Cloud Computing

The essential components for the deployment of the cloud framework are deliberated in this section. Some vital components are discussed here:

Virtualization: In the deployment of the cloud, virtualization has a vital part and it is a prearranged component in the cloud that uses multiple consumers and allows the physical resources [16].

Multi-Tenancy: In this model, there are multiple customers or users present in the Multi-tenant framework which can share the applications or resources in an execution environment and will not perceive or share other's data, although they belong to many organizations [17].

Cloud Storage: It is a module, which is accomplished, conserved, and made open over the entire network, which is accessible to the user.

The Hypervisor: The main element of virtualization is the VM monitor or manager. This monitors and controls the operating systems working in a mutual physical scheme.

Cloud Network: Numerous conventional data center are operated using the cloud network; there are hundreds or thousands of servers in a typical data center [18].

1.5 Need for Security in Cloud

Cloud computing is adopted by a lot of organizations due to its benefits even though there might be possible security constraints that prevail to be a barrier due to adapting CC. The service provider is responsible for the protection and data management in CC. The damage on the physical computing device resulting from malware is reduced by the secured computing environment. In a secured environment, the cloud services cost is reduced significantly. The

performance is enhanced due to security and there is a chance to reduce the destruction of data, hardware, and software. In CC, a security design is wanted to manage the multi-tenancy and scalability with trust requirement. Multiple users in CC can access to the resources as it is of abundant. In the cloud, the data stored or managed are prone to security issues. When an organization using their characteristics, facts, and infrastructure, move towards the cloud environment, they must be ready to hand over some level of control. The CC systems and providers should be trusted by the organization. Moreover, they should verify cloud events and processes. Compliance, access control, data security and event management are the basics of trust and verification.

1.6 Benefits of Cloud Security

The CC having features such as flexibility, power and ease, contain a lot of security issues. To access applications and make work simple, CC terms to be a new intuitive way. Several problems/issues can influence its adoption. Some issues in this field are revealed by a non-exhaustive search. Some of them are security, QoS, SLA, etc.

Automatic updates are one of the features of CC when the administrator changes anything which could reflect on its users. A large number of users are notified when any kind of fault occurs in the software, which is a risky situation for any organization having the least security level. Many researchers have agreed on this state that the adoption of cloud computing has security concerns. Existing surveys present that among challenges in CC security is ranked first. When an organization has its top-class security with no time-to-time updation of security policies could be liable to security breaches in the near future. Some of the benefits of cloud security are as:

- Data Encryption

The cloud-based security systems with robust data encryptions have considerably minimized the prospects of data breaches; a layered approach is offered by these solutions, which comprise

key management, security intelligence, and secure access controls. The organizations are given full freedom to choose their users who are accessing the outsourced data, which is an excellent way to avoid any attempts to interfere with personal or professional data. Due to the employees of the organization threat of internal data theft are faced. These threats can be avoided by more robust access control. The possibilities of a data breach can be avoided by the multi-layered security features. Data, regardless of its type, must always be secured. Any breaches can be risky to the generosity and the functioning of an organization.

- Evade DDoS Attacks

For entertainment companies, these DDoS attacks can result in heavy losses. The website is targeted by Hackers by focussing the traffic from various sources to the end website, which exhausts the system. The clients begin to lose trust due to these DDoS attacks, which may taint the reputation of the company.

This upcoming threat is prevented by the Cloud-based security systems with authentic scanning of potential risks; additionally, this function is used as a cautionary tool for certain systems which permits the tracking of incoming attacks and threats rapidly – this allows the admins of the website to divert the traffic to other locations.

- Governing Compliance

SOC1 and SOC2 certifications are provided by the Cloud computing security solutions to the entertainment businesses which are reliable. These certifications ensure periodic scrutiny of data and all types of possible anomalies. Cloud-based solutions manage the necessary arrangement for regulatory compliance and the protection of data. A comprehensive AWS report about the security control management confirms all organizations pay attention to their commercial operations, deprived of fretting about compliance requirements.

1.7 Contribution of Cloud Security in Thesis

In today's world, CC has been considered as the main computing or storage component because

of the irrefutable need for computation and storage resources. Though, this widespread phenomenon has a lot of issues about vulnerabilities and security challenges. Many threats are faced by the cloud environment. Therefore, ample knowledge and the best possible solution are mandatory to deal with each of these threats. Several studies are reviewed in this current study and some of them have more importance. The main contribution of cloud security in this research work is to deliver better cloud data security and avoid hijacking and unauthenticated entry and various security issues or challenges such as Authentication in the cloud, Session hijacking, Phishing problem, Eavesdropping, Virtual machine allocation policies, Service level agreement, Quality of Service and Energy efficiency. Holistic security issues study in the clouds that enclosed total cloud components, network layers, and cloud stakeholders.

1.8 Authentication in Cloud Environment

The Cloud computing environment is filled with good characteristics and it has a rich set of distributed resources. The data available in the cloud environment is accessed and stored by a user with a proficient authentication mechanism. By using an authentication process, the user's identity must be verified before providing access to shared resources. The customers of the cloud are permitted to store their data without the awareness of the location and storage of data. The authentication information is exchanged when accessing every cloud service by the customer [19]. Three different types of authentication factors are used in a cloud environment. The factors considered to authenticate the users are the inherence factor, knowledge factor, and the possession factor.

Knowledge Factor: states "Something we know", denotes the authorizations such as a username, a password, or a personal identification number (PIN).

Possession Factor: which contains "Something we have" that is the credential such as user's hardware device like a cellular (smart) phone which can receive a one-time password, PIN or the message generated by authentication apps.

Inherence factor: represents "Something we are" is normally trusted on the biometric credentials, containing thumb or fingerprint, retina scan, facial recognition, or a new form of biometric data [20].

1.9 Intrusion Detection Systems (IDS) in Cloud

Imitating the legitimate users, Intruders can access cloud infrastructures affecting legitimate users. In the cloud IaaS component, the attackers can easily get the victim machines information [21]. Cloud users can be easily attacked by attaining the information. Distributed denial of service (DDoS) and Denial of service (DoS) attacks are some of the attacks that mainly focus on data privacy, reliability, and accessibility. By applying IDS, such attacks can be avoided. Additional security measures are provided by IDS approach.

Into two groups, Intrusion detection can be categorized as (1) misuse detection (MD) and (2) anomaly detection (AD) [22]. MD makes a comparison with database results and deals with data features of the user's input. In contrast, user behaviour is stored by the anomaly detection in the feature database and compared with the current behaviour. The invasion occurs if there is a maximum difference rate in comparison. There are two kinds of IDS (1) host-based (HIDS) and (2) network-based (NIDS). The HIDS monitors a single host's behaviour. The NIDS analyses the flow of traffic through a network [23]. IDS is used in the cloud to detect the attacks on their service. Moreover, the cloud user should know if the hosts or used services are used to attack other victims. It would be beneficial for each user to isolate the IDS from the actual module.

If the IDS is used to observe a VM host, it is not certain that the IDS works correctly when the host is conceded, as any modifications could be done by the attacker to stop any reports to be sent. To configure the cloud users' private IDS a distinct set of thresholds and rules are needed. Attacks should be detected by the cloud providers on their cloud infrastructure. A user or an external attacker who may or may not be conceded can perform these attacks. From the

monitored target, the IDS needs to be separated for security reasons and to optimize efficiency.

1.10 Cloud Computing Threats

A threat in computer security is described as something which causes severe destruction to a computer system. The threats in the computer system or the network set-up can lead to possible attacks. In this section, top threats in cloud service relevant to the security, a framework is defined [24].

1.10.1 Different Service Delivery/Receiving Model

Different ways of delivery/receiving services are used by cloud computing and business models. The CSP organizes the application and services to a remote site, the risk factors related to the cloud should be examined by the company. From one location to another location the cloud data's are traversing, different security laws are used by both locations. At the time of usage, major threat can be generate. A common standard security law, robust end-to-end encryption and a trust management scheme can remove such threats.

1.10.2 Abuse and Despicable Use of Cloud Computing

Some of the utilities provided by IaaS providers are boundless bandwidth, network, and storage volume. For a predefined trial period, certain providers provide their services to use, which has a smooth registration process in which anybody can register deprived of any security process. They do not have enough control over the user during this trial period. Consequently, malevolent code authors, spammers, and other convicts could accomplish the attack, certain potential threats has key cracking and password, captcha solving farms, DDoS, and hosting malicious data. The IaaS and PaaS service infrastructure are affected by these forms of threats.

1.10.3 API and Insecure Interface

The user is provided with a software set of interfaces and APIs by the CSP for communication. The cloud complexity is increased by this interface which is positioned above the cloud framework. Such an interface is arranged for all administrational and monitoring services.

These APIs are acknowledged by cloud security. But occasionally, the security of these APIs can be affected accidentally and also by malicious attempts.

1.10.4 Malicious Insiders

The malicious insider threats are vital in the CC. The reason for executing this threat is owing to the non-existence of transparency and IT services. An employee resulting from this gets a better access level. This leads to a state in which an insider attacker can affect the cloud services by accessing the confidential data. An attacker could simply penetrate the framework via IDS or firewall when the security framework considers it as an authorized action.

1.10.5 Common Technological Concerns in A Multi-Tenancy Environment

The virtualization concept is adopted in a multi-tenant framework in which the services are provided by IaaS vendors. Among the multiple users, the same resource is shared in virtualization. In a multi-tenant framework, a malicious user gains knowledge about the user which is allowed by the hypervisor causing major threats due to the lack of robust isolation. The overall cloud infrastructure is affected by the concept of sharing. This issue can be prevented by strong access control and authentication mechanisms.

1.10.6 Leakage and Data Loss

The data loss examples are data deletion, theft, and alteration, deprived of securing the actual content, data loss also occurs due to the encoding key loss and the prolific and sharing nature. The vital cause for leakage and data loss is the absence of authorization, verification and access control, fragile keys, poor encryption algorithms, lack of disaster recovery, and unreliable data center. This threat affects the IaaS, PaaS, and SaaS, service models. Some of the prevention methods are secure storage, secure API, strong algorithms and encryption keys, data integrity, and backup.

1.10.7 Service/Account Hijacking

In this process, the user is diverted to a harmful website. The website could be prone to scams,

phishing, and manipulation of software liabilities. These kinds of attacks are often caused by the reuse of passwords and credentials. If an attacker in cloud computing access somebody's identifications, they could seize the actions, manipulate data, transaction data, redirect the client to illegal sites, or return untrue information and hack the account.

1.10.8 Risk Profiling

Cloud is least concerned with tenure and handling the software and hardware due to the heavy workload. To deal with the software and hardware infrastructures the cloud gives the contract to the organization. As it is a fair concept, but the cloud is not aware of the internal security procedure, [25], auditing, patching, hardening, security policies, and logging process of the organization. Risk and threats are formed due to this ignorance. The cloud must make sure to have an altering and monitoring system along with the consciousness of partial infrastructure particulars, records, and data for the removal of threats.

1.10.9 Identity Theft

In this type of threat, somebody takes off the user's identity, credits, service benefits, and other related resources. The victim exposed to these threats undergoes many annoying results and losses. Due to, phishing attacks, key loggers, and weak password recovery methods this threat can happen. A strong password recovery process and a multi-tier authentication mechanism are followed by this model.

1.11 Secure Data Validation and Transmission in Cloud

In computing, the cloud has become an important topic; though, a new range of security issues have been established that need to be addressed. The data and related software are in the cloud are not under their control.

Furthermore, the communications of cloud networks are rising day by day. It is vital to protect the data flow path. Regarding security mechanisms, the present researches only emphasize acquiring the information flow in the communication networks. For improving the

performance of the network lot of work has to be done. Not considering the optimized use of the network resources and only using the information encryption and decryption the security mechanisms functions. The proprietary information and confidential data are sent via a secure channel in a secure cloud data transmission [26].

The payment facility is provided by the CSP that saves the primary data to be stored on remote servers. In literature, many techniques have been presented, but there are several problems. They are listed below,

- Only one level of security is available in most distributed computations hence the security there is not reliable.
- Traditional encryption plans have many compliance problems and thus, they are not secured.
- Additional security measures are needed for automated data transfer, as during the transaction data is more likely to be stolen.
- When a computer receives a large amount of information, it must be checked for reliable and accurate resale. However, cloud storage does not mean this is possible.

  Due to the reasons mentioned above, there is a need to design a new method for secure data transmission in cloud computing.

1.12 VM allocation and Task Scheduling in Cloud

Resource management and task scheduling are needed to exploit the revenue and resource utilization. In terms of performance, resource allocation and scheduling are the significant hurdles of CC resources [27]. For this reason, the researchers are keen on investigating task scheduling in CC. The incoming requests (tasks) in Task scheduling are appropriately arranged to utilize the resources. The resources are utilized properly in cloud computing [28]. Internet users without considering the hosting infrastructure can access the contents all the time. The service provider maintains and manages such hosting infrastructure with various machines and

capabilities. The capabilities of such infrastructure are enhanced by cloud computing accessing the Internet. The entire stack of computing services are used by the cloud service users ranges from hardware to applications.

Cloud computing services are employed on a pay-as-you-go basis. The resources available can be reduced or increased by the cloud service end-user depending on the demands of the applications. At any time, the resources can be rented by the cloud service user and discharge with no complexity. Mainly based on these two methodologies, the efficiency of the resource is valued. The use of a scheduling algorithm is suggested to deal with intricate task issues. Such algorithms control the resources.

1.13 Energy-Efficient Resource Allocation in Cloud Environment

Recently the cloud computing is advanced from grid computing owing to mounted utilization of virtualization at the datacenter. It offers online resources and updated services essential for the clients exclusive of changing their existing structure. The size of the data center is increasing exponentially due to the aggregate demand for cloud services and fulfilling. This demand more servers are needed. Hence, more heat is generated from the data center and there is a need for more cooling devices to maintain the data center at a specific temperature ensuing more energy consumption and emission of CO_2 [29]. To reduce the total energy cost at the data center there is a need for energy-efficient resource allocation techniques [30-32].

1.14 QoS and Service Level Agreement Policy in Cloud Environments

An adequate quantity of resources is provisioned by the CSP to safeguard that the QoS necessities of the cloud service clients like budget constrictions, deadline, and response time are met [33]. Next-generation CC's success depends on how proficiently these frames will discover and endure computing strategies in an active way [34]. These applications based on the QoS requirements will be considered and identified as SLAs. The recent cloud scheme is not fully customized to honour the probable SLAs.

For cloud providers, a vital challenge is to systematize the supervision of virtual servers, maintaining the expense of resource supervision and the QoS requirements of hosted applications. The Cloud market structures do not react to the dynamic variation of consumer desires and are consistently static [35]. There is a need for an adaptive approach to responding to these issues regarding the bounding SLA patterns based on consumer requirements.

1.15 Objective of Research

In the computing paradigm, Cloud Computing has developed as a computational technique. Cloud computing implementation has attracted computing as a utility and allows pervasive applications from consumer and business domains. Cloud also offers many advantages like other technology, which come with some rider cost associated with it. Cloud also has its flaws and that is security. There is no change in the security of the cloud environment compared with the traditional computing models. The major focus in both cases is on the topics of guarding data from theft, deletion, or leakage. Security issues in the cloud are slightly different from traditional computing models. When an organization or an individual user moves the data and computer systems to the cloud, the security reliabilities become shared between the CSP and the user. The cloud environment is highly vulnerable to security threats due to its intrinsic nature, conversely, as compared to its counterpart as some third-party provider stores the data and accessed on the web which upturns the overall liability and thus affects entire reliability.

On the other hand, for the operation and maintenance of cloud data centers, energy consumption is becoming a vital issue, cloud computing providers are becoming deeply concerned. In this dynamic cloud environment, because of the drastic increase in cloud usage, proper and efficient resource allocation becomes a challenging task. Several approaches with the intension to enhance the ability of the resource allocation process are established. When the system is fully loaded there is an absolute inability in respect of power consumption and scheduling. The task scheduling algorithm for energy-efficient is compulsory to improve the

resource allocation process efficiency.

The main objectives of this thesis are summarized below:

- To develop a cloud-based Efficient Authentication Agreement Protocol Policy.
- To detect and mitigate the network attacks and associated security and privacy challenges in cloud environments using novel techniques.
- To implement energy-efficient task scheduling algorithms to enhance the efficacy of resource allocation and optimization procedures to boost up cloud services.

1.16 Thesis Organization

This thesis is organized into eight chapters. Chapter two provides a review which is related to various security issues or challenges such as Authentication in the cloud, Session hijacking, Phishing problem, Eavesdropping, Virtual machine allocation policies, Service level agreement, Quality of Service, and Energy efficiency.

Chapter three presents a Intrusion detection based hybrid clustering optimization Approach and Efficient Authentication Agreement Protocol (EAAP) incorporating the Diffie-Hellman key exchange appliance with ECC to offer a good security policy for the cloud atmosphere.

Chapter four presents a Cryptographic approach using Character Stuffing and Prime numbers to Avert Data Hijacking. This study uses RSA-CS using prime numbers. For attaining better outcomes, the RSA algorithm is adapted from cloud environment perspectives. This approach avoids hijacking as well as unauthenticated access and offers better security of cloud data.

Chapter five presents a Secure Data Validation and Transmission in Cloud and IoT through Ban Logic and KP-ABE. This key policy, based on attributes utilizes a secure transmission in the cloud using KP-ABE. Initially, the authentication of the user is verified. Then the user data is encrypted with the help of the KP-ABE algorithm. Finally, data validation and privacy preservation are done by Burrows-Abadi-Needham (BAN) logic. This confirmed and displayed

that the introduced encryption is correct, secure, and efficient to solve unauthorized entree and prevention of data leakage so that fewer chances of data/identity, theft of a user is the analysis and performed by KP-ABE, that is access control approach.

Chapter six presents an FTOPSIS approach for effective task scheduling with WOA for load balancing among VMs. The proposed model controls the admittance of the requests by achieving target QoS in terms of response time. Hence the admittance is controlled so that the requests which are accepted do not face a delay greater than the time limit stated in the SLA

Chapter seven presents two different approaches for minimum energy utilization. In the first approach, the Spider Monkey Optimization (SMO) is used for attaining an optimized resource allocation. The key parameters considered to regulate the performance of SMO are its application time, migration time, and resource utilization. Energy consumption is another key factor in cloud computation, and this work adopted the Green Cloud Scheduling Model (GCSM) for the energy utilization of the resources. This is done by scheduling the heterogeneity tasks with the support of a scheduler unit that schedules and allocates the tasks which are deadline-constrained enclosed to nodes which are only energy-conscious. Assessing these methods is formulated using the cloud simulator programming process

The second approach offers a blockchain-based resource management framework and an optimized resource allocation strategy using the SMO algorithm based on energy consumption and makespan optimization models in the cloud domain. The SMO is a novel evolutionary algorithm based on spider monkey's foraging behaviour. It is a perfect approach for the optimization of benchmark functions and antenna design complications. The use of SMO in this approach successfully optimizes resource allocation when evaluated with the prevailing resource allocation algorithms. In addition to this, the energy depletion of the resources is minimized by applying a Brownout based Energy model.

Chapter eight presents two different methods for QoS and Service Level Agreement policy.

The first approach utilizes the Fuzzy-TOPSIS and particle swarm optimization (PSO) approach. Initially, the available task and the no. of VMs (virtual machines) are optimized by the PSO algorithm. The multi-objective SLA-based task scheduling problem is solved by the Fuzzy TOPSIS, which uses the weighted sum of energy, cost, and execution time as an objective function. Based on these three patterns, the experimental results are attained.

In the second approach, a Fuzzy Ant Bee Colony (FABC) algorithm is presented with the intention of QoS aware scheduling with security measures in the cloud domain. Here the proposed metaheuristic algorithm is used for security-aware scheduling. A task is allocated to the ideal VM based on the QoS and security level of the users. The main objective of this work is to offer QoS, i.e. cost, makespan, and minimized migration of tasks with security enforcement. The proposed algorithm guarantees that the admitted requests are executed without violating service level agreement (SLA). These objectives are attained by the proposed Fuzzy Ant Bee Colony algorithm.

In chapter nine, the thesis concludes the critical analysis of the works described in the previous chapters with the future scope in this field.

CHAPTER II

Review of Literature

CHAPTER II
REVIEW OF LITERATURE

A literature review is presented and discussed in this chapter, to offer a speculative background and to acquire a perceptive of the impact and role of Efficient authentication policies, secure data validation and transmission in the cloud, a QoSs and SLA based task scheduling algorithms with load balancing and energy-efficient scheme for the cloud computing, efficient resource distribution techniques in cloud and novel intrusion detection systems that aims to deal with security risk, crises and disasters and data availability in the cloud.

2.1 Introduction

Cloud computing is needed for the modern computing environment of tomorrow. The goal of this computing facility is to provide resources as per user requirement and decrease the cost of the whole computing system by sharing application. It provides a data center with hardware and software. Cloud computing offered various functionality, e.g. Infrastructure management, on-demand accessibility of data. It depends on the related organization to reduce the cost, energy and other services used in cloud computing. It is used today, in all our everyday need in life such as shopping, personal data storage, satellite launching etc. Based on the International Data Corporation (IDC) survey report, in 2019, the expenditure on IT cloud services will be more than US$141 billion worldwide [36]. Cloud computing contains scarce resources (e.g. Servers, applications and storage) to offer services to end-user by the service provider. The Web browser is responsible for accessing on-demand cloud services to users also.

Basically, Cloud computing infrastructure contains 3-layer architecture: SAAS, PAAS, IAAS. SAAS is generally identified as topmost layers in cloud infrastructure, called software-as-a-service. It is also known as the application layer, which allows the application to run on the cloud to fulfil the user's requirement, e.g. VMware, Amazon Elastic, etc. PAAS named

Platform-as-a-services or platform layer, act as a middle layer in cloud infrastructure. This layer designed to deliver a platform for the user to use relevant applications. It provides control over the application deployment, e.g. Google Docs, Google Talk etc. Finally, the third layer is Infrastructure-as-a-service is the bottom layer, known as IAAS [37]. It includes servers, network devices, memory and storage etc. The resources are available for user's on-demand services. It also uses virtualization technique, which capable to form complex network infrastructure via virtual machines.

Many techniques can be used in several ways in security aspect in the cloud-like Authentication of data in the cloud, Authentication of the user, Encryption of data, Denial of service over the network, QoS infrastructure management. Here we illustrate all the policy which handles the cloud computing security challenges. This chapter is mainly based on the security topics relevant to the cloud framework. When the data sharing is done with a third party, the cloud users want to leave an uncertain cloud provider because information may be in many forms, e.g. Medical records, Credit card details or any other private information. So the security is must to be added to secure essential and confidential information of the user stored on the cloud [38].

To secure data in the cloud platform, generally, we used the textual password technique. With this technique, it is easy for attackers to guess the information. It may lead to eavesdropping, shoulder surfing and dictionary attack problem. The authors in [39] presented an efficient and secure scheme for sharing the knowledge and resources in the cloud computing environment. This scheme provides fine-grained data access control and security against many attacks in the cloud environment. An efficient security framework has been designed in [40], which observers the VM network traffic. The anomaly and signature-based methods are used, which detects both known and unknown attacks. For reducing the overall computation cost, the signature-based detection is applied for the detection of an anomaly.

The Authors in [41] proposed an effective security framework to provide information integrity and data confidentiality to the cloud users. This scheme handles the privacy and integrity of data securely. Without liable on the probability of the cloud provider, this approach allows security, network usage, privacy and cloud storage. A strong foundation is delivered by the application of the AES algorithm that safeguards the data stored in the cloud also approves data access only on effective authentication and verification.

The authors in [42] proposed the colour scheme authentication (CCA) is used to overcome textual based password problems. This is implemented on a private cloud using JavaScript, CSS, jQuery, PHP and MySQL. This CCA scheme solves the shoulder surfing. It also uses a challenge-response system (CRS). A model to prevent and show directly the authentication credentials [43]. In this model devoted firewall defines between the cloud host and the clients supported by VPN, to arrange whole traffic passed by the tunnel. This model helps to reduce the computational cost of complex schemes. The Authors in [44] defines an authorization process model, specially designed for healthcare system on the cloud platform, which combines mobile devices and cloud platform using the cryptographic approach for remote areas medical services.

The authors in [45] presented a novel methodology to increase the Cloud service provider's capability to model users' behaviours. For detection and recognition process, the particle swarm optimization-based probabilistic neural network (PSO-PNN) was used. For ensuring the user's data, the authors in [46] proposed an enhanced security framework which consists of encryption/decryption technique, access control methodology and digital signature algorithms. High held keys are made using a key generation algorithm, i.e. Elliptic Curve Cryptography.

The authors in [47] present analysis relate it with an incident the online hijacking of The New York Times. Here also explained all possible prevention strategies to solve the above problem or incidents. Here, all the incident described step by step and guide for preventing phishing

attacks. The authors in [48] discussed possible threats over the cloud platform. Here, the problems generally found in cloud discussed in two manners. One, the experts concerned about the security issues and threat in the cloud, as the other questionnaire session used to know the perception of the West England University students on the security issue on the cloud in the perspective of data. The authors in [49] proposed DROPS techniques to prevent data leakage by dividing the data file using multiple numbers of nodes to store a single file. This fragmented file used for replication of cloud. The authors in [50] classified the leakage of information in three categories in the cloud platform as Unintentional leak, intentional leak and malicious leak. Further, data loss prevention is being handled by open source software, MyDLP.

The authors in [51], proposes an antiphishing protocol, which allows the only valid use of the cloud. This protocol provides better security and minimum cost due to cutting edge technology of elliptical curve cryptography (ECC). In this technique first, we have to authenticate the valid users using any service on the cloud platform. Here a single password is used for a particular client. The authors in [52], mainly focused on a link-eavesdropping performance model. However, both nodes eavesdropping and link-eavesdropping problem, but the investigation is done on recovering data in the inter-cloud storage system, by link-eavesdropping. It compares the eavesdropping techniques used before with link-eavesdropping.

The authors in [53] determined the security limits of a password-based authentication scheme which was recently proposed and exposed that their approach is susceptible to falsification and other attacks. This method fails to provide mutual authentication, user anonymity and forward secrecy. To avoid these kinds of issues, the authors proposed a secure authentication scheme. The authors in [54] proposed an approach using biometric-based authentication which used effective data storage. This approach supports user authentication for the cloud environment. Iris and fingerprint are considered here for user authentication. For extracting the feature values, the local binary pattern is employed. An ECC based mutual authentication framework

was proposed in [55] for secure communication. The user establishes a session key and authenticates each other. In the public communication channel with the help of the session key, the user can be connected securely. Estimation of bilinear pairing is not required for the proposed approach, which makes this protocol more effective in the communication environment.

For securing the virtual machines in the cloud framework, a host-based intrusion detection system (H-IDS) is proposed in [56]. Logistic regression is used to select the vital features of each class and next using the regularization technique the values are enhanced. A novel intrusion detection system was proposed in [57] combining a fuzzy c means clustering (FCM) algorithm with support vector machine (SVM). This approach improves the detection systems accuracy.

To overcome all these concerns, the authors in [58] presented a novel access control model. For fast and efficient data accessing a temporary table has been maintained by the CSP based on the popularity value and data type of the DO. Using this table the CSP can reduce the data accessing time and search the data owner easily.

A secure and new cloud-based service is proposed in [59]. This approach based on IP-WSN (Internet Protocol-Wireless Sensor Network) and uses advanced internet communication machinery (ICM).

The authors in [60] proposed a new balanced virtual machine allocation policy against such a threat, the coresident attacks in the cloud platform. It helps to prevent unauthorized users who build a side channel to get private data from virtual machines and mainly focused on the initial virtual machine allocation strategies. The authors in [61] introduced a new approach to identify attack at client-side and service provider too. Here IDS (intruder detection system) is used to identify attack using its virtual machine on the back end. The authors in [62] proposed a software defined networking (SDN) and DDoS attack. SDN changes the way of defeat

distributed denial of service attacks in the cloud environment. SDN is used as a tool here to prevent DDoS attack. The authors in [63] explained the energy consumption issues. With the increasing number of resources on demand for customer, application migration on cloud, energy consumption is also rapidly used. The authors in [64] discussed the working of Dynamic Voltage and Frequency Scaling (DVFS) technique used for energy consumption on cloud platforms.

A DVFS-aware algorithm for solving a problem of on-line consolidation and proposed a way to handle the inconsistencies between DVFS techniques and consolidation. The authors in [65] describe the evaluation technique on energy efficiency and analysis of the machine tools, machining systems. It described all the related work which emphasis on the methods which motivated on reducing the energy. It also described the energy-saving model for machine tools and peripheral components or subsystem. As the increasing the number of users, high storage capacity application is also growing on the distributed networks. The application reduces access latency by requesting relevant data centers. The data center is also geographically distributed. Because of this energy consumption is a more effective field for attention [66].

For efficient dynamic resource allocation process, an enhanced task scheduling and an optimal power reduction scheme is introduced [67]. Using dynamic resource table updating algorithm and prediction mechanism, the response time and resource allocation efficiency based on the task completion is attained. The proposed approach lessens the power usage of data centers and brings a proficient outcome as to power reduction. Accurate values are provided by the proposed approach for updating the resource table. With the reduced power consumption and improved task scheduling technique, an efficient resource allocation approach is achieved. To monitor the system load [68] presented a control mechanism to manage the use of VMs in a PM based on the feedback from VMM to DCM. Evaluation of the proposed mechanism is done using a CTMC and the systems QoS parameters is derived. When the system is in the inactive

state, the consumption of power under the proposed mechanism is modelled and valued. The proposed approach significantly saves the consumption of power and provides a command tool for the control parameter.

The authors in [69], proposed an architectural model and QoS control techniques which fulfil the user requirements and the address cloud security. The above project model named as UBIS (Ubiquity and Integration of Services). The authors in [70], explained a survey report by introducing and describing hardware on data center networks. It classifies a detailed architecture of networks of the data center with switch and server-centric architecture. The authors in [71] explained the issue on data segregation and encryption strategies used in cloud computing and proposed probabilistic method for secure private data using Private Data Bucket (PDB) and Non-Private Data Bucket (NPDB). A key is also commonly used for both of the above bucket techniques. The authors in [72] identified the most possible issues which affect cloud-based E-Learning. Nowadays, e-learning is used by many countries, due to its better accessibility, flexibility for user and availability on-demand facility. The authors in [73] described the encryption and decryption process. Here is also a small introduction is also defined related to Data-Encryption Standard (DES), Advanced-Encryption Standard (AES), Asymmetric Key Algorithm-RSA. There are many encryption and decryption algorithms, e.g. AES, DES, RSA, Cipher Block chaining is discussed.

The efficiency of cloud user with the benchmarking data is secured with keystroke feature [74]. As an emerging trend, the IoT services are developing now, which can be interconnected to embedded devices for communication. The security issues in IoT can be handled with the support of Elliptic curve cryptography [75]. The authors in [76] presented stable asymmetric cryptography in algorithm form [77]. Several cryptographic methods, e.g. Advance encryption algorithms (AES), RSA algorithms are employed to improve the data security on the cloud, which enables the intention towards a complete security solution [78]. There are several

authentication approaches based on single and multi-factors. An example of a single-factor methodology is the Smart card-based verification approach [79]. Crucial security protocols satisfy the three-factor authentication agreement policy using proper authentication process such as Real-OR-Random model, BAN logic, etc. For simulation, AVISPA tool along with elliptic curve cryptography can be used as an application tool.

The key agreement protocol policy with secure authentication scheme can be used to accomplish monitoring of agriculture stream with wireless sesnsor networks. The verification among the participants is done with BAN Logic validation approach [80]. In antiphishing protocols, the verification policy is beneficial to a safe cloud environment. Cookie information is used in the three different phased employed by the authors. Authentication, pre-computation and login phases are the three phases available for processing the tasks [81]. The elliptic curve technique is used by the key-based scheme for M2M cloud local environment. Results are evaluated in terms of processing time corresponding to the performed operations [82].

The realistic methodology can be known by handling several attacks and by acquiring the execution time. With two different attacks, they combine namely password guessing attack and replay attack. It involves three phases of authentication [83]. Fake user can be prevented with the help of an IP Traceback based authentication mechanism. FACT, which is a temporal token-based framework is used in Cloud-based trusted authentication process [84]. The authors in [85] proposed a two-factor authentication methodology which uses the password and devices. Authentication and registration are the names of the two phases [86]. When compared to the RSA algorithm, the ECC approach is well known for its popularity or less bit usage. With the mathematically derived definition, the implementation of ECC is demonstrated [87]. With the elliptical curve cryptography method, some of the anonymous techniques are used to share data among organizations [88, 89]. When compared with RSA the Elliptical curve provides improved security along with few complexes. The simulation outcomes are also better

than RSA. In a cloud environment, several types of risk of attacks prevail for example control plane and Byzantine saturation attacks, flow table overloading, Sec-SDN etc. The cloud security framework Sec-SDN is designed to deal with the resistance, routing, attack, and third party handling [90]. Bidirectional verification and authentication operation are used to offer effective load distribution policy, error handling, user's minimum computational overhead and privacy conserving examining protocol. The data duplication based on the cloud attribute is used to provide better security and to manage data leakage during the statement.

In cloud platform, the Kerberos-based identity policy is employed for verification and authentication of the user or data for big data. For auditing purpose, a trusted strategy has been used [91]. For wireless sensor network (WSN) an authentication approach has presented with cost-effective value using public-key cryptography. Software-based solution with ECC is being used here. The Diffie-hellman key exchange, the Kobitz curve and TNAF are also implemented in the network channel above the cryptographic exchange key [92]. An intrusion detection approach is proposed in [93] in this approach the accuracy is improved by the SVM and FCM algorithm. In [94] the authors presented a hybrid classifier with double layers for intrusion detection. In this approach improved SVM, Fuzzy clustering are used and Bayesian Fuzzy clustering and GG-SVNN are used for clustering.

The authors in [95] presented a WAO algorithm with a wrapper built that addressing the traditional Whale Optimisation Algorithms drawbacks. The intension of this proposed approach was to solve the challenge of achieving optimal position value and this is controlled by a crossover operator. The authors in [96] proposed QALO-K, which is a hybrid clustering and capably inherits the advantage of both. In this approach, the k-means helps to attain the global way. With the intelligence algorithm, this approach induces the clustering technique. The authors in [97] presented the GA for a huge sum of data which is a factor for multiple technologies for intrusion detection. To distinct the network data into normal and attack in [98]

proposed the SVM classifier. To delete redundant features and to select the correct features IG is used. The authors in [99] described a survey on Signcryption, which is based on an attribute that finds the essential access control and suitable of cloud data. The authors in [100] explained and proposed a mechanism which prevents unauthorized access of files using hash function labelling protection and auto-detectable approach. The authors in [101] strengthen on prefix hijacks held at a random location in the internet topology.

This case study results using hijacks incidents, occurred on the network. Here direct customers are most resilient of tier-1. The authors in [102] demonstrated the solution of attacking and detection policy over the network using genetic algorithm and proposed an effective mode for best outcomes/results. The authors in [103] explained several approaches to solve the attack on android application. A shadow system approach with an example is used with email login by the user in the mobile application.

The authors in [104] introduced a technique to detect and resolve network attacks automatically using machine learning algorithms with minimal training and compare it with other relevant supervised learning detectors. To deal with the issues in network security issue [105] presented an approach which supports the clients to deal with the attacking problem. It provides detailed information about session hijacking and discussed the prevention mechanism. The authors in [106] focused on the security issues and given some proactive measure to prevent the security breach on the cloud system. It deals with different types of problem like Data Loss, Denial of Service (DoS), Data Breaches, Account Hijacking, Insecure API's, Malicious Insider, Abuse of Cloud Services.

The authors in [107] developed a dual authentication based protocol for medical data in cloud computing. The authors in [108] observed the problem related to the bit shifting and stuffing and suggested a new idea of cryptography to improve security. Here BSS method stuffing is done replacing unused bit which shifting by another character. Here encryption and cypher text

generation is done using 8 bytes. The authors in [109] demonstrate IOT based authentication and key agreement policy, which motive to shift key between public infrastructure (PKI) and cryptography environment without a certificate (CLC). This approach solves three problems mainly, which are legal authentication access, faithful non-repudiation and key agreement, resolve denial of service (DOS) attacks. The authors in [110] gave potential mitigation methods to solve security or attacking issues. The authors in [111] explained return-oriented programming (ROP) attacks protection. The user also protected from reverse engineering.

The "Code obfuscation Engine" (CobE) accomplish system calls and out-of-band space utilization and code stirring. The protection is done due to hijacking specifically flooding of buffer and return-oriented programming problems. The authors in [112] demonstrated improved RSA algorithm using bit stuffing technique on SSL, which provide better communication. To enhance security, they applied cryptographic approaches to prevent the attack of the proxy user or account hijacking or data hijacking. The authors in [113] demonstrated the discussion on intrusion detection system in IoT-field. Their contribution leads to develop a robust intrusion detection system in a crucial environment. The authors in [114] described a technique using cryptography approach RSA with Fermat's rule in cloud computing to provide secure data transmission as well as communication. We use Fermat rule to speed up the encryption process of RSA. The authors in [115] proposed a protocol to prevent the dictionary-based and brute force attack.

The discussed protocol named bounds the login attempts from unauthorized user. It uses the ATT (Automated Turing Test) approach to provide convenience to authorized attempts. The authors in [116] suggested a framework for dynamic decision making on Smartphone devices. It takes different parameters like CPU utilization, execution time, memory usage and energy consumption for offloading decision making. Their optimization model protects the data from any hazard. The authors in [117] worked for a biometric security threat. They proposed a new

e-Finga scheme for secure authentication service that uses user's fingerprint.

The cloud task execution was done using the intended dynamic clustering league championship (DCLCA) scheduling method, which also handles fault tolerance and this lessens the autonomous task failures. The proposed algorithm improves the overall execution of the cloud setting and offers a quality fault tolerance aware scheduling [118]. A novel approach regarding the resistance and recognition of DDoS attacks. Particle swarm optimization (PSO) and multi-agent system are employed in this approach by the agents among themselves to have precise decision making and robust communication [119].

In the public cloud domain, the presented algorithm is implemented and when validated with the current algorithms, this algorithm attains minimized energy and storage time with improved security [120]. An approach was made using improved Artificial Bee Colony (ABC) algorithm, the intension of the proposed algorithm is to provide security and scheduling satisfying the QoS requirements in cloud domains. In each datacenter, a hive table is maintained which aids in decreasing the makespan, cost, task migration, security issues and load balance is presented in [121].

The authors in [122] addressed the multi-objective task scheduling problem by presenting an effective EDA-GA hybrid algorithm. In this approach, the task completion time is minimized and the systems load balancing ability is enhanced. The EDA operation is followed to generate some feasible solutions and a new solution is generated by selecting the GA in the preceding step and at last, the optimal solution is attained. A distributed algorithm is proposed in [123], which is depended on the experience of mutual performance of players partaking in the game and the Iterated Spatial Prisoner's Dilemma (ISPD) game.

Many researchers have analyzed secure data transmission in cloud computing. A portion of the exploration works are broke down here: The authors in [124] have developed a structure for cloud building which securely provides data transmission from the relationship of the client to

the CSP servers. To provide two-path security, they have used a joined procedure of steganography and cryptography on the network through which the data is transmitted. To begin with the data gets changed over into a coded plan utilizing an encryption algorithm and a while later, this coded bunch data is again changed over into a disagreeable picture utilizing steganography. Also, steganography furthermore covers the nearness of the message; along these lines ensuring the chances of data being modified was insignificant. The authors in [125] analyzed, secure information transmission utilizing the RSA algorithm. The RSA algorithm can be characterized as a lopsided key algorithm that was utilized to build up the solid security model. Secure cloud storage of information proposed in [126]. The information put away in the cell phones was expanded as further applications were conveyed and executed. If the telephone was harmed or lost, at that point, the data put away in it gets lost. Secure information transmission in a cloud situation has investigated in [127]. In this work, they have portrayed the genetic algorithm and visual cryptography related papers, which assists with knowing all zones where these strategies would be utilized. A genetic algorithm was being used for giving encryption and decoding, for concealing basic information they were utilizing visual cryptography. They infer that the security highlights of the genetic algorithm were incredibly streamlined utilizing visual cryptography.

Protected information transmission systems in cloud IoT has introduced in [128]. Elliptical curve cryptography is executed by this assessment on the IoT moreover; a get-together imprint is used by it with limit riddle sharing instruments to ensure the Map-Reduce technique on the cloud computing stage. The authors in [129] created enhanced profound made sure about information transmission in cloud conditions giving IoT security utilizing AI procedures. To start with the HNS Public Key Generation (PKG) system figures the open key and a banner worth, at that point using an open key. The authors in [130] analyzed secure information transmission in the cloud. In the cloud, the information is moved among the server and

customer. Cloud security was the current conversation in the IT world. The information was made sure about in server-based on clients' decision of security strategy so information was given high secure need. The authors in [131] have investigated secure exchanges in the cloud. They have clarified that the utilization of a progressive exchange apparatus can improve information security. For secure information transmission and recuperation, they used a fast response code and a hash-based timestamp with the objective that on-going attacks could be stopped or blocked. The fundamental issue with that protected information exchange was that they were not familiar with recovering information from other new kinds of assaults. The authors in [132] implemented an IoT communication system along with embedded cloud and MANET integrated framework for enhanced and secured communication. Cybersecurity using a multi-layer machine learning approach was introduced in [133]. The research gives an outline of cybersecurity data science and introduces an intelligent decision-making approach for protection against cyber-attacks.

In a cloud environment, the authors in [134] present the task scheduling in a cloud-mist condition and afterwards intend a heuristic-based calculation, whose significant goal was accomplishing the harmony concerning the makespan and the money related expense of cloud assets. Bandwidth conscious distinguishable task scheduling for cloud figuring have created [135]. For the detachable task-scheduling issue a nonlinear programming model based on the limited multi-port type was introduced. By fathoming that model, the streamlined portion plot that decides the correct quantity of tasks allotted to every virtual asset hub was acquired. Initiated on the upgraded assignment plot, a heuristic algorithm termed bandwidth-aware task-scheduling (BATS) was offered.

The authors in [136,137] have analyzed task scheduling and asset portion. A load-balancing task scheduling in cloud figuring with the qualities of cloud registering and unique adaptive genetic algorithm (AGA) developed in [137]. This procedure deals with a task scheduling

succession with a normal job and the shorter job makespan yet also fulfils between hubs load balancing. In a heterogeneous multi-cloud condition [138] have analyzed a productive algorithm for task scheduling. The MCC algorithm was a solitary stage scheduling though rests were two-stage scheduling. Task schedule dependent on the meta-heuristic technique in the cloud have investigated [139].

A scheduling strategy for cloud task was proposed in [140], which were based on Ant colony optimization (ACO) algorithm contrasted with distinctive FCFS scheduling algorithms. These approach's fundamental objective is to limit given tasks makespan. ACO would be utilized for apportioning the approaching jobs to the VM's. Exploratory outcomes indicated that cloud task scheduling dependent on ACO beat FCFS and cooperative methods. In cloud platform [141] has dissected a multi-target task scheduling. In this study, a multi-objective nested PSO approach is used to improve the vitality and preparing time. The results of the algorithm are executed in an open-source cloud platform. The exploratory outcomes showed that the techniques MOPSO out-played out the BRS and RSA.

A study in which a chaotic social spider algorithm was proposed [142] to deal with task scheduling problems in a wide range of heterogeneous VMs. In this research work, the overall makespan was reduced with effective load balancing. This work uses the social spider approach with chaotic inertia weight. A study to deal with the issue of task scheduling by proposing the TOPSIS–PSO approach is presented [143]. The optimized fitness value (FV) is calculated using the proposed method. Hence as a fitness evaluation tool, the TOPSIS is used. In this study, three main principles are employed such as execution time, transmission time and cost. An implementation of a hybrid approach with ant lion optimization (ALO) algorithm and differential evolution (MALO) is discussed in [144]. These works deal with the multi-objective task scheduling issues in the cloud domain. A study conducted in [145] using a hybrid job scheduling algorithm. The hybrid approach was done using Harmony and Tabu search

algorithms. In this approach, the method used is based on some of the QoS factors. Comparison of results was made with the existing hybrid algorithms. The superiority of the intended approach was validated in terms of the QoS parameters.

A study is also conducted in [146] for improving the task scheduling for that an enhanced PSO algorithm was proposed. In the existing PSO algorithm, the problem of inertia weight assignment was solved by a tuning function based PSO (RTPSO). Surveys of PSO based scheduling algorithms are discussed in [147].

In the cloud domain, the clustered resource management techniques using the ABC algorithm is examined in [148]. In this algorithm, three kinds of bees are utilized for probing food sources and they are scout bees, employ bees and onlookers. (1) In the cloud VM, the scout bees are engaged randomly in the initial population phase. (2) Fitness is determined about the Evaluation of Population. (3) the best fitness scout bees being picked and the sites accessed are extracted from the VMs region. (4) Based on VM request a cluster is calculated. The VM in this step has also been grouped to meet the response bias of its resources. (5) Through the processing time, the VM load is calculated. If the loaded VM's normal derivative is only the average load, the device is in a balanced condition, or else in an imbalance condition have presented in [149]. The studies are modelled with 100~800 tasks with 10 data centers.

During the ABC optimization process, the VM's resources specifications are randomly generated and grouped. The integration of a Crow Search algorithm and Firefly algorithm have implemented [150]. The algorithm focus is to enhance global search capacity, which reduces the efficiency of the cloud system and optimizes the overall output. For the task scheduling, the authors in [151] presented the multi-objective optimization based whale optimization algorithm (WOA), targeting at enhancing the cloud systems efficiency with provided resources. In this regard, the author suggested to augment the WOA approaches solution search capabilities for cloud task scheduling (IWC) using the improved WOA. The author presented

the execution of IWC and the simulation outcomes reveal that in comparison with the current metaheuristic algorithms, the IWC has an excellent convergence precision and ideal task scheduling plans. In the case of large-scale and small operations, it can also yield better results on resource optimization [152] have designed and developed a task scheduling algorithm that is capable of selecting the appropriate resource to manage virtual machines applications (divergent and complicated) by using a modified PSO algorithm.

A deep reinforcement learning-based resource allocation presented in [153]. This work provides the user with an effective resource allocation approach in the network. In the dimensionality problem, the conventional Q-learning model fails to succeed in an increase in state space. The introduced scheme is joined with ideal resource allocation using deep reinforcement learning to provide better allocation. The authors in [154] presented An Energy-based Flower Pollination Algorithm (E-FPA) for VM provision. To enable energy-based allocation of various VMs in a PM is the main aim of this system and this was attained using the Dynamic Switching Probability (DSP).

A novel design was proposed by the authors in [155] for optimal resource allocation and management. Combining the PSO's velocity update in GWO the optimization concept was proposed and the proposed system was named as VU-GWO. A novel objective function was modelled for optimizing the resource allocation that considers the balanced cluster use, threshold distance, the system failure and the total network distance.

A study conducted [156] on a blockchain-based cloud manufacturing architecture. This study intended to augment decentralization and information transparency. The manufacturing resources are exposed by the proposed platform and they are enfolded as services. Any user can purchase the manufacturing services by accessing the platform. To record transaction results and to intermediate the service composition the blockchain is used in this study. A decentralized resource management agenda using blockchain developed in [157]. The main

issues in cloud data centers (DCs) are cost minimization. This study presented minimizes the energy consumption cost of the traditional power grid, requests migration and scheduling cost in DCs. For saving the cost, this framework presents a requests migration method dependent on RL and embedded with smart contract. With the aid of blockchain presented a resource management system termed BCEdge in D2D-assisted mobile edge computing [158]. This system discharges the load of edge clouds and is a reliable scheme. Using interaction charts and flow charts, the advantages and technical details of BCEdge are explained in the study. The superiority of the presented scheme is validated. The VM placement and task allocation problems in a single cloud/fog computing environment devised and presented in [159]. As a solution for VM placement and task allocation problem, this work presents a Genetic Algorithm Based Virtual Machine Placement and a task allocation algorithm.

Because of the objectives of developing the QoS performance and lessening the deployment cost presented in [160]. This work presents a better optimization algorithm for resource allocation. Within the given budget, the proposed approach allocates the resources considering the QoS requirements of different customers. A load balancing and scheduling algorithm were proposed in [161] which is of quality-assured and SLA-aware. This algorithm migrates the tasks from the overloaded host VMs and presents it to the high capacity under loaded host VMs. The SLA parameters considered in this algorithm are VM memory capacity, processing power and bandwidth.

A resource allocation algorithm using the hybrid differential parallel scheduling is presented in [162]. In this approach, the first thing designed is the data and the grid structure. The resource attributes are classified using the clustering analysis process; then the sliding window is split into multiple sub-windows. In [163], this study presented a hybrid optimization algorithm by using simulated annealing (SA) and artificial bee colony (ABC). Efficient scheduling is done based on the priority of the request, size of the task and the optimal distance. An effective

algorithm for task scheduling presents in [164]. The tasks of the user in this approach are stored in the queue manager. This approach calculates the priority and the proper resource allocation is done for a task. An efficient task allocation algorithm by Hybridizing GA and PSO presented in [165]. When compared with some of the existing approaches the proposed approach succeeds in minimizing the tasks total execution time and cost. The workflow application load balancing is improved using this approach.

Based on feedback control (QVRA-FC) presented a QoS-aware virtual resource allocation, the resource allocation between multiple VM instances are carried out using a feedback control method in this study [166]. Recently this approach has been applied in many areas, such as for energy-efficiency optimization, temperature control and load-balancing, etc.

CHAPTER III

Hybrid Clustering-Optimization Approach and Efficient Authentication Agreement Protocol (EAAP) for Authentication

The content of this chapter is published in-

1. **NGCT 2018, Communications in Computer and Information Science, vol. 922. Springer, Singapore. ISBN: 978-981-15-1718-1**
2. **Materials Today: Proceedings, Elsevier, ISSN: 2214-7853. SCOPUS Indexed, (In Press)**

CHAPTER III

HYBRID CLUSTERING-OPTIMIZATION APPROACH AND EFFICIENT AUTHENTICATION AGREEMENT PROTOCOL (EAAP) FOR AUTHENTICATION

3.1 Introduction

Cloud computing (CC), is an advanced gift of information technology that allows the user all over the world to access resources through the internet. National Institute of standards and technology defines dynamic resource pooling, cloud as on-demand, and ubiquitous network for quick access and storage with adaptability. Even though the cloud offers various features, it lacks full security in one or more forms, where authentication plays a vital role. It is a process by a user ensured through validation. The validation process involves policy verification using either password, OTP (one-time-password) or biometric techniques etc. Remote access is done for the user from the cloud to both software and hardware resources by employing inclusive distributed services [51].

CC deals with software applications, platforms, infrastructures and several in the form of usage and request-service. The implementations, storage and cloud resources virtualization are the foremost requirement of CC. By a central hypervisor machine, the cloud structures whole operational function are managed. Hence, because of the massive traffic created in a cloud atmosphere, this knowledge has become a noticeable structure for the hijackers and intruders. In the cloud framework, the cyber-attack is the emerging threat for cloud information, mostly the DDoS attack. Besides, bandwidth and resources utilization damaged by the packets flooding in transmission protocols [71]. The entire environment or short term

problem will be collapsed. Generally, to guard against zero-day attacks, these security anxieties covered the mode for the intrusion detection software deployment. The false alarms are present in the prevailing harms with IDS that donates to misuse challenge and in cloud anomaly detection schemes are applied to minimize these attack types.

But, applying these detection schemes in the cloud increases the event quantity, hence, the approach used for detection turn into a load which is sorted using soft computing. These improve the accuracy and efficiency of anomalies detection rate and includes Genetic Algorithm (GL), Artificial Neural network (ANN), Fuzzy Logic (FL), and so on. Due to the capability to deal with data, ANN is widely used which is not complete. For intrusive data detection, the mining rule association scheme is also a presently adopted method. In many ways, ANN is used in intrusion detection[168].

The increased amount of training sets and requires an appropriate amount of time for efficient implementation are the major drawback of IDS. The ANN is robust as well as secured technique in the cloud which is combined with GA for improved performance. The PSO, Harmony Search and Artificial Bee Colony are some among examples. The ability of IDS is enhanced by search methods which achieve determining the ideal restrictions of the network. Furthermore, password guessing, UDP SYN floods, FTP/Telnet port scanning, eavesdropping, phishing, and e-mail bombs are placed in fuzzy rule-based detection schemes and made to manage intrusions in the network. These rules address the diversity of variables and demanding a certain time period for training. For sensing such interruptions confined training samples are being used with SVM in a networking atmosphere. Concerned with data dimensions, it also keep-up with the classification accuracy. In the case of SVM classifiers produced better results in terms of false positives[167,169].

The users in the cloud can store and transfer from browsers to personal devices their

data such as documents, image, video etc through the internet. Yet to transfer these data in a secured manner strong security mechanism should be implemented and still security remains as the main challenge in cloud computing In this work an EAAP is implemented that uses Diffie-Hellman key exchange mechanism with ECC.

3.2 Methodology for IDS With Hybrid Clustering Optimization Approach

In IDS, the rate of detection and accuracy is based on the ability of the classifiers, which properly tracks the events without any conceding with the detection performance. Also, a major incidence of false alarms is faced by these systems which is a serious burden for internal operators handling such actions. A significant concern about this is adequate resources and lack of time and the organizations dealing with the generated false alarms have been developed as major anxiety moreover it initiates caution and develops the prospect of the anomalous behaviour which are undetected. DL and ML techniques nowadays are proficient to be implemented as IDS. The IDS are domain-specific and their structures are very simple. High precision rate is attained by using high-quality data ML techniques. The enormous volume of data is handled by the deep learning approaches. The execution time can be reduced with the support of nature-based algorithms, hybrid optimizations and fuzzy clustering systems. The algorithms such as ABC, SA, GA and PSO are consequent from nature-inspired procedures. For attaining better performance in the detection schemes, the spider monkey optimization (SMO) algorithm can be used. This technique is also used to detect disease in the plant in a high-dimensional subset. The intruders in the network can be classified using the hybrid approach of SMO with FCM. Complex real-world problems are solved using this system and they offer solutions that are efficient and resource-intensive. The implementation of this methodology presents improved performance recognition by advanced accuracy of the IDS in the cloud environment. The Euclidean distance is used by the recent approach for updating

and to attain the optimal solution. The optimization problems are handled using the fuzzy rules which builds a strong wall to deal with these concerns moreover an effective swarm intelligence algorithm is used to process and monitor the processor location including the sizing problems. Thus for reduced energy consumption and optimal resource utilization, it is implemented in cloud environments. The Block diagram of the proposed approach is depicted in Figure 3.1.

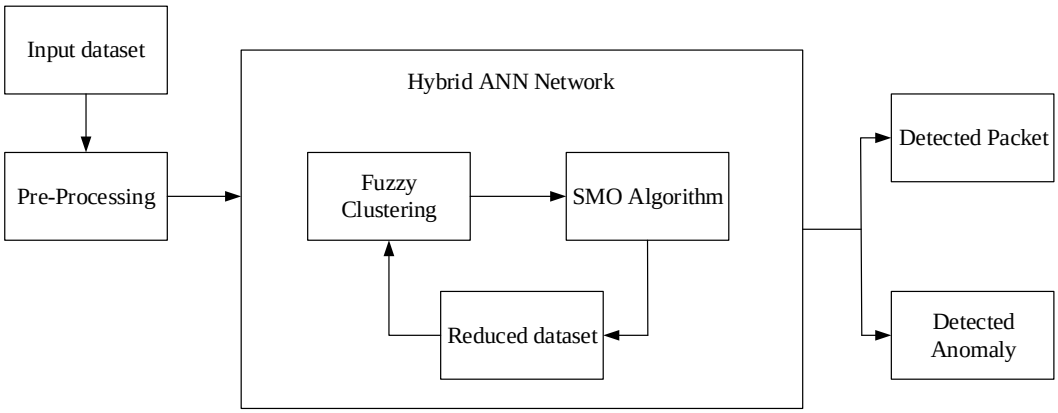

Figure 3.1: Schematic representation of the proposed work

3.2.1 Fuzzy C-Means (FCM) Clustering Technique

The well-known method used for clustering is the FCM. In each cluster this approach changes the data points; therefore the small clusters are made forcibly to gather in large neighbouring clusters. There is a continuous membership among the point between two cluster centres. The same scale should be possed by the clusters(c) and the cluster numbers should have prior knowledge.

Step 1: Segregating the data points in k-dimensional vector.

Step 2: Using objective function obtain the cluster centres in each cluster

Step 3: Employ fuzzy separation.

This method is entirely different from hard c-mean. The the range of membership matrix

elements are [0, 1].

3.2.2 SMO Algorithm

The foraging behaviour of the advanced spider monkeys forms the SMO which is a metaheuristic strategy. The foraging activities of the Spider monkeys' emphases on the social system of fission-fusion. This algorithms character depends on the social structure of a group. The association's representative as an entire is here named the national leader while the local leaders are known as the regional group representatives. This algorithm does not have any impact on the solution due to the food shortage. In this algorithm, there is less number of apexes at any minority group. The Spider Monkey (SM) is the logical solution to this algorithm. The next section describes the process involved in SMO.

3.2.2.1 Global Leader Selection

In this stage, this algorithm notices the packs in the cluster which is diverse from the cluster site. In each packet's header, the IP address is available. The solution is updated on behalf of the probability of selection, which is designed using the below equation.

$$fn(fit)_k = \begin{cases} \dfrac{1}{1+f_k} & ,if\ f_k \geq 0 \\ 1+abs(f_k)\ , & if\ f_k < 0 \end{cases} \tag{3.1}$$

In this phase, the formula below computes the probability of fitness value.

$$PROB = 0.9 \times \frac{fn(fit)_k}{\max[fn(fit)]} + 0.1 \tag{3.2}$$

The position is updated in the next phase.

$$Cnew_{l,m} = Cnew_{l,m} + dis(0,1)*(gl_{n,m} - Cnew_{lm}) + dis(-1,1) \times (C_{rm} - C_{lm}) \tag{3.3}$$

The global leader is represented by the random number (dis) in the range (−1, 1). In the first component, the current packet persistence is displayed, the packet attraction in the second component is exposed towards the global leader and the stochastic behaviour of the algorithm

is retained in the final component. In this equation to improve the search space efficiency the second component is used, while in the final component the risk or the premature convergence of being wedged in the optimum locale is prohibited. Based on the location value the anomalous packets are identified by the selection process of the global leaders. Among the other packets, a local leader is recognized isolating the clusters for sophisticated anomaly recognition.

3.2.2.2 Local Leader Phase (LLP)

In this stage, the entire clusters updated themselves which is a vital process for SMO algorithms. Because of local community leaders and the local leader's response to the location of the packet in the cluster is often changed. Each packets fitness is updated and evaluated, if it is greater than that of its existing one,

$$Cnew_{l,m} = Cnew_{l,m} + dis(0,1) * (ll_{n,m} - Cnew_{lm}) + dis(-1,1) \times (C_{rm} - C_{lm}) \quad (3.4)$$

The local leader is represented as *ll* and dis() is a random number in the range (−1,1).

3.2.2.3 Local Leader Decision Phase

The Local leaders in this phase have been united with the global leader. In the Local Leader Level, there is no local leader updated and the positions of the cluster members are changed using Eqn 3.5. The disturbance intensity is used.

$$Cnew_{l,m} = Cnew_{l,m} + dis(0,1) * (gl_{n,m} - Cnew_{lm}) + dis(0,1) \times (C_{rm} - ll_{lm}) \quad (3.5)$$

From equation 3.5, it's known that global leader changes the search directions and positions. The prevailing local leaders reject the solutions which are not updated by the local leader to the TL. The TL is incremented when attaining a fixed value and is considered as a threshold counter.

3.2.2.4 Global Leader Decision Phase (GLDP)

The global leader(gl) boundary is the limit in which the global leader identification is not done. The swarm is combined or split into two subgroups. Within a given range, the GLL parameter monitors for premature convergence, when GLL exceeds it is set to zero. The group is separated by the gl once the whole clusters are lesser than the pre-set considerable groups.

3.2.3 Hybrid FCM-SMO Method

The FCM is used for clustering the packets and the packs are assembled together into n number of clusters. From k initial starting values the clusters are then initialized. Depends on the position value each cluster finds the global and local leaders which are the incoming packets the IP address.

The clusters without irregularities are fused when the algorithm influences it is optimal and to find the intruder clusters with these local or global points are segregated.

Steps of the algorithm are specified beneath

Step 1: Set k –Select the preferred number of clusters, k.

Step 2: Initialization –k is selected as the initial starting value.

Step 3: Classification - Obtain global and local leaders;

Step 4: Position value of the local leader is updated

Step 5: Position value of the global leader is updated

Step 6: Discover the global leaders

Step 7: Discover the local leaders

Step 8 Position of the local leader is updated.

Step 9: To elect fission or fusion the decision phase of the global leader is used.

Step 10: Halt and state the best solution when reaching the end criteria or else go to step 3.

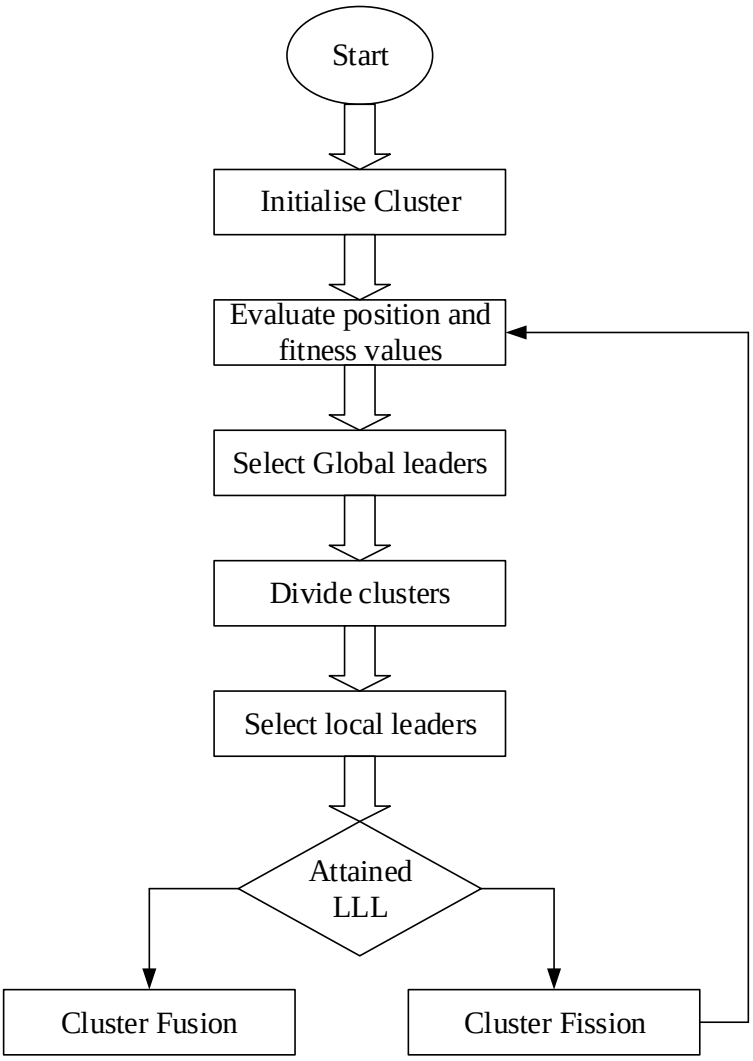

Figure 3.2: Algorithm flow diagram

In a step by step procedure, the SMO works in which the search region has the local leaders and the position updates are done by the global leader. Every member of the cluster in the local leader updates the position in the global leader phase, the position values are updated in the clusters optimal points. Amongst the other search-based algorithms, the SMO algorithms special feature presents it an enhanced one and a natural method is followed by the proposed algorithm for checking the immobility. During deadlock, periods to monitor the search operation the global and local leader learning phase is involved. Both the leaders' make a decision in such cases and the local leader ensures an advance exploration in the decision phase,

a fusion and fission choice is made. During classification, the search speed is stabilized by SMO.

3.2.4 SMO Based Dimensionality Reduction

The dataset dimension reduction is done in this section using the optimization algorithm. During classification when the features are high causes the overfitting problems. The proposed approach uses the SMO which is used to deal with the dimension problems. Searching operation is carried out using the SMO in an exclusive way for gaining a datasets best dimension. The optimal dataset is the one which has better accuracy with a lesser error rate. In intrusion detection problems the dimensional reduction is subject to objective conflicts to increase classification accuracy and minimize the dimension count and error rate. Achieving optimal results is difficult when there is an incidence of trade-offs among contrasting priorities. In this situation, to minimize or optimize the detached functions a multi-objective optimization technique is used. To achieve the maximum accuracy (A) the proposed approach was intended. To calculate the SMO's classification error (E) the precision is used as an output metric in this study.

To calculate the individual causes the fitness function fit(fn) is used and described below;

$$fit(fn) = \lambda \times (1 - C) + (1 - \lambda) \times SD \tag{3.6}$$

For dimension subset extracted, the classifier accuracy is represented as C, the classification accuracy and dimension reduction are regularized using the constant λ, S represents the extracted dimension subsets, D represents the number of dimensions in the range [0, 1]. The resultant dimensions of the datasets are passed for further classification. A group of anomalous packets or a group of detected normal packets are present in the classified cluster. The hybrid approach used for classification results in reduced resource allocation with high detection ratio and accuracy.

3.3 Methodology for Efficient Authentication Agreement Protocol

Usually, secure communication between client and server is established using user name and password as shown in figure 3.3.

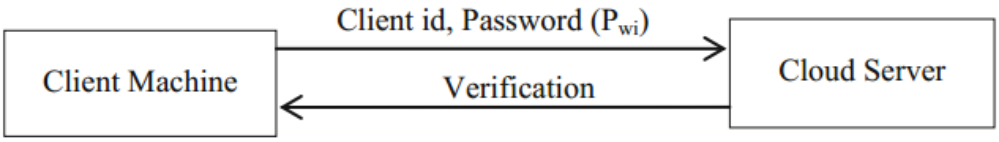

Figure 3.3: Effective System model

The proposed mechanism is processed in three phases i.e. Authentication phase, Verification phase, Registration phase, and log in. The elaborated steps are explained below. Table 3.1 illustrates the notation used in this process.

Table 3.1: Notation used in the proposed mechanism

Ui	Machine identity of client
S_R	Server
P_{wi}	Password for client
K_i	Public key
R_i, R_k	Random value generated by user
R_s	Random value generated by server
H_f ()	Hash function
OTP_c	One time password for client
Ecx	Key used in ECC
P	Large prime number
G	Generator Point
C_{ki}	Cookie information
End_time	Expiration time of the client
$\oplus$	XOR Function
|	Concatenation symbol
I	Integer value for client

Phase1: Registration:

- A user requests to the server using the public key (Ki).
- Random value generation by the user (Ri) and server (Rs).

- Expiration time (end_time) and Cookie information is computed.
- Storing of end_time, cookie by user accompanied by generation point G and public key (Figure. 3.4).

Cloud User U_i	**Server S_R**
Submit Ui and P_{wi} to the server then perform and store Ui, $R_i \oplus H_f(P_{wi}) \oplus K_i$	$R_i \oplus H_f(P_{wi}) \oplus H_f(Ecx\|Ui) \oplus K_i$
Select R_i	Select R_s
Computes $C_{ki} = (R_i \oplus H_f(P_{wi}) \oplus H_f(Ecx\|Ui))$ Stores C_{ki}, Ui, K_i & End_Time	

Figure 3.4: User registration on cloud sever

Phase 2: User Login and Verification:

- Retrieve the information required by the user (verification in P2 and P2, expiration time, cookie value) if the client has cookie information.
- Perform the computation process with a random number, user id and password if the user has no cookie information.
- Through Elliptical Curve points, the Random value of client (I) is made sure by P2 in both P1 and P2 (Figure.3.5).

Value of C_{ki},Ui & End_Time extract and Computes P2' and Verify P2 and P2'		
If cookie is saved	Select	Computation
Ui, P_{wi} is selected	I P1=I*G R_k is selected	 $R_k \oplus H_f(P_{wi})$ P2= I*C_{ki}
If cookie is not saved	P1, Ui $\oplus$ $R_i \oplus H_f(P_{wi})$	$R_k \oplus H_f(P_{wi})$

Figure 3.5: User Login and verification

Phase 3: Authentication Process:

- Client request for OTP with the public key.
- Server reply with matching key and OTP.
- Verification of OTP using Diffie-Hellman operation.
- If the matching of key and OPT occurs dynamic password is ended by the user to the server.
- Now the user is allowed access to the server (Figure. 3.6).

Extract	**Computation**
OTP_c and K_i	
	$R_i \oplus (P_{wi})$
$R_i \oplus H_f(P_{wi}) \oplus OTP_c \oplus K_i$	
Choose a random No.	OTP_c *I*P3
	$R_i \oplus R_k$
$R_i \oplus H_f(P_{wi}) \oplus OTP_c$	

The Value of K_i is verified by comparing S1 and S2 with two prime number A, q and two private keys with diffie-hellman key exchange security policy

$K1=A^a \text{mod} q$ and $K2=A^b \text{mod } q$

Shared key S1=S2 is being matched by exchanging Public key K1 & K2 to show existence of diffie-hellman algorithm.

Figure 3.6: Authentication method

Public key exchange process using Diffie-Hellman is elucidated below:-

Let us assume that for client and server two private keys are taken that is a = 3, b = 6; A and q are preferred as two prime number, let A = 7, q = 23; the value of shared public key S1 & S2 are computed below.

Client side	Server Side
$K1 = A^a \text{ mod } q$	$K2 = A^b \text{ mod } q$
$K1 = (7)^3 \text{ mod } 23$	$K2 = (7)^6 \text{ mod } 23$
$K1 = 21$	$K2 = 4$

In the client and server-side, K1 and K2 are exchanged these are considered as shared public

key. Using the formula, the shared secret value is calculated with the help of the private keys

$S1 = (K2)^a \bmod q;$
$= (4)^3 \bmod 23;$
$=18;$

$S2 = (K1)^b \bmod q;$
$= (21)^6 \bmod 23;$
$=18;$

Hence the value of K1 &K2 is similar, which please the Diffie-Hellman shared key algorithm.

3.3.1 Outline of the Proposed Methodology

The user request is sent by the cloud user to the server and after computation produces expiration time and cookie information. Based on the cookie information does not exist user can access information using the password and user id with nonce value (Ri) continued by authentication. If the user satisfies the validation, it can execute its operation. Working of user and server in the proposed authentication process is parted into three modules, explained below.

In the first module:

The user registration data retrieved by server and attached with public key followed by cryptographic computation. Random value generation by user and cookie information and expiration time and saved by on client-side.

In the second module:

When the client possesses the cookie value then the procedure is moved to its last stage, if not server performs verification using end_time and user id.

In the third or final module:

Authentication is performed by matching the valid OTP and public key of the relevant user. If the particular user satisfies all the required parameters, the user is then allowed to access (Figure.3.7).

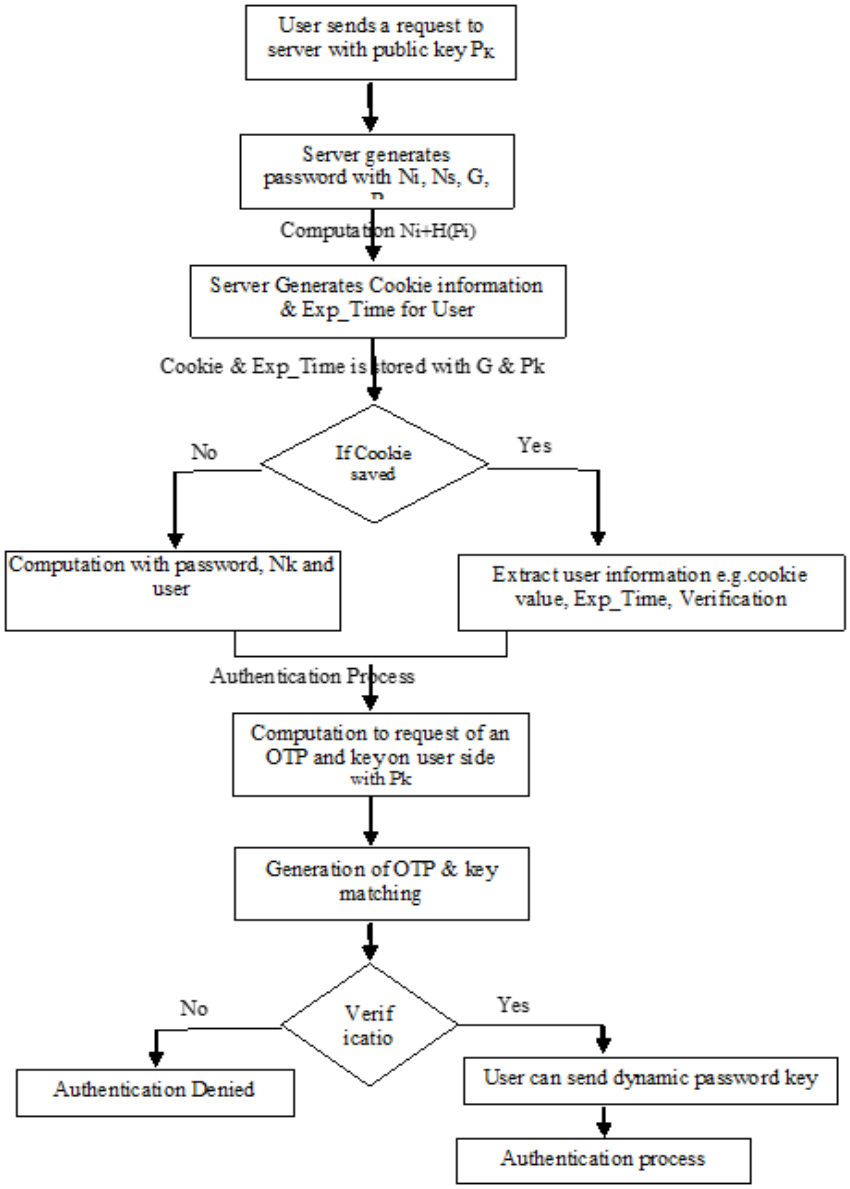

Figure 3.7: Flowchart of the mechanism

3.4 Results and Discussion

The presented EAAP and SMO based authentication approach is compared with some of the current methods and the performance is superior concerning the accuracy, precision, sensitivity, specificity, recall and F-measure. The labels for all cases in the data are available in the NSL-KDD test dataset, which is used for evaluation.

a) Precision:

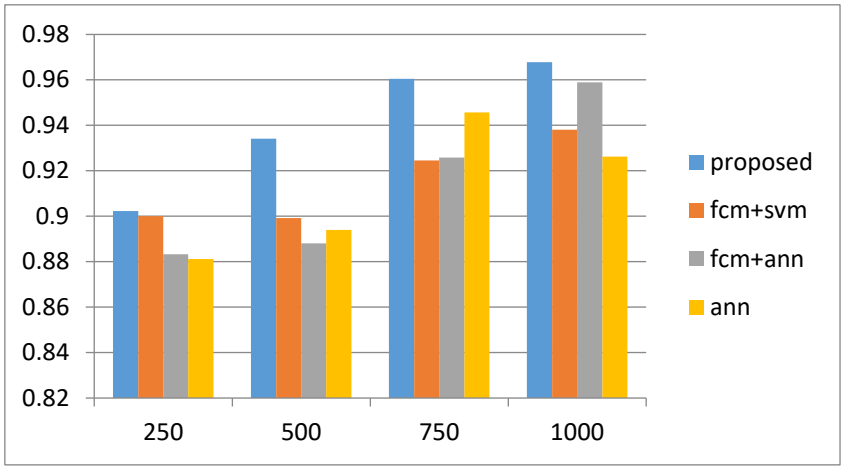

Figure 3.8: Precision

The x-axis of figure 3.8 denotes the number of data is displayed, i.e. 250,500,750 and 1000 and the precision is shown in the y-axis. The proposed approach, when validated with the other methods in terms of precision attains the best value of 0.857, 0.884, 0.866, and 0.847.

b) Recall:

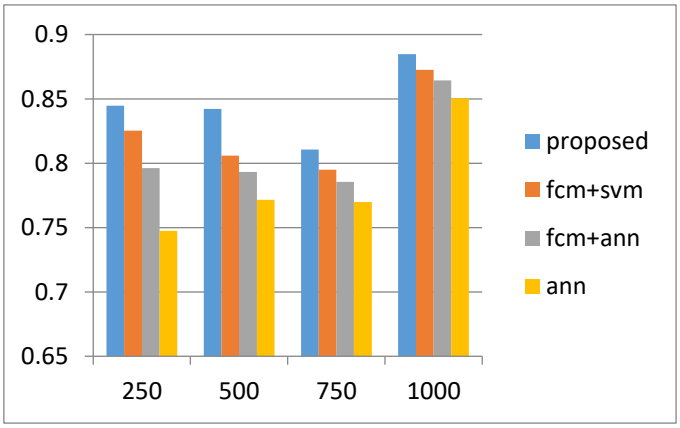

Figure 3.9: Recall

The x-axis of figure 3.9 denotes the sum of data which is 250,500,750 and 1000 and the recall is represented in the y-axis. When compared with the prevailing methods, our proposed method achieves an ideal value of 0.844, 0.842, 0.810, and 0.884.

c) F measure:

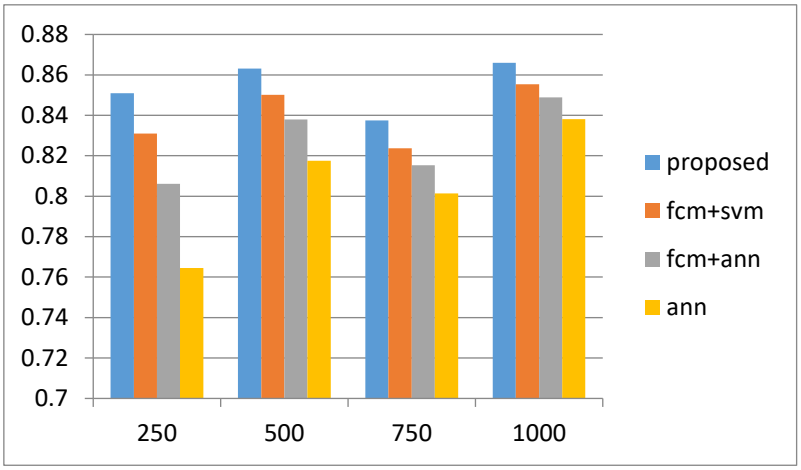

Figure 3.10: F-measure

In figure 3.10 the x-axis indicates the sum of data which is 250,500,750 and 1000 and the f-measure is indicated in the y-axis. When validated with the other methods the suggested method attains an ideal value of 0.850, 0.863, 0.837, and 0.865.

d) Sensitivity:

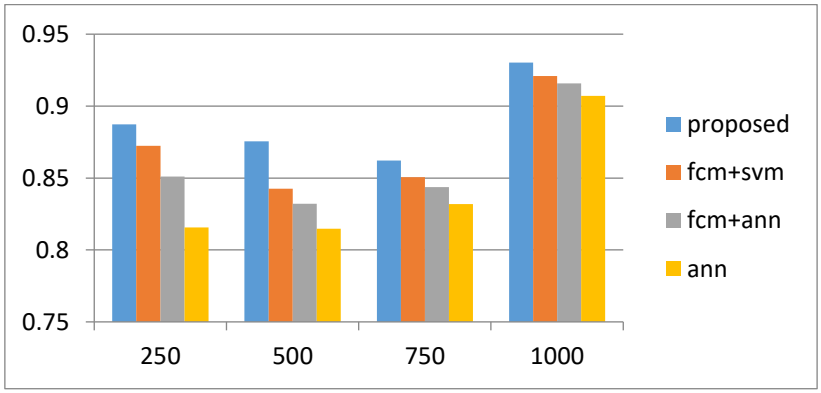

Figure 3.11: Sensitivity

In figure 3.11 the x-axis indicates the sum of data which is 250,500,750 and 1000 and the sensitivity is indicated in the y-axis. When compared with the existing methods the projected method achieves an ideal value of 0.887, 0.875, 0.86, and 0.930.

e) Specificity:

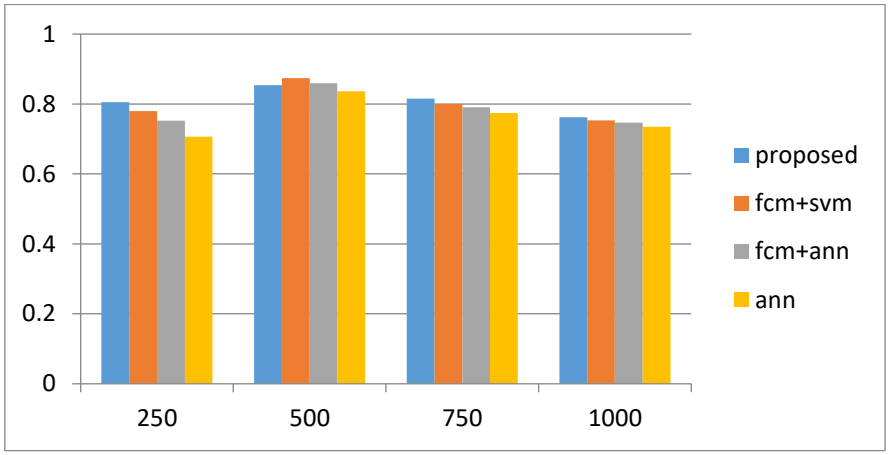

Figure 3.12: Specificity

In figure 3.12 the x-axis indicates the sum of data which is 250,500,750 and 1000 and the specificity is indicted in the y-axis. When compared with the existing methods the anticipated method achieves an ideal value of 0.805, 0.853, 0.815, and 0.762.

f) Accuracy:

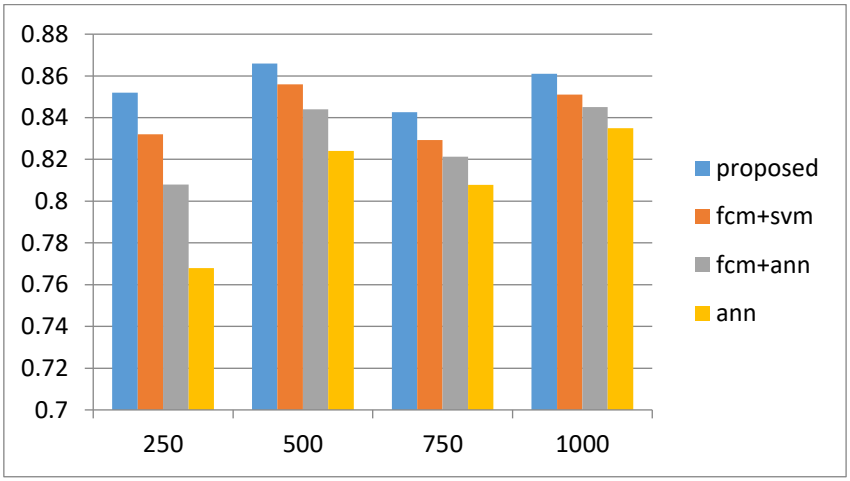

Figure 3.13: Accuracy

In figure 3.13 the x-axis signifies the sum of data which is 250,500,750 and 1000 and the accuracy is indicted in the y-axis. When compared with the existing methods the proposed method attains an ideal value of 0.852, 0.866, 0.842, and 0.86.

CHAPTER IV

Traffic Hijacking Prevention through Prime Number and Character Stuffing Mechanism

The content of this chapter is published in-

1. **International Journal of Recent Technology and Engineering (IJRTE), vol. 7(6), pp. 1043-1048, 2019, ISSN 2277-3878. SCOPUS Indexed.**

CHAPTER IV

TRAFFIC HIJACKING PREVENTION THROUGH PRIME NUMBER AND CHARACTER STUFFING MECHANISM

4.1 Introduction

Cloud computing is a high-performance computational environment with great availability of resources, convenient to end-user, providing services from the remotely located server with large network access feature. It's easy to maintenance and on-demand self-device model-based technology. Therefore, many international companies interested to adopt cloud as a consumer and some are in competition to provide large storage capacity as a provider to consumers. Cloud security also a feature of cloud computing, however, most of the research is still going on to enhance security policies of data on the cloud. Traffic hijacking is the most important problem found which act as a phobia in a large organization as well as cloud users. Here we describe a data security policy to handle hijacking problem of data with stuffing technique [108]. Input data is taken as a character and perform a stuffing approach with RSA algorithm. Generally stuffing refers to the mechanism where data is break/partitioned along with relative cryptographic mechanism. In this chapter, stuffing approach is used with a modified RSA algorithm. For both private and public domain, cloud computing is developing fashion with scalable space accessibility feature. Now, for achieving the objectives of entire security

necessities, cloud security becomes a challenging work. Due to more scope of this research, these issues fascinate the attention of scientists. It prevents the significant and private data of people and reduces the traffic hijacking and cyber fraud even cyber-crime. A cryptographic scheme named RSA-CS with prime numbers has been discussed in this chapter. In the viewpoints of the cloud environment, the RSA scheme is modified for improved outcomes and the proposed scheme is compared with the existing stuffing strategy and utilized for network security. The unauthenticated access and hijacking are prevented by the proposed approach, also it offers superior cloud data security. Eclipse IDE software is utilized for the implementation of the proposed mechanism. Compared to the existing approaches, the modified RSA with character stuffing using prime numbers achieved maximum performance demonstrated by the implementation outcomes.

4.2 Formulation of RSA Mechanism

Assumption 1: In this phase, we take any positive prime no is selected shown as Xi = Pn1, Pn2,....., Pnn that is Pn1 > Pn2 > Pn3 > Pn4 >.....> Pnn, where all Pn denotes prime no. the entity, Where value of Xi must be > 0 (mathematics fundamental theorem).

Assumption 2: n1 and n2 are two-factor value integers as a greatest common factor gcf named df, where integer n1 and n2 proceed with coefficient along with de defined in the linear combination. The coefficient can define as m1, t belongs to Z, where df satisfy following Euclid method as:

$$df = m1int1 + t\ int2. \tag{4.1}$$

Assumption 3: let pn1 is a prime number, for all positive integer value where prime no. should also follow Fermat rule as pn1, x (pn1-1) ≡ 1 (mod pn1).

Assumption 4: let pn1 and pn2 are all relates to prime number and pn1 ≠ pn2, then

$$\phi(pn1\ pn2) = \phi(pn1)\,\phi(pn2) = (pn1 - 1)(pn2 - 1) \quad (4.2)$$

Assumption 5:If the taken value of x not relates to prime no or is a co prime among n values, then we follow Euler rule

$$x^{\phi}(n) = (\text{mod } m) \quad (4.3)$$

4.2.1 Mechanism for Key Generation

1. Calculate the product of random numbers pn1, pn2 and ϕ as:

   $$y = (pn1-1)(pn2-1) \quad \text{(as according to Assmp. 4)} \quad (4.4)$$

2. Input an integer E, $1<E<\phi$ where gcd (E, ϕ)=1 (according to in Assmp. 2)
3. Evaluate encryption exponent $E*df = 1(\text{mod } \phi)$ where $1<df<\phi$.(according in Assmp. 6)
4. The public key is (y, E) and the private key is (y, df) where

   df, pn1& pn2 and ϕ are the secret values.

   E = encryption exponent

   df = decryption exponent

4.2.2 Encryption Algorithm

At sender side:

1. User find the public key (y, E)
2. Present text in positive integer in variable z
3. Encryption proceeds as $fi = z^E \text{ mod } y$
4. Send encrypted data to the receiver side

4.2.3 Decryption Algorithm

At the server-side:

1. Plaintext evaluation with the private key (y, df)
2. as : $z = fi^{df} \bmod y$
3. The user received plaintext/original input data

4.3 Proposed (RSA-CS) Algorithm

1. Let four prime number are pn1, pn2, pn3 and pn4.
2. An integer Ec use as a encryption key;

   $1<Ec<(\phi\ (pn1-1)(pn2-1)\ (pn3-1)\ (pn4-1))$; (4.5)

   gcd(Ec, ϕ production of (pn1-1)(pn2-1) (pn3-1) and (pn4-1))=1, Where Ec and ϕ(n) are co-prime.

3. Find df, Ec*df=1 mod ϕ(production of (pn1-1)(pn2-1) (pn3-1) and (pn4-1));

   $0 \leq df \leq$ (production of (pn1-1)(pn2-1) (pn3-1) and (pn4-1)).

4. We use the public key to send every data (D) or message as :

   $Cipher = D^{Ec} \pmod n$ ` (4.6)

5. Encrypted data message stored and used for stuffing named as (Cstuff), form as a character and add stuffing Cstuff in Ciphertext.

   for e.g. Cipher = Cipher + Cstuff (4.7)

(if more than one digit has in Cstuff than we add these digit and regenerate as one step digit).

6. Now, we retrieve Data (D) by removing Cstuff at receiver end as

Cypher = Cipher - Cstuff and original data transform (4.8)

$$D = Cipher^{Df} \pmod{n} \quad (4.9)$$

4.4 WORKING EXAMPLE

Here we've to choose four prime numbers and retrieve public and private keys

Let prime numbers are

Pn1 = 3, pn2 = 5, pn3 =17, pn4 = 2

Calculate n = pn1*pn2*pn3*pn4;

So n = 3*5*17*2 = 510

$\phi(n) = (pn1-1)(pn2-1)(pn3-1)(pn4-1)$

$\phi(510) = (3-1)(5-1)(17-1)(2-1)$

$=2*4*16*1$

$=128$

The range of E is $1<Ec<128$

$\phi(n)$ should not be divide by E

Let Ec=3

Select $Ec \pmod{\phi(n)}$ to calculate private key

as df = Public key (n = 128, Ec = 3)

Private key (n = 1995, df = 43)

Given Character Data D = 11;

Encryption:

Cipher = $11^3 \bmod 510$

= 311

Now we perform character stuffing as

Cstuff = 3+1+1=5

now cipher = 3115

Decryption:

Remove last stuffed we find original data as plain text/data.

Data (D) = $311^{43} \bmod 510 = 11$

The receive side gets the original data.

4.5 Existing RSA with Stuffing Vs Modified RSA with Character Stuffing (RSA-CS)

Here we used character stuffing with RSA algorithm using n prime numbers to improve cloud security and reduce account hijacking by the theft of information. This can be used to resolve phishing, identity theft problem.

Table 4.1: Comparison between existing RSA with stuffing and Modified RSA with Character Stuffing (RSA-CS)

Sr. No.	Standard RSA	Improved RSA with stuffing
1	Access of data is fast	Accessing is slow
2	The security level is low as compare to stuffed data	High-security level
3	Less overhead during the transformation of data	It proposed High overhead in data transmission
4	It can use for phishing and identity theft problem with limitation of resources	Along with account hijack which leads traffic hijack problem in the cloud, we can use it to resolve phishing as well as identity theft problem adding stuffing techniques accurately
5	It needed more time to execute security policy e.g. encryption and decryption	Less time required for the execution of security policy e.g. encryption and decryption

4.6 Results and Discussion

The above security policy to resolve account hijacking on the cloud which leads traffic hijacking and identity theft problem over the network is done using Eclipse IDE software.

Step1: we implement standard RSA algorithm by using two prime numbers.

Step2: we use four prime numbers following above implementation for the generation of public and private keys. We use encryption and decryption of input relevant user information data.

Step3: we use character stuffing mechanism adding in standard RSA algorithm based on process mentioned above.

Following are the implementation part of the proposed RSA-CS algorithm using stuffing with randomly selected input and then we use encryption and decryption policies on input data. Finally, we add stuffing technique to provide more security and improve the complexity of data in perspective of a hacker or unauthorized user to resolve traffic hijacking problem of any organization/user/group in a cloud environment.

Figure 4.1: Blank layout of the screen during execution

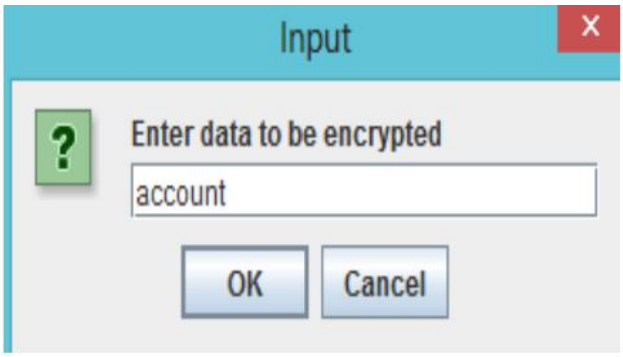

Figure 4.2: Data input on the screen

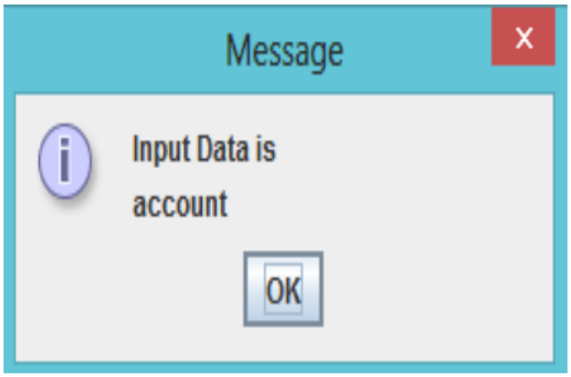

Figure 4.3: Confirmation of data input

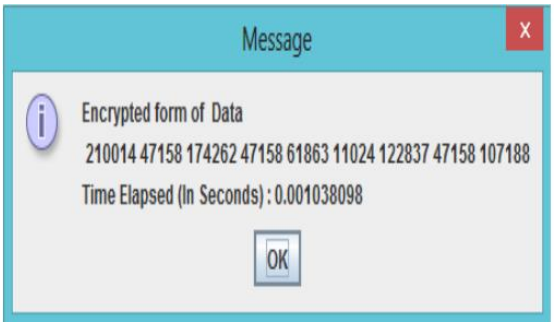

Figure 4.4: Encrypted form of data input

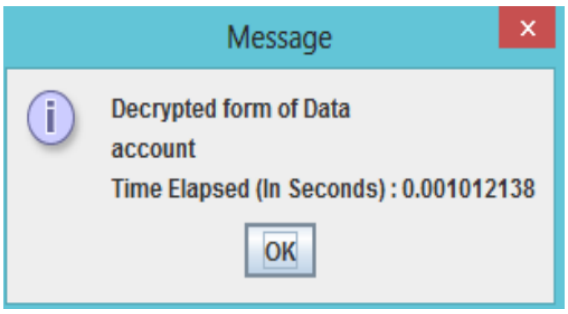

Figure 4.5: The decrypted form of data input

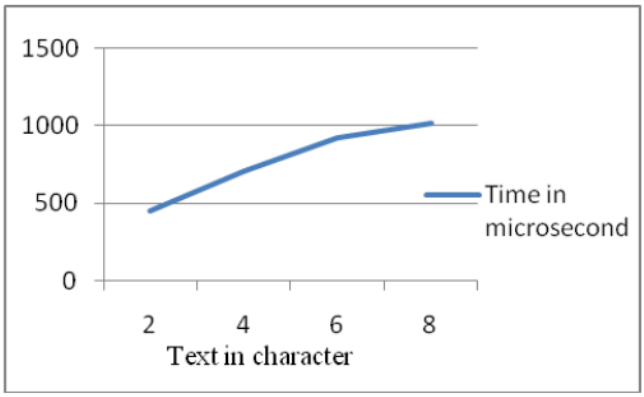

Figure 4.6: Taken time for decryption

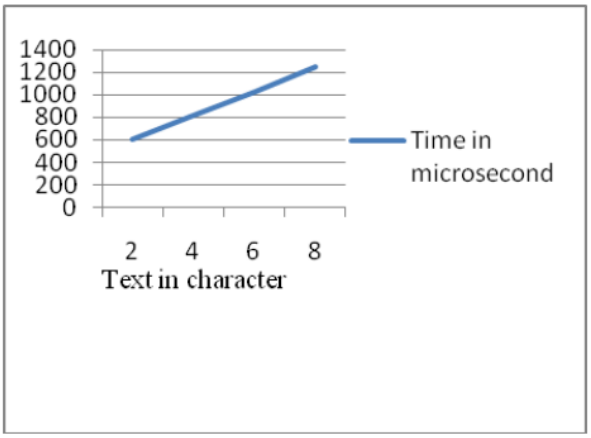

Figure 4.7: Time taken for encryption

Table 4.2: Comparison of implementation time between existing and introduced RSA-CS technique

Input data	Performance time (in Microsecond)	Proposed performance time (in Microsecond)
2	2990	1126
4	3960	1545
6	5160	1986
8	5949	2113

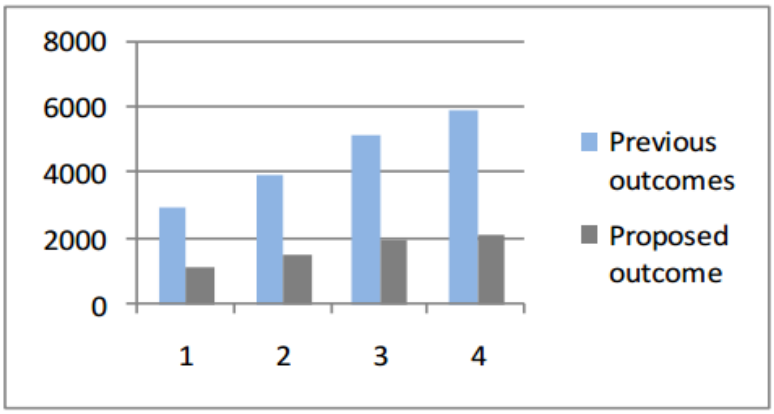

Figure 4.8: Comparison of encryption/decryption time with existing [108] and proposed mechanism.

Evaluation of throughput is also done after the encryption and decryption process as follows:

$$Throughput = \frac{\text{Encrypted text size in MB}}{\text{Encryption time in second}} \quad (4.10)$$

Table 4.3: Throughput of the modified algorithm

Plaintext	Data size (MB)	Encryption time (seconds)	Throughput
2	0.0009530	0.0012	0.7941
4	0.0009450	0.002	0.4725
6	0.0009589	0.00232	0.4133

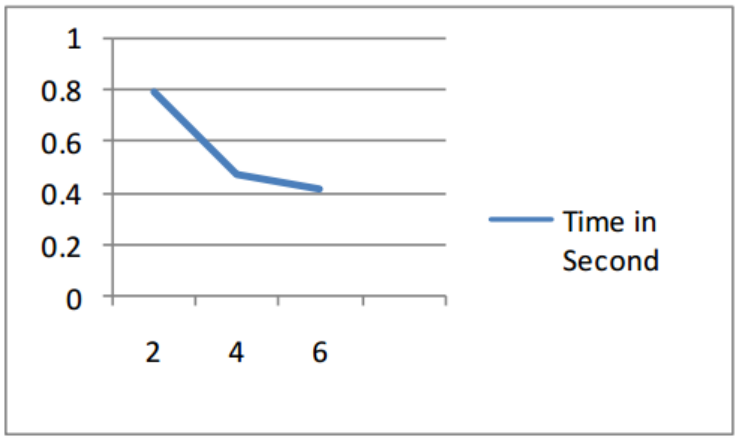

Figure 4.9: Throughput of proposed RSA-CS technique

CHAPTER V

KP-ABE WITH BAN LOGIC TECHNIQUES FOR ACCESS CONTROL

The content of this chapter is published in-

1. **International Journal of Sensors, Wireless Communications and Control, Bentham Science, ISSN: 2210-3287. (Web of Science Indexed) (Accepted)**

CHAPTER V

KP-ABE WITH BAN LOGIC TECHNIQUES FOR ACCESS CONTROL

5.1 Introduction

The cloud is a developed concept in information technology (IT) which makes remote access scalable and easier. This makes the number of users in the cloud to increase day by day and also hackers due to its open nature. Cloud traffic is one among the present most research area in cloud computing along with cost and adaptability. Cloud also owned by particular organization unlike normal computing environment, therefore the concern for the security of information from dangers is at peak.

Even though there are various problems concerned with the cloud there are some techniques which help to lessen the burden on the cloud. This makes cloud to be accessed in less cost, versatile scaling and solves other security issues. The number of a user is increasing who tries to transfer their sensitive data to a remote location and make the framework supportive for their application through cloud. This paves way for stockpiling status, provisioning, web application and application readiness. Cloud also allows using remote resources by using internet service and makes hackers login as users which is difficult to trace out.

The distribution of cloud data across the globe gives quality, availability and low cost but the security is the most critical thing to be resolved for customers of the cloud. The information security is a major part to be governed and the cloud has increased security risk that changes day by day. Prevailing cryptographic techniques, which are the ultimate goal of information security insurance, are not legally accepted because they, unfortunately, limit the information of customers under cloud computing. Due to the variety of client's information in

the cloud, it is important to ensure the security of information stored in the cloud.

Along with these lines, information mystery and approval of cloud customers accept a colossal activity and significantly affect ensuring security to cloud information stockpiling in the business exchange planning. About by definition taking care of and planning information in the cloud to convey with it noteworthy security and assurance stresses, a long way past those that apply in any condition where sensitive information is taken care. That is, except for because of a private cloud, asserted and worked by the information owner, use of the cloud incorporates overlooking control that information to the affiliation giving the cloud organization. Lately, numerous improvement calculations have been utilized to make sure about cloud information transmission. Along these lines, attribute-based encryption is utilized. Attribute-based encryption is utilized to fortify information and is likewise utilized for scrambling the information [39].

Secure cloud data transmission means a transfer of confidential data or proprietary data through a secure transmission channel. Cloud Service Provider (CSP) is a payment service that provides a payment facility that saves important data to be stored on remote servers. Many techniques have been used in the existing paper, but there are several problems. They are listed below,

1) Most distributed computations have only one level of security. The security of computer computation is therefore not reliable.
2) Traditional encryption plans have numerous adaptability issues and thus they could not give total security to the information.
3) Automated data transfer requires additional security measures, as data is more likely to be stolen during the transaction.

4) When a computer receives a large amount of information, it must be checked for reliable and accurate resale. However, cloud storage does not mean this is possible.

This motivates us to design a new technique to secure data transmission efficiently in cloud computing through an encryption algorithm. Privacy and security are challenging issues for cloud users and providers. This chapter aims at ensuring secured validation of user and protects data during transmission in a public IoT-cloud environment. Existing security measures, however, fail by their single level of security, adaptability for a large amount of data and reliability. Therefore, to overcome these issues and to achieve a better solution for vulnerable data, the suggested method utilizes a secure transmission in the cloud using key policy attribute-based encryption (KP-ABE) [170]. Initially, user authentication is verified. Then the user data is encrypted with the help of KP-ABE algorithm. Finally, data validation and privacy preservation are done by Burrows-Abadi-Needham (BAN) logic [80]. The proposed encryption is correct, secure and efficient to prevent unauthorized access and prevention of data leakage. The access control is performed by KP-ABE, where the method attains the maximum of 88.35% of validation accuracy with a less encryption time, which is better when compared to the existing methods. The proposed mechanism is done by MATLAB. The performance of the implemented method is calculated based on the time of encryption and decryption, execution time and validation accuracy. Thus the proposed approach attains the high IoT-cloud data security and increases the speed for validation and transmission with high accuracy and used for cyber data science processing.

5.2 Proposed Method

The implementation of cloud computing provides multiple paths to web service delivery to meet diverse needs. However, data protection and privacy have become a major problem limiting many cloud applications. One of the main security and privacy concerns is due to the possibility for cloud operators to access sensitive data. The objective of the proposed

mechanism is to provide a secure data transmission in a cloud-IoT computing environment using KP-ABE. Initially, user authentication is verified. After authentication, user data is stored in the cloud. For secure storage, the recommended method uses an encryption mechanism for confidential files, which prevents leaks or threats that leads to the loss of sensitive data. Here the proposed method employs the key policy attribute-based encryption (KP-ABE) algorithm for secure storage of the encrypted data in the cloud. Finally, to validate the privacy of input data the recommended technique utilizes the BAN logic. The architecture of the overall system is shown in Figure 5.1.

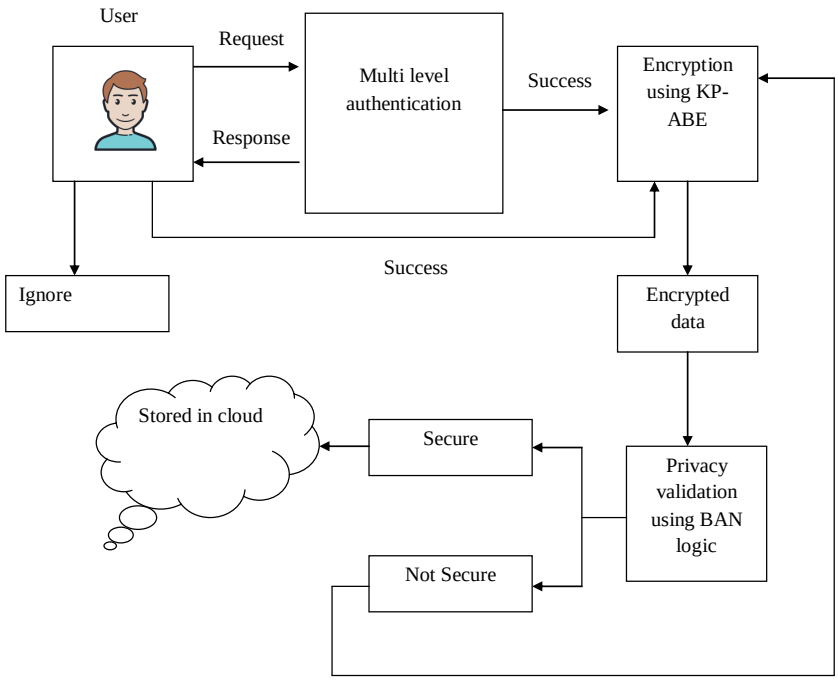

Figure 5.1: Proposed system model

Four main phases represent the proposed approach i.e. user registration in the cloud, multilevel authentication, secure data storage and access policy and privacy validation. All these phases have been discussed one by one in this section.

5.2.1 User Registration in Cloud

A registration request to the cloud service provider (CSP) is sent by the client whenever another client needs to enlist at the CSP. Subsequently, to get the request, the CSP makes a

client profile and accumulates the client details.

5.2.2 Multilevel Authentication

When the registration stage is finished, the client can log in into the framework and transfers the data to the cloud. The server can only be used if the user uploads the data. To start with, the server checks the client information. At the point when the confirmation procedure is finished, the server permits the client to get to the server. This kind of authentication keeps unapproved individuals from getting to the server. To sign in to the server, one has to enter the client's mail id and secret key. On the off chance, that the data gave by the client is right for the particular username, the server will permit the client to get to the information in any case, and the server will disregard the request. Now a data request can be sent by the client to the CSP. Here the data owner or client scrambles the information before the transmission to cloud. For secure storage, the suggested method utilizes the KP-ABE algorithm. The detailed process is explained in the further section.

5.2.3 Secure Data Storage and Access Policy

To improve security, the recommended technique uses the KP-ABE algorithm for encryption. Attribute-based encryption (ABE) algorithm gives a capable device to deal with the issue of fine-grained and secure information sharing and decentralized access control. The accompanying two techniques based on ABE have been proposed: key policy (KP-ABE) and cypher policy (CP-ABE). KP-ABE plans are increasingly appropriate for organized associations with rules about who may peruse specific records. So that the suggested method uses the KP-ABE algorithm for secure storage. The step by step procedure of KP-ABE encryption algorithm is described in the following section.

5.2.3.1 Key-Policy Attribute-Based Encryption (KP-ABE)

KP-ABE algorithm empowers the senders of the interconnected IoT users to encrypt messages based on a set of attributes/identity and release private keys with access functionality that determines the cypher, the key holder will be authorized to decrypt. Thus, the IoT users are validated and the data science security is ensured by the data transmission security using KP-ABE.

The proposed KP-ABE algorithm has four fundamental steps, for example,

1. Setup
2. Key generation
3. Encryption
4. Decryption

Setup:

In this step, a security boundary β is taken as input and restores the master secret key MSK and the public key PK. For encryption, the message sender uses PK. User secret keys are used by MSK and are recognized uniquely to the authority.

Key Generation:

This step takes the information as an access structure AS and the master secret key MSK. A secret key SK is a yield that allows the user to decrypt a message scrambled under a set of attributes (V) if and only if equal to AS.

Encryption:

In this step, a set of attributes is taken as input, data or message D and the Public key PK. It publishes ciphertext C.

Decryption:

Input cypher text C, Access structure (AS) and the user's secret key (SK), which was encrypted as per the set of attributes. A message D is provided as output only if the user's access structure

is satisfied by the attribute set. The input data is encrypted based on the above process. Once the input data is encoded, the resulting output is delivered to the next phase.

5.2.4 Privacy Validation

The innovative approach employs the Burrows-Abadi-Needham (BAN) logic for validation of the proposed privacy. BAN Logic depends on the validation of elements and how their connections develop during the run of a protocol. Moreover, using this logic the message trading schedules can be depicted with no uncertainty, clarifying clearly what suppositions are required and what data ought to be considered for the authentication of the members.

The detailed explanation of BAN logic is illustrated in the further section,

5.2.4.1 Burrows-Abadi-Needham (BAN) logic

BAN logic is rules for analyzing and characterizing the data exchange algorithms. In particular, this helps its users to determine whether the information exchanged is reliable, protected from listening, or both. Three main stages are involved for analyzing any protocol using BAN logic, they are:

1. Message appearance verification
2. Freshness verification
3. Reliability verification

To apply the BAN logic, the actions and messages of the participants are first transformed into formulas. Some basic BAN logic rules:

Meaning of the message: It allows the sender's identity of an encrypted message to be derived from the encryption key that is being used.

$$R1 = \frac{\left(A \left| \equiv \ B \overset{\beta}{\leftrightarrow} A, B \ \rhd \{D\}_{\beta}\right.\right)}{A \mid \equiv B \mid \sim d} \tag{5.1}$$

Where β is a shared key between B and A; so, if A receives any message encrypted with β, it must have originated from B, and A must ignore its own messages.

Freshness-verification: This rule allows the derivation of beliefs from freshly uttered messages.

$$R2 = \frac{\text{A} \mid\equiv \#(\text{d}), \text{A} \mid\equiv \text{B} \mid\sim \text{d}}{\text{A} \mid\equiv \text{B} \mid\equiv \text{d}} \tag{5.2}$$

If A believes that B once said D, then, A believes that B once believed D. If D is fresh, then, B should still hold this belief.

Jurisdiction rule: This rule allows belief based on jurisdiction to be derived. If A trusts B as an authority on D, then, A should believe D if B does so.

$$R3 = \frac{\text{A} \mid\equiv \text{B} \overset{\beta}{\Rightarrow} \text{d}, \text{A} \mid\equiv \text{B} \mid\equiv \text{d}}{\text{A} \mid\equiv \text{d}} \tag{5.3}$$

Authentication using KP-ABE algorithm,

The original message of the authentication phase is representing as follow:

MSG 1: $U_1 \rightarrow$ CSP$\triangleright$ U_1, U_2 from CSP

MSG 2: CSP $\rightarrow$ $U_2\triangleright$ {NU_2, # (PK, MSK), $\overset{\beta}{\rightarrow}$ CSP} β^{-1} from CSP

MSG 3: $U_2 \rightarrow$ CSP$\triangleright$ {NU_1, SK, V, AS, $\overset{\beta}{\rightarrow}$ CSP } β from U_2

MSG 4: CSP $\rightarrow U_1 \triangleright$ {NU_1 ,# (M), V , $\overset{\beta}{\rightarrow}$ CSP } β^{-1} from CSP

MSG 5: $U_2\triangleright$ {NU_1, C, AS, V, $\overset{\text{MSK}}{\longrightarrow}$ U_1 } MSK from U_1

MSG 6: $U_2 \rightarrow$ $U_1\triangleright$ {D, $\overset{\beta}{\rightarrow}$ U_1} $_{\text{SK}}$ from U_2

Apply Rules

MSG 2: $U_2\triangleright$ {NU_2, # (PK, MSK), $\overset{\beta}{\rightarrow}$ CSP} β^{-1} from CSP

$$R1 = \frac{U2 \mid\equiv \overset{\beta}{\rightarrow} CSP \, , U2 \triangleright \{ \text{N}U2 \, , \# \, (PK \, , MSK \,), \overset{\beta}{\rightarrow} U2 \} \beta^{-1}}{U2 \mid\equiv \text{C}SP \mid\sim \overset{\beta}{\rightarrow} CSP} \tag{5.4}$$

$$R2 = \frac{U2 \mid\equiv \#(\text{N}U1), U2 \mid\equiv \text{C}SP \mid\sim \overset{\beta}{\rightarrow} CSP}{U2 \mid\equiv \text{C}SP \mid\equiv \overset{\beta}{\rightarrow} CSP} \tag{5.5}$$

$$R3 = \frac{U2 \mid\equiv CSP \Rightarrow \overset{\beta}{\rightarrow} CSP, U2 \mid\equiv CSP \mid\equiv \overset{\beta}{\rightarrow} CSP}{U2 \mid\equiv \overset{\beta}{\rightarrow} CSP} \quad (5.6)$$

The result is:

$$U2 \mid\equiv CSP \mid \equiv \overset{\beta}{\rightarrow} CSP \quad (5.7)$$

$$U2 \mid \equiv \overset{\beta}{\rightarrow} CSP \quad (5.8)$$

MSG 3: CSP ⊳ {NU_1, SK, V, AS, $\overset{\beta}{\rightarrow}$ CSP } β from U_2

$$R1 = \frac{CSP \mid\equiv \overset{PK}{\longrightarrow} U2 \ , \left\{ NU1 \ , SK, V, AS, \overset{\beta}{\rightarrow} CSP \right\} SK}{CSP \mid\equiv U2 \mid\sim \overset{\beta}{\rightarrow} CSP} \quad (5.9)$$

$$R2 = \frac{CSP \mid\equiv \#(NU2), CSP \mid\equiv U2 \mid\sim \overset{\beta}{\rightarrow} CSP}{CSP \mid\equiv U2 \mid\equiv \overset{\beta}{\rightarrow} CSP} \quad (5.10)$$

$$R3 = \frac{CSP \mid\equiv U2 \Rightarrow \overset{\beta}{\rightarrow} CSP, CSP \mid\equiv U2 \mid\sim \overset{\beta}{\rightarrow} CSP}{CSP \mid\equiv \overset{\beta}{\rightarrow} CSP} \quad (5.11)$$

The result is:

$$CSP \mid\equiv U2 \mid \equiv \overset{\beta}{\rightarrow} CSP \quad (5.12)$$

$$CSP \mid \equiv \overset{\beta}{\rightarrow} CSP \quad (5.13)$$

MSG 4: U_1 ⊳ {NU_1 ,# (M), V , $\overset{\beta}{\rightarrow}$ CSP } β^{-1} from CSP

$$R1 = \frac{U1 \mid\equiv \overset{\beta}{\rightarrow} CSP, \quad U1 \rhd \{ NU1, \#(D), V \overset{\beta}{\rightarrow} CSP \} \beta^{-1}}{U1 \mid\equiv CSP \mid\sim \overset{\beta}{\rightarrow} CSP} \quad (5.14)$$

$$R2 = \frac{U1 \mid\equiv \#(NU1), U1 \mid\equiv CSP \mid \sim \overset{\beta}{\rightarrow} CSP}{U1 \mid\equiv CSP \mid\equiv \overset{\beta}{\rightarrow} CSP} \quad (5.15)$$

$$R3 = \frac{U1 \mid\equiv CSP \Rightarrow \overset{\beta}{\rightarrow} CSP, U1 \mid\equiv CSP \mid\equiv \overset{\beta}{\rightarrow} CSP}{U1 \equiv \overset{\beta}{\rightarrow} CSP} \quad (5.16)$$

The result is:

$$U1 \mid\equiv CSP \mid \equiv \overset{\beta}{\rightarrow} CSP \quad (5.17)$$

$$U1 \equiv \overset{\beta}{\rightarrow} CSP \tag{5.18}$$

MSG 5: $U_2 \triangleright \{NU_1, C, AS, V, \overset{MSK}{\longrightarrow} U_1\}$ MSK from U_1

$$R1 = \frac{U2 |\equiv \overset{MSK}{\longrightarrow} U1 , U2 \triangleright \{ NU1 , C \overset{MSK}{\longrightarrow} U1\} MSK}{U2 |\equiv U1| \sim \overset{MSK}{\longrightarrow} U1} \tag{5.19}$$

$$R2 = \frac{U2 |\equiv \#(NU1), U2 |\equiv U1| \sim \overset{MSK}{\longrightarrow} U1}{U2 |\equiv U1| \equiv \overset{MSK}{\longrightarrow} U1} \tag{5.20}$$

$$R3 = \frac{U2 |\equiv U1 \Rightarrow \overset{MSK}{\longrightarrow} U1 , U2 |\equiv U1| \equiv \overset{MSK}{\longrightarrow} U1}{U2| \equiv \overset{MSK}{\longrightarrow} U1} \tag{5.21}$$

The result is:

$$U2| \equiv U1| \equiv \overset{MSK}{\longrightarrow} U1 \tag{5.22}$$

$$U2| \equiv \overset{MSK}{\longrightarrow} U1 \tag{5.23}$$

MSG 6: U_2 □ $U_1 \triangleright \{D, \overset{MSK}{\longrightarrow} U_1\}_{SK}$ from U_2

$$R1 = \frac{U1| \equiv \overset{SK}{\longrightarrow} U2 , U1 \triangleright \left\{D, \overset{MSK}{\longrightarrow} U1\right\} SK}{U1 |\equiv U2| \sim \overset{MSK}{\longrightarrow} U1} \tag{5.24}$$

$$R2 = \frac{U1| \equiv \#(NU1), U1 |\equiv U2| \sim \overset{MSK}{\longrightarrow} U1}{U1 |\equiv U2| \equiv \overset{MSK}{\longrightarrow} U1} \tag{5.25}$$

$$R3 = \frac{U1 |\equiv U2 \Rightarrow \overset{SK}{\rightarrow} U2 , U1 |\equiv U2| \equiv \overset{MSK}{\longrightarrow} U1}{U1| \equiv \overset{MSK}{\longrightarrow} U1} \tag{5.26}$$

The result is:

$$U1 \mid \equiv U1| \equiv \overset{MSK}{\longrightarrow} U1 \tag{5.27}$$

$$U1| \equiv \overset{MSK}{\longrightarrow} U1 \tag{5.28}$$

From the results, it shows our authentication protocol is safe. Considering the above process the suggested method validates the privacy of KP-ABE algorithm. The exhibition of the recommended technique is tested and the effectiveness of the suggested method is compared with other methods in the below section.

5.3 Results and Discussion

In this section, the experimental outcomes attained from the proposed procedure are analyzed. Here, the implementation is done in MATLAB with a cloud simulator. The proposed strategies are analyzed with various parameters, for example, Execution time, Encryption and decryption time and validation accuracy. To build up a protected storage KP-ABE encryption algorithm is utilized in the proposed technique. The experimental outcome and the performance of the proposed strategy are given underneath in detail. At first, the client enlists their details in the cloud server. The new registration of the client appears in figure 5.2.

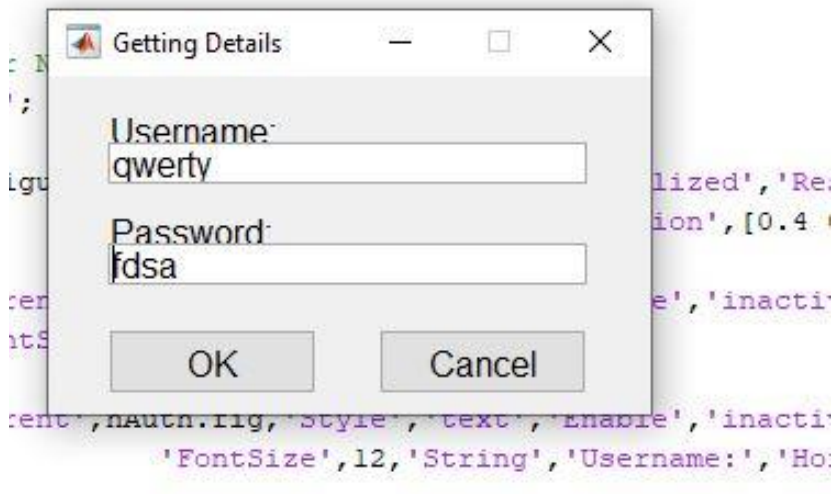

Figure 5.2: New registration details of the user

After completing the registration process, the user uploads the information to the cloud for authentication. Once the user authentication is verified, next the user uploads the data to the cloud. For secure storage, user data is encrypted before uploading the cloud with the help of KP-ABE encryption algorithm.

5.3.1 Performance analysis

The performance of the proposed method in terms of encryption and decryption time, execution time and validation accuracy are done. The main purpose of the proposed method is

to securely transact data. For binding purposes, multi-level authentication is used. This multilevel authentication is used to store data with a user password. The implemented method is examined based on the figure below,

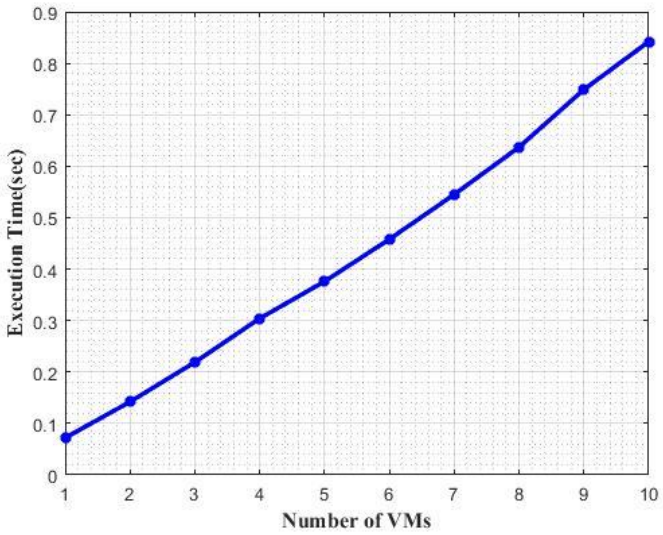

Figure 5.3: Performance-based on the execution time

When analyzing the above statistic, it shows the performance analysis of the implementation time by varying the number of virtual machines (VM). As the number of VMs increases, the overall execution time of the proposed method increases. The overall execution time of the proposed method is 0.434ms that is illustrated in Figure 5.3. The proposed methods of encryption and decryption time are shown in Figure 5.4 and Figure 5.5.

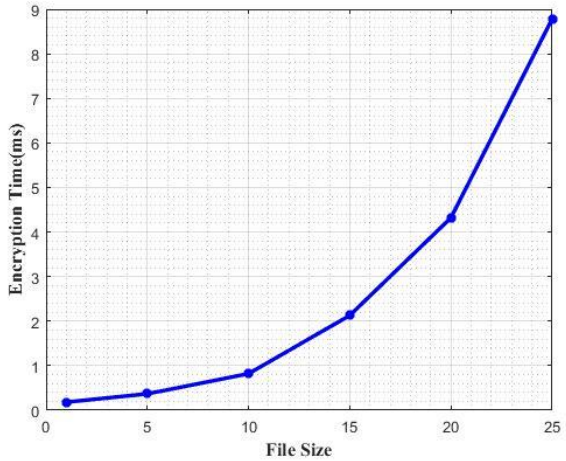

Figure 5.4: Performance of the proposed method based on the encryption time

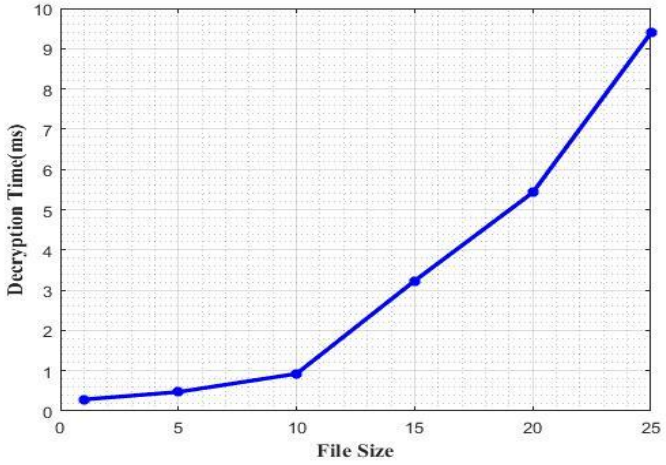

Figure 5.5: Performance of the proposed approach based on the decryption time

In the recommended method, to encrypt a 5kb file takes 0.368 milliseconds for encryption and 0.473 milliseconds for encryption. When changing the file size to 10kb, 15kb, 20kb and 25kb, the encryption time and decryption time also vary. Here the method takes 20kb file for encryption; it takes 4.321 milliseconds and 5.426 milliseconds for decrypting the same file size. After encryption, the recommended method ensures privacy with the help of BAN logic. The performance value of the proposed verification accuracy is shown in Figure 5.6.

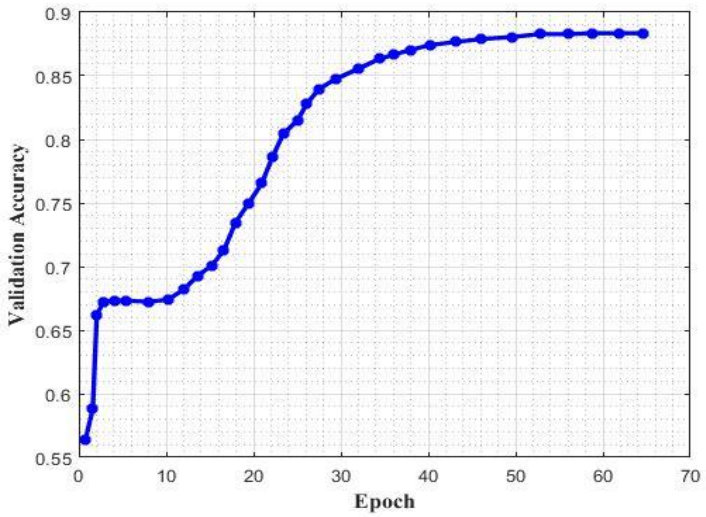

Figure 5.6: Performance of the proposed method based on the accuracy

As the number of epoch increases, privacy validation is also increasing. Here initially, epoch start with zero then the suggested method varies the number of epoch as 10, 20, and 30

up to 100 epochs. The proposed method of overall privacy validation is 88.35% of accuracy. The effectiveness of the proposed method is analysed and the results are compared in the further section.

5.3.2 Comparative analysis

With several existing strategies, the proposed technique is compared and the outcome is plotted beneath. Figure 5.7 shows the encryption time of the proposed strategy compared with the existing technique. In the existing method, the encryption is done by KP-ABE algorithm and the encryption is done by key policy scheme. The results are plotted in below,

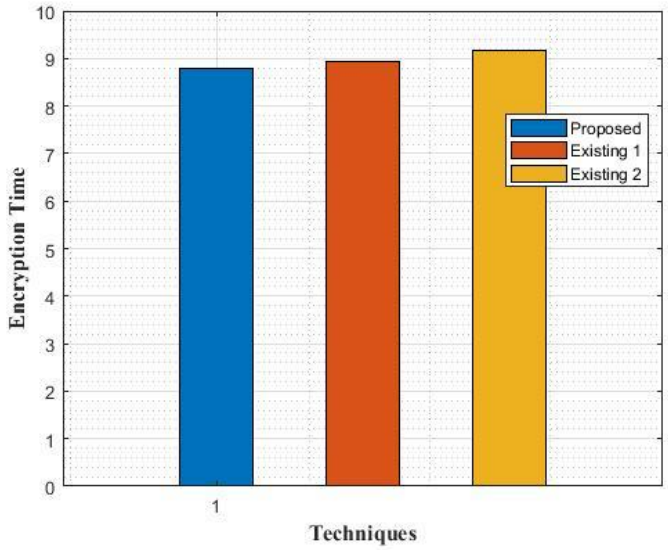

Figure 5.7: Comparative analysis based on the encryption time

From the above figure, it is explicit that the presented method consumes minimum encryption time compared to the existing methods. The overall encryption time of the proposed is 8.78ms, but the existing method 1 and 2 have an overall encryption time is 8.93ms and 9.15ms. The proposed comparison of validation accuracy is shown in figure 5.8.

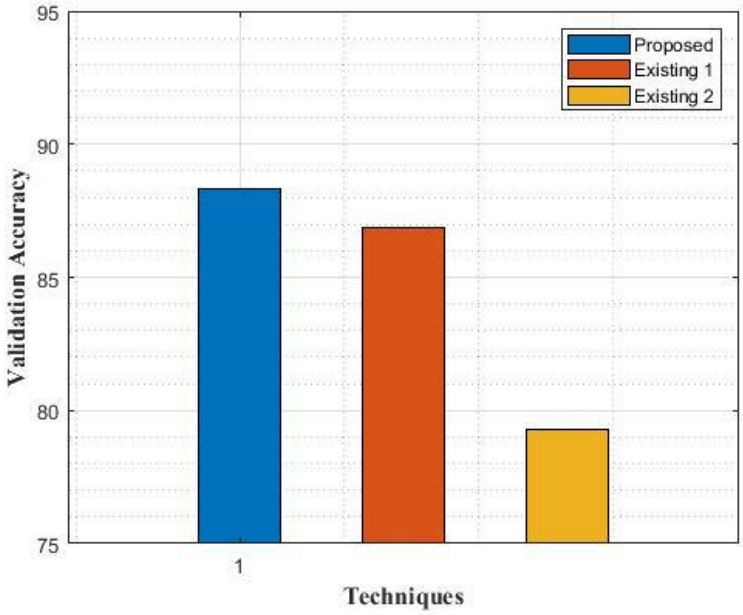

Figure 5.8: Comparative analysis of the encryption time

From the figure, it shows the proposed validation accuracy reaches the maximum value when compared to the exiting method 1 and 2. Here the suggested method achieves the validation accuracy is 88.35% but the existing method achieves the minimum validation accuracy value. This is because the proposed method uses BAN logic for verification so that only the proposed method achieves the maximum accuracy value.

CHAPTER VI

Secure Virtual Machine Allocation Using FTOPSIS-WOA Based Task Scheduling and Ant-Bee Colony Mechanisms

The content of this chapter is published in-

1. **Indian Journal of Science and Technology(IJST), vol. 13(35), pp. 3675-3684, 2020, ISSN 0974-5645. Web of Science Indexed**
2. **5th International Conference on Computing, Communication and Security (ICCCS-2020), IIT Patna, India. SCOPUS Indexed.**

CHAPTER VI

SECURE VIRTUAL MACHINE ALLOCATION USING FTOPSIS-WOA BASED TASK SCHEDULING AND ANT-BEE COLONY MECHANISM

6.1 Introduction

The components of Cloud computing are grid computing, distributed computing, autonomic computing and utility computing. The users of cloud computing don't have a clear idea where and in which part of the infrastructure the services are located. The services are used by the users through the cloud set-up and pay for the services. On-demand access is provided by the Cloud infrastructure for some shared resources and services. In literature lot of heuristic and metaheuristic algorithms are available in cloud resource management, for load balancing and task scheduling. An optimal solution can be attained using both types of algorithms. To find an optimal solution and to solve a problem more quickly the Heuristic algorithms are suggested. Still, to obtain the best solution they do not guarantee. Due to this reason, they are considered as assumption oriented and inaccurate algorithms. A search space is efficiently found in the Meta-heuristic algorithms to find the optimal solutions which are in proximity. Furthermore, the meta-heuristic algorithms when compared with heuristic algorithms have high time complication. Due to the reason, the iteration of the solution should reach the stop criteria or the maximum number of iterations. However, the main purpose to implement the metaheuristics algorithms is to augment the heuristic algorithms efficiency. The users of the cloud service provider use the pay per use model for gaining cloud resources.

In the cloud, at a present lot of applications that deliver effective resources to the end-user are deployed. Therefore, to reduce the resource access a large volume of users can access the same resource. To handle this problem certain load balancing and task scheduling algorithms have been established in a friendly manner [171-172]. To lessen the makespan, execution time, cost and transferring time the task scheduling is considered as a significant solution. For finding the best (task, VM) pair the computation time rises rapidly only when there is a rise in the number of VMs and the size of the task. A solution to scheduling is provided by some of the traditional strategies, like Round-Robin (RR), First Come First Served (FCFS), Shortest Job First (SJF), but the requirements of cloud computing may not satisfy with their performance. Evolutionary computational algorithms are a good selection for such computationally hard (NP-hard) problems because in a feasible time they can obtain ideal or near-optimal solutions. As the major parameter, the makespan is considered that is being scheduled in the VMs. Some of the few constraints such as resource utilization and cost are noted since both the consumers and the cloud providers must be gained with their requirements.

Cloud provides several services by means of the Pay per use-based services and they are software as a service, platform as a service, and infrastructure as a service. The delivered services could be measured and monitored using the quality of service (QoS). Currently, the cloud services are scheduled based on the resource availability without confirming the expected performances. To meet the QoS requirements of each cloud components, the cloud provider's ecosystem should be developed. The efficiency of resources in the CC environments have been enriched due to the Virtualization of resources and Containerization Platforms such as Dockers.

These strategies have been acknowledged by several heterogeneous service performances, such as MapReduce outlines, databases, web servers and multi-purpose virtual machines (VMs) on similar physical resources.

The performance and energy efficiency in CC environments depends on hardware qualities. Due to the suitable scheduling policies there is difference in the task completion time, this leads to very less energy consumption. The CC systems should ensure a proper security level for every task that are deployed on the system and the CC operators should be provided with tools to enhance the security backgrounds appropriate to their use cases. The cloud has been exposed to attacks from inside and outside due to its distributed nature, in this aspect the organizations are worried about their safety of the resources.

In the QoS, one of the parameters to be considered is prioritizing the customer tasks as their conditions are not confirmed by all the available VMs. Thus, the task of the customer comes under these two types, (i) high QoS task and (ii) low QoS task. In the first category mapping of the tasks is done, while in the second category all the tasks can be mapped to the VMs that are available. Hence, more priority is found in a high QoS task. The load balancing algorithms have been presented by many researchers for task distribution. Though, the QoS parameters have not been considered in their algorithms. In this study FUZZY with TOPSIS (FTOPSIS) is combined to solve the task scheduling problems. TOPSIS is mainly used to find the best solutions for local optimum [143]. A Whale optimization algorithm (WOA) is used to deal with constrain in the load balancing which improves the whole cloud computing systems performance because of the consumers and the cloud providers [151].

The cost for communication in cloud databases, can be minimized when effective access techniques along with storage facilities are used for storing and data retrieval. In network communication the main challenge is the security. In the literature studied related with cloud security, scheduling, data storage and energy-related problems has been examined and the solutions for them are proposed. Using an optimization principle a job can be complete in very less expense, time and security when the user stipulates a deadline or budget description.

Thus, the designed scheduling algorithm must map jobs on resources because of the constraints and the optimization criteria identified by the user and the cloud service providers.

The user guarantees the performance when submitting a job which is treated with a type of agreement known as SLA. The user achieves minimum time when more cost is expended. So, for minimizing the time and cost an approach this chapter presents FABC algorithm which enforces the security features and satisfies the QoS during the scheduling.

6.2 Scheduling and Load Balancing Strategies

The main task of the scheduler is to pick the suitable VM and based on the intended algorithm tasks are allotted to the VM. Figure 6.1 depicts the block representation of scheduling and load balancing strategies.

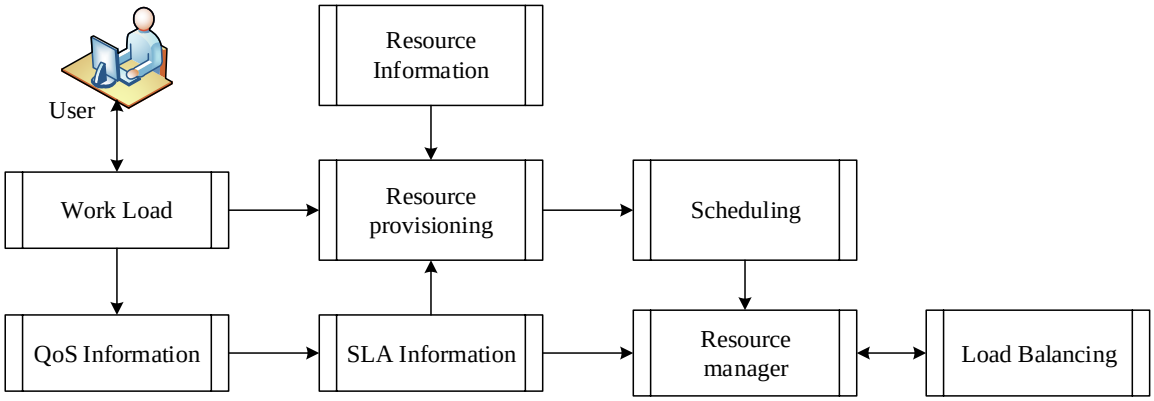

Figure 6.1: Block diagram for the strategy used for Scheduling and load balancing.

The scheduler allocates the time arrival jobs in proper VMs which are least utilized. The load balancer chooses the task migration from the VM's which are heavily loaded to a least loaded VM or an idle VM at run time when a least loaded VM or an idle VM is found. Communication with the VMs resource probe is undertaken by the Resource monitor which collects each VM's current load, the VM capabilities along with the overall jobs in the waiting/execution queue. The user provides the task requirement which contains the dimension

of tasks which is to be transfers and executed.

6.3 TOPSIS–FUZZY Based Task Scheduling Algorithm

In the real world, the multiple criteria decision-making (MCDM) complexions are effectively handled using the TOPSIS technique. In this study, TOPSIS is extended to the fuzzy environment to propose the fuzzy TOPSIS (FTOPSIS) algorithm to do scheduling effectively based on the size of the task, request priority and optimal distance between the server and the client nodes. The proposed algorithm on behalf of multiple criteria helps to achieve an optimal solution without a rise in time consumption. There is a set of PM's in the system model to be considered ie $PM = (PM_1, PM_2, \quad P_{MM})$ in which each PM holds some $VMs = (VM_1, VM_2, \quad VM_j)$. To each VM certain numbers of tasks are assigned to perform the execution process. In a parallel and independent manner, every VM runs on its own resources. The Scheduling algorithm of the FTOPSIS method is presented below:

Step 1: Develop an expert committee for evaluation.

Step 2: Find the criteria for evaluation.

Step 3: Pick up the suitable linguistic variables for evaluation.

Step 4: Find the weight of the alternative related to each condition.

$\tilde{P}_k = (d_k, e_k, f_k), k = 1,2,3, \quad K,$ the Fuzzy rating is found subsequently $P = (d, e, f), k = 1,2,3, \quad K.$ Here $a = \min_k (d_k), e = \frac{1}{k}\sum_{k=1}^{K} e_k, = \max_k (f_k)$

Step 5: Create the Fuzzy matrix and normalise it.

For normalization, linear-scale transformation is applied and $\tilde{P}$ is obtained.

$$\tilde{P} = \left[r_{ij}\right]_{m \times n} \quad \text{i} = 1,2,3, \quad \text{m}; \quad \text{j} = 1,2,3, \quad ,\text{n} \qquad (6.1)$$

In which $\tilde{r}_{ij} = \left(\frac{d_{ij}^{*}}{fj}, \frac{e_{ij}^{*}}{fj}, \frac{f_{ij}}{fj} \right)$ and $F_j^* = \max_i F_{ij}$

Step 6: Create a normalized weighted Fuzzy matrix. Considering the weight of each criterion, for computing the weighted decision matrix which is normalized and is denoted as Y.

$$\tilde{Y} = \left[\tilde{Y}_{ij} \right]_{m \times n} \tag{6.2}$$

$\tilde{y}_{ij} = \tilde{r}_{ij} w$ is the weighted vector of the evaluating criteria which is represented as 'w'

Step 7: Find the Fuzzy negative ideal solution (FNIS) and Fuzzy positive ideal solution (FPIS).

$$FPIS(P^-) = \left(\tilde{Y}_1^-, \tilde{Y}_2^-, \tilde{Y}_3^-, \quad , \tilde{Y}_n^- \right) \text{ \& } FPIS(P*) = \left(\tilde{Y}_1^*, \tilde{Y}_2^*, \tilde{Y}_3^*, \quad , \tilde{Y}_n^* \right) \tag{6.3}$$

Where $\tilde{Y}_j^- = \min_i \left\{ y_{ijk} \right\} \& \tilde{Y}_j^* = \max_i \left\{ y_{ijk} \right\}$.

Step 8: Compute the alternative distance from FNIS and FPIS as

$$D_i^- = \sum_{j=1}^{n} D_v \left(\tilde{y}_{ij} . y_j^- \right); \text{ i} = 1,2,3,...\text{m and } D_i^* = \sum_{j=1}^{n} D_y \left(\tilde{y}_{ij} y_j^* \right); \text{ i=1,2,3,….,m} \tag{6.4}$$

The distance measurement between two Fuzzy numbers is represented as D_v.

Step 9: The closeness coefficient (Ce_i) is evaluated. For each alternative, the closeness coefficient is found.

$$Ce_i = \frac{D_i^-}{D_i^- + D_i^*} \tag{6.5}$$

Step 11: Based on the closeness coefficient rank the alternatives.

The ranking of the alternatives according to the closeness coefficient can be fixed.

6.4 Load Balancing Algorithm

One of the vital aspects of task scheduling problems is Load balancing. In this process, the workload among multiple servers is dispersed in a way that the entire resources are used efficiently to attain the optimal throughput and response time. A suitable load balancing

algorithm can (1) enhance the VMs efficiency (2) avoid overload and (3) decrease the request waiting time. For allocating the tasks optimally to the VMs and accomplishing load balancing the whale optimization algorithm (WOA) is described. The WOA initiates with the set of solutions. The current solution is considered as the optimal solution and on behalf of the current solution, the process is executed.

Till attaining the best solution this process is continued.

Step 1: Initialization

The search agent's population is initialized in this phase. Let $S_j (j = 1,2,....,k)$ be the initial population and S_j be the optimal search agent.

Step 2: Prey encircling

The position of the prey is realized by the humpback whales and surrounding them immediately. Later it confirms that best prey is the current solution and the position of the search agents are updated according to the current best agent's position.

Which is signified subsequently

$$A = \left| T.S^*(x) - S(x) \right| \tag{6.6}$$

The current iteration is represented as *X*, the position vector is represented as S and the best solution position vector is represented as S^*. The coefficient vector is denoted as T.

The current best search agent's position is represented in Eq. (6.6).

The Eq. (6.7) calculates the new position.

$$S(X+1) = S^*(X) - N.A \tag{6.7}$$

The coefficient vector is denoted as N.

Eqs. (6.8) and (6.9) calculates N and T are calculated by the

$$\overline{N} = 2n.o - n \tag{6.8}$$

$$T = 2.o \tag{6.9}$$

Where, the n value lessened from 2 to 0 and the random vector in [0, 1] is denoted as o.

The best search agents surrounding places are visited after modifying the value of N and T.

Step 3: Exploitation phase

There are two levels in this phase, (1) shrinking encircling process, (2) Spiral updating position.

The N value is set to [−1, 1] in shrinking encircling process. The agents' new position is denoted by the initial position of the agent and the agent's current optimal position.

By the following equation the spiral can be updated in the spiral updating position.

$$S(X+1) = A'.h^{st}.\cos(2\pi t) + S^*(X) \tag{6.10}$$

Where, *t* is the value in [-1, 1] and *s* is the constant. Using Eqn (6.10) A' is calculated,

$$A' = \left| S^*(X) - S(X) \right| \tag{6.11}$$

Where, the position vector is represented as S and the best solutions position vector is represented as S^*

Then, the search agent's position can be updated amid by the spiral position or the encircling process.

$$S(X+1) = \begin{cases} S^*(X) - N.A & ;\text{if a} < 0.5 \\ A' h^{st}.\cos(2\pi t) + S^* & ;\text{if a} \geq 0.5 \end{cases} \tag{6.12}$$

Where, *a* is the random number in the range [-1, 1].

Step 4: Exploration phase

This phase updates the search agents position as below.

$$A = \left| T.\ \vec{S}_{rand} - S \right| \tag{6.13}$$

$$S(X+1) = \vec{S}_{rand} - N.A \tag{6.14}$$

The random position vector is denoted as $\vec{S}_{rand}$.

Step 5: Termination

Beyond the search region if the search agents are found then set $X = X + 1$ and update S^*. This load balancing is based on the WOA. Initially the search agent's population is set. The optimal agent is made ready, position is updated by other search agents. The search agent position is updated by the Eqn 6.10. The search agent's positions are updated by Eq. (6.7) if the probability value is less than 0.5. Until reaching the optimal solution this process is repeated.

6.5 Methodology for Security and Resource Optimization Using Fuzzy Ant Bee Colony

6.5.1 Problem Formulation

Guaranteed performance is expected from the cloud when a job is submitted by the user. The requirements of the users are submitted as SLA. Once the job is submitted the SLA agreement is contracted between the provider and the customer. Two types of users are satisfied by the scheduling issues: cloud service provider and cloud consumer. The problem related to varying size and complexity can be solved by executing the job of cloud users. Their job is required to be accomplished with minimum response time, improved scalability, cost-efficient optimal scheduling with high security. For the execution of the consumer job, a contribution is made by the cloud provider in providing resources. The main requirement is to enlarge the return on investment, load balancing and resource usage. A new algorithm has to be proposed to find an optimal solution which provides an apt tradeoff. Since a solution cannot be attained in a polynomial time. The number of users at the same time in a cloud computing environment needs resources, scheduling method should provide resources in less time to avoid delay. Algorithms of dynamic data heuristic features are used to fulfil the cloud environments nature. Real-time problems are solved using swam intelligence and nature-inspired algorithms moreover an

optimal solution in a polynomial-time interval is attained. These type of algorithms are ant colony optimization (ACO), particle swarm optimization (PSO), artificial bee colony (ABC), genetic algorithm and cuckoo search algorithm [171-176].

6.5.2 Hybrid Fuzzy-ABC (Ant Bee Colony) for Cloud Scheduling and Security

A hybrid Fuzzy-ABC is proposed in this work for VM scheduling and security that promises an active cloud service. The fuzzy module proposed estimates the historical data to compute the pheromone value and choose a proper server while maintaining the best computing time. The proposed algorithm is applied to describe high-performance applications based on effective cloud architecture.

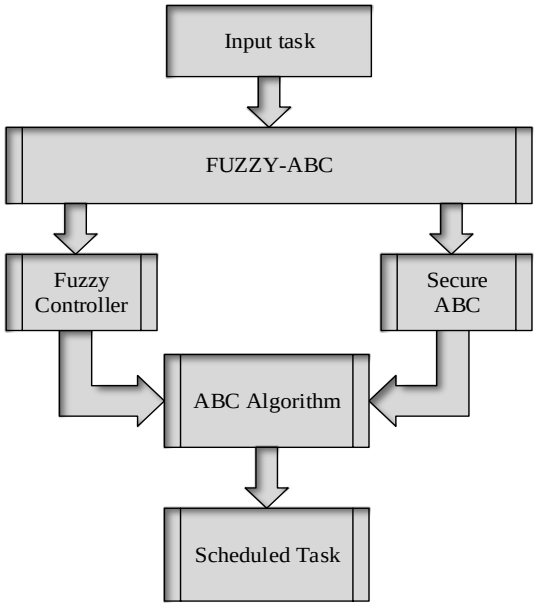

Figure 6.2: proposed Block diagram

Moreover, an important need is to ensure QoS during job scheduling to the user. In the boundary of the third party, the scheduling process takes place therefore ensuring its security is an essential criterion. The intension of the proposed work is to offer QoS without violating SLA. The block wise representation of the proposed method is illustrated in Figure 6.2.

These objectives are achieved using the proposed algorithm. The Experimental outcomes

confirm that the objectives of secure job scheduling with assured QoS are achieved by the proposed system.

6.5.3 Fuzzy ABC scheduling and Resource allocation

In the cloud system, the improved ABC algorithm is used to solve the scheduling problem. The data and the pheromone formulation should be identified before implementing the ABC algorithm. The pheromone in our case permits the evaluation of a selected server's adaptableness to obtain a VM based on its cost, heuristic details and technical capacity. After each positive assignment of a VM to a server, the heuristic part is updated. The proposed algorithm minimizes the computational time by switching the pheromone value estimation by the fuzzy evaluation. The fuzzy controller takes charge of the pheromone calculation and receives as inputs the values of storage, memory, bandwidth and CPU. In this methodology, the pheromone value is displayed as output that can be eminent and using the evaporation ratio they are updated. This process is reiterated by the algorithm until the end and the optimal solution is attained. Two significant steps are available in the proposed algorithm. In the first step, the local solution that matches to an optimal allocation of the VM is identified. The pheromones matrix is updated in the second step which corresponds to updating the servers which are accessible and the unavailable servers are avoided. The pheromones matrix and the probability values are updated by the bees after each iteration. Randomly the bees are distributed at the beginning of the algorithm. The probabilistic function is applied by the bees after each step to select the next location. The probability for a bee located in the nodes' required to be moved to node 'd' is prepared based on the equation below:

$$P^k(A,B) = \frac{[\tau(A,B)\ ]^\alpha [\eta(A,B)]^\beta [\mu(A,B)]^\gamma}{\sum_k [\tau(A,B)]^\alpha [\eta(A,B)]^\beta [\mu(A,B)]^\gamma} \quad (6.15)$$

The pheromone value calculated using the fuzzy module is represented as τ(A,B),

μ(A,B)=1⁄totalCloudlets, η(A,B)=1⁄total cost, pheromones influence factor is denoted as α, the influence factor of cost is denoted as β, and the queue of user request influence factor is denoted as γ .

Algorithm 1

Input: VM, Hosts, Cloudlet lists, datacenters and Set of Pheromone values.

Output: Optimum Task Resources

Step 1: Prepare the pheromone table, number of VM with its cost, time and security features.

Step 2: Assign the execution time for a task after confirming if it is a parallel task or deprived of a parent task.

Step 3: Prepare the VM parameter to contain the hive table.

Step 4: Calculate the task length and the load based on the number of tasks allocated to the VM.

Step 5: Assign the task which has the parent task and calculate the tasks end time and the processing time.

Step 6: Else follow the same calculations and assign it to the optimal VM.

Step 7: Perform the security mechanism when the security level value is low.

Step 8: In the end generate the Job Schedule.

6.5.4 Secured ABC for cloud

The main challenge in a CC environment is security. Security services are applied necessarily to safeguard the application of users which are existing in a cloud domain to overcome the problem of phishing and eavesdropping. The tasks at the execution time are covered with the threat in the cloud domain. Three vital attacks in the cloud are snooping, spoofing and alteration. Some of the security measures are provided to deal with these attacks i. e. integrity, confidentiality and authenticate measures. The security requirement of the cloud

users are specified with three tuples $sd_i = \{sd_i^1, sd_i^2, sd_i^3\}$ of their task and the security services are applied based on that.

For the task t_i, the offered security services are represented by the set $sl_i = \{sl_i^1, sl_i^2, sl_i^3\}$. The level of l[st] security solution provided to the task t_i is represented by sl_i. Each algorithms security level is assigned with a range varying from 0.08 to 1. Level 1 Security is treated as potent. Overheads to the existing system are initiated by the security solutions, which are based on the service level and size of data. Eqn. 6.16 is used for calculating the security overhead of confidentiality and integrity.

$$SO(t_i) = \sum_{lv \in \{auth, inter, conf\}} SO^{lv}(t_i) \quad , \text{lv} \in \{\text{auth, inter, conf}\} \tag{6.16}$$

The security requirement level is denoted as where sd_i^{lv} and the protected data d_i^{lv} of task t_i. The entire security overhead can be computed as

$$SO(t_i) = \sum_{lv \in \{auth, inter, conf\}} SO^{lv}(t_i) \tag{6.17}$$

The required security level is selected by the cloud user for execution.

To compute the risk rate the workflow should be analyzed. The risk rate analysis is done by the Poisson probability distribution.

An exponential distribution is used to find the tasks risk probability with lst security service.

$$RR(t_i, sl_i^l) = 1 - e(-(sd_l^{lv}, sl_i^{lv})) \tag{6.18}$$

Negative exponent denotes the failure probability and the difference of increase are represented as (sd_l^{lv}, sl_i^{lv}). In the workflow, the set of tasks is denoted as 'T'. The entire workflows risk probability is found below

$$RR(T) = 1 - \prod_{t_i \in T} (1 - RR(t_i)) \tag{6.19}$$

In the CC environment the security level of the user application is ensured. T is set of task T =

{t1, t2,…,tm} of user Job. For each task a set of leased VM is represented as V = {v1, v2, v3...vn}, where vi is of three tuples vi = { $VM_s^y(t_i)$, l_{st} ($t_{i,}VM_s^y$), L_{et} ($t_{i,}VM_s^y$)}. The VM type used for the task t_i is denoted as $VM_s^y(t_i)$ having leased end time ($t_{i,}VM_s^y$) and leased staring time l_{st}($t_{i,}VM_s^y$). A security level is needed by every task. SL = {sli, where i=1.2….n} is chosen. The total execution cost and time are computed below

$$EXCE(t) = \max\{ET(t_i), t_i \in T\} \tag{6.20}$$

$$EXC(c) = \sum_{i=1}^{n} C_s^y[l_{st}(t_i VM_s^y) - l_{et}(t_i, VM_s^y)] \tag{6.21}$$

Thus the proposed work performs scheduling with very less time and costs.

6.6 Results and Evaluations

In this section, the CloudSim framework is used to evaluate the performance of the proposed algorithm. Also the performance evaluation of the proposed Fuzzy -ABC algorithm is conducted. The tasks are submitted by the Cloud user which can be a dependent workflow schedule or an independent task. The intension of the simulation is to provide QoS and security-aware job scheduling. The performance evaluation is done based on certain parameters e.g. makespan, execution time, waiting for time, cost and degree of imbalance. For comparison, some of the well-known algorithms are used. Small, medium and large are the types of task distributions used i.e. 200, 400, 600, 800, and 1000. Table 6.1 presents the parameters for the experiment setup.

Table 6.1: Simulation metrics

No of tasks	1000
No of VMs	100
MIPS	1000-2000ms

Bandwidth	500-1200kbps
Number of PMs	1-5
Cost per VM	1$

In Figure 6.3, variation in makespan is displayed. And when compared with the existing algorithms the proposed algorithm is found better in makespan.

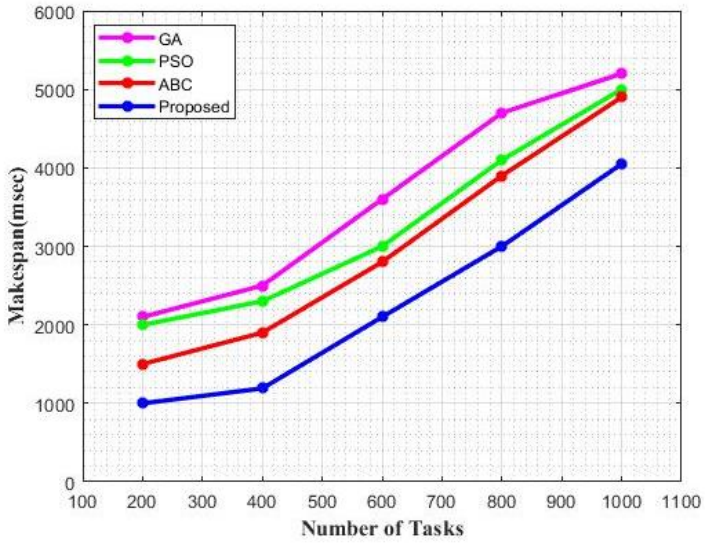

Figure 6.3: Makespan

The overall performance is affected due to the Computational cost. The experimental probe of the involved operational cost is presented in Figure 6.4 and when compared with the other algorithms our proposed has very less computational cost. All suitable providers who strive to win submit the bids, resources at a less possible or the best price are offered by the providers. The customers provide the resources at the right market price are somewhat high. Thus, to reduce the procurement cost the reverse auction is induced. The results exposed that when the sum of tasks are set to be 200 the proposed attains minimum cost than the existing algorithms. When the no. of tasks are increased a slight improvement is seen in cost minimization. The proposed approach shows an average enhancement when no of tasks reaches

to 1000.

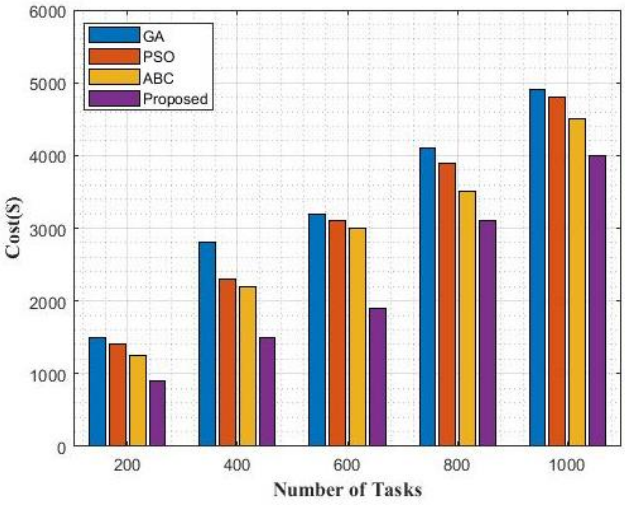

Figure 6.4: Operational cost

The resource utilization of the method implemented is presented in Figure 6.5. The algorithm proposed offers better developments in resource utilization than the existing methods.

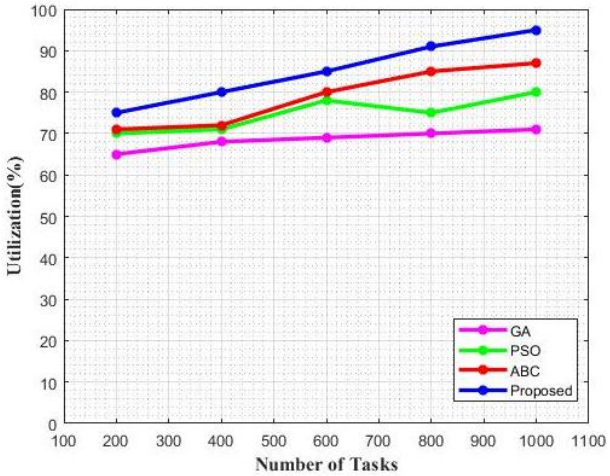

Figure 6.5: Resource utilization

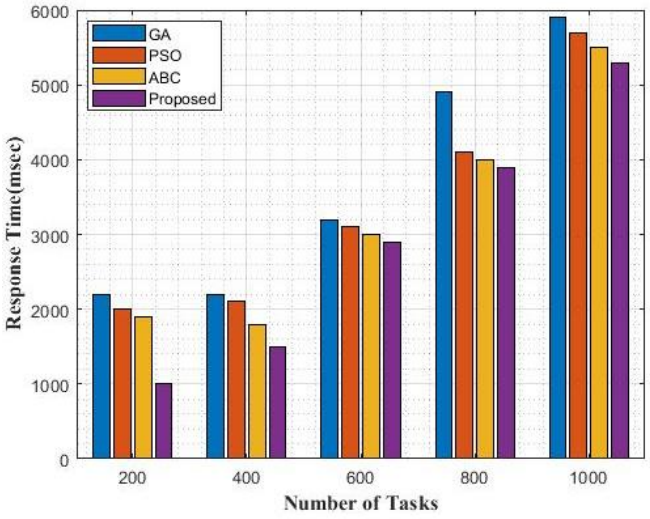

Figure 6.6: Average Response Time

The average response time of the proposed approach is shown in Figure 6.6. It is specified that when the no of a task is increased there is much enhancement in reducing the response times. There is a substantial improvement when compared with the existing algorithms.

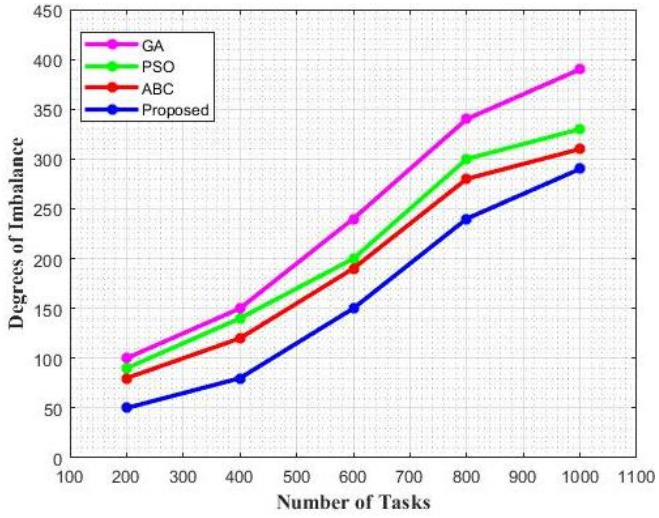

Figure 6.7: Degree of Imbalance

The degrees of imbalance is analysed in Figure 6.7. In cloud resources when the user tasks are scheduled there is a chance for the VM to get overloaded. A load of VMs can be evaluated using the degree of imbalance metric. The graph in the above figure confirms that

the proposed algorithm yields a nominal degree imbalance when validated with other approaches. The proposed approach provides very less degree of imbalance when the number of tasks are increased due to this there is a uniform distribution of the tasks which doesn't affect the performance of the resource.

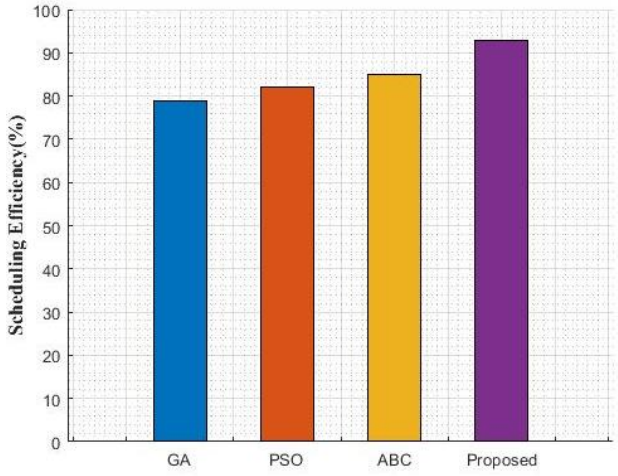

Figure 6.8: Scheduling efficiency

In figure 6.8 it's clear that there is a progress in the effectiveness of the proposed compared with the existing algorithms. Superior cost optimization is achieved by the proposed method, this is considered as an advantage for the consumer who utilizes the cloud services.

Figure 6.9 displays the execution time comparison of the proposed approach with other algorithms.

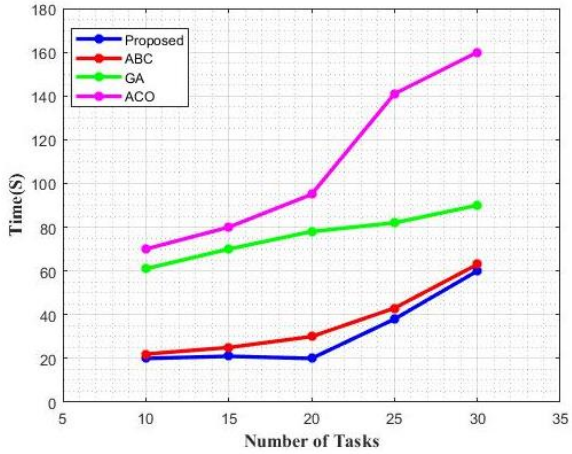

Figure 6.9: Comparison of execution time

Compared to other metaheuristic algorithms the proposed algorithm has a minimum execution time. The search time is reduced since the task allocation is conducted through the information of the hive table. Optimal VM is gained by the task. This the main reason for the variation in the execution time. Figure 6.10 displays the comparison of cost made with the existing algorithms.

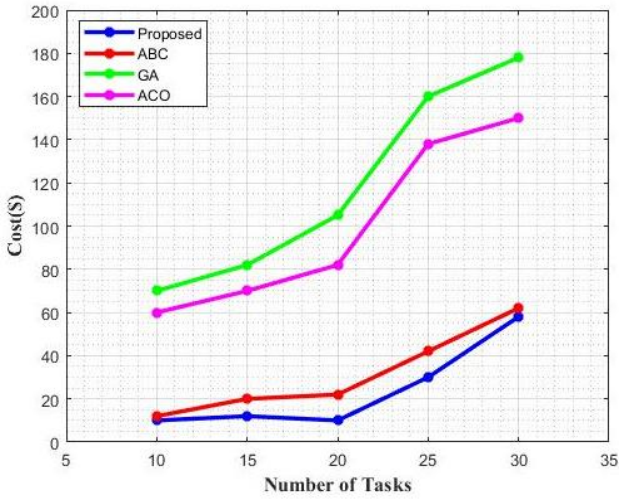

Figure 6.10: Comparison of cost

The requirement of the user is considered during the task allocation and the task is allocated to the optimal VM and due to the proposed algorithm, there is an amendment in cost.

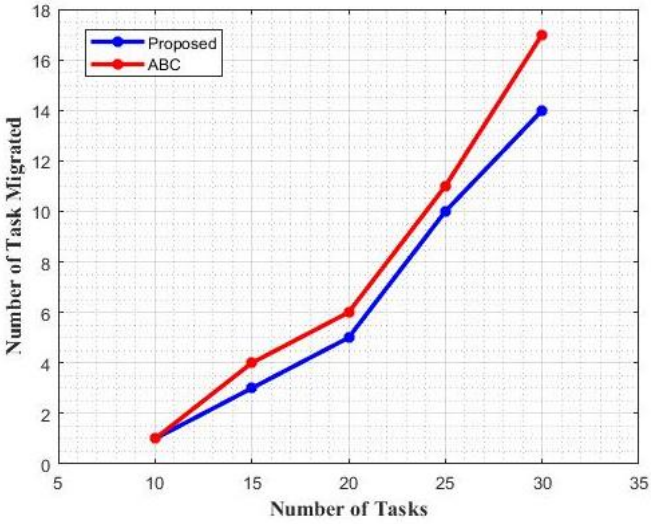

Figure 6.11: Number of task migration

The number of task migration is displayed in Figure 6.11. The proposed algorithm examines each VM load before allocating the task to a certain VM. Due to this allocation, a balanced state is offered in every VMs in the data center this certainly minimizes the task migration. Figure 6.12 displays the cost for execution in several risk rate conditions.

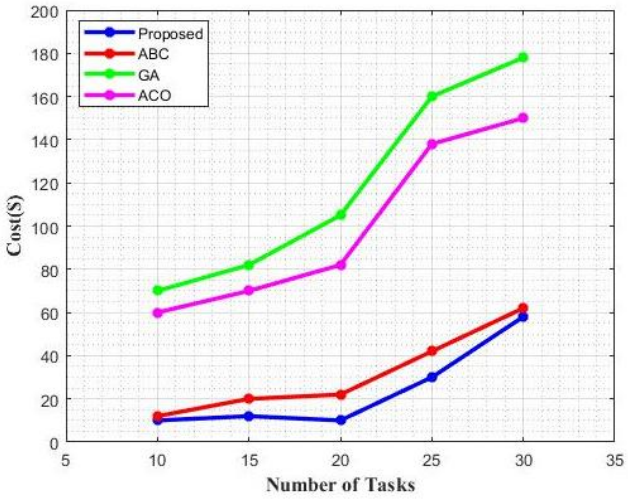

Figure 6.12: Cost execution in several risk rate constraints

There is an increase in the risk rate from 0.1 to 1 with a rise of 0.1. When there is a higher risk rate the security services should be an advanced one. The data is safeguarded by the security services and prevent them from modifying and accessing unlawfully. When compared with the proposed algorithm the execution cost of other approaches are excessive. In contrast, if a user utilizes improved security services the processing time will be elongated. Moreover, this will affect the cost and makespan. Hence in the Job execution, a proper tradeoff should be followed by the users between cost and security. The experimental outcome exposed that the proposed algorithm outperforms the existing algorithm and assures QoS and security to the cloud users without violating the SLA.

CHAPTER VII

Minimum Energy Utilization through Spider Monkey Optimization Technique

The content of this chapter is published in-

1. **Walailak Journal of Science and Technology, ISSN: 2228-835X. SCOPUS Indexed. (Communicated)**
2. **Book Chapter of Blockchain for 6G-Enabled Network-based Applications: A Vision, Architectural Elements, and Future Directions, Springer Nature, SCOPUS Indexed (Accepted)**

CHAPTER VII

MINIMUM ENERGY UTILIZATION THROUGH SPIDER MONKEY OPTIMIZATION TECHNIQUE

7.1 Introduction

Globally, Cloud computing is a trending technology, where its providers concentrate on the internet storage, 'pay-as-you-go' and elastic provisioning model to support the requests of customers. This technology concentrated on providing massive data centers as well as reducing greenhouse emissions by lowering the maintenance cost of IT infrastructure. This definition highlights the fact where modern IT sector needs opportunities to expand resources progressively and increase capacity, thus reducing the need for time and resources to buy additional Infrastructure. In cloud computing, the key feature is multi-level capabilities that allow a vast pool of clients to share resources and costs. Also, alternative techniques for resource allocation are desirable because they have advanced architectural features. In this context, it is essential to determine the best scheduling procedure for each data management. Resource management contributed to provision, distribution, and schedules in cloud computing. The main contributors to the conjunction of cloud computing are its scientific workflows. Significant monetary costs may also lead to possible drawbacks, for example, inabilities to satisfy workflow demands based on time or pick the incorrect resource for a job. The availability of the appropriate storage and calculation tools results in a decisive cost reduction, with no significant effect on the efficiency of applications.

Now a days, the resource allocation approaches are based on a decision tree model, dynamic sliding window, support vector machine and so on. In the resource allocation process uses the networks computing resources to enable the execution of the complex tasks which needs a significant computation. Many factors are considered for resource allocation i.e.

Makespan, load balancing and energy consumption [63-64]. In the cloud, the main thing to consider is picking the resource nodes which are favorable to execute a task and based on the properties of the task they have to be selected properly. Especially, the allocation of cloud resources is done to satisfy the user-specified (QoS) requirements via service level agreements (SLAs) and also to minimize the energy depletion [68].

When compared to a traditional cloud computing infrastructure the blockchain cloud is thin. In the year 2008, the Blockchain was developed mainly for the Bitcoin cryptocurrency to facilitate a payment system. This system allows distrusted personals to form a stable, transparent and constant record of exchange and managing deprived of any central authority [156]. There are certain layers in the blockchain system such as a network layer, data layer, incentive layer, consensus layer, application layer and contract layer. The data blocks are constructed by the data layer. Distributed peer-to-peer networks are present in the network layer for communication and data verification among the nodes. The incentive approach is developed by the incentive layer. Scripts or algorithms are used by the contract layer to formulate smart contracts. Based on several application scenarios of blockchain technology the application layer is constructed. Relevant studies have been carried out on the combination of blockchain technology with cloud computing, edge computing and fog computing. Includes studies combining with the access control technology, Internet of Things (IoT), and other relevant fields.

As a consequence, cloud resource management is the focus of extensive and up-to-date attention. Several algorithms for cloud computing techniques are implemented for resource allocation. The algorithm for the resource optimization technique was proposed in this study is a spider monkey algorithm. The development of new techniques for optimizing Internet infrastructure at all rates is essential to tackle rising energy usage, increasing operating costs, and carbon emissions. This research, therefore, involves the GCSM approach for optimizing

energy along with the SMO technique. This chapter offers a blockchain-based resource management framework and an optimized resource allocation strategy using SMO algorithm based on energy consumption and makespan optimization models in the cloud domain. The SMO is a novel evolutionary algorithm based on the spider monkeys foraging behavior. It is a perfect approach for the optimization of benchmark functions and antenna design complications. The use of SMO in this study successfully optimizes resource allocation when evaluated with the prevailing resource allocation algorithms. In addition to this, the energy depletion of the resources is minimized by applying a Brownout based Energy model. The simulation outcomes expose that the proposed approach has the enormous ability as it bids high ability for the enhancement of energy efficiency and substantial cost savings which can satisfy the customers SLA requests.

7.2 Proposed Research Approach for Attaining an Optimized Resource Allocation

Though numerous advantages are offered by the cloud in technical, operational and economical viewpoint. There is an improvement needed for efficiently allocating the resource for data centers. In this study, the proposed approach highlights the vital complications encountered by the providers of cloud infrastructure. The resource management is mainly done using a blockchain-based framework. The main intention to adopt this framework is to save the expense on energy by the scheduler which is continuing in the existing models. For effective resource management, some of the factors taken for consideration are Service Level Agreement dynamic resource demand pattern and resource utilization. The main objective is to effectively allocate the resources to minimize makespan to achieve an energy-efficient schedule. In many decision-making problems and real-world design involves real-time optimization of multiple objectives. In our work, we designed an optimization model for a resource allocation that will fully incorporate the two factors of energy-efficient and makespan optimization. The SMO is

used to optimize resource allocation based on makespan optimization and a Brown out based energy model is adopted to reduce the reduce energy and carbon footprint.

The proposed algorithm in this investigation is SMO which is recognized as metaheuristic methods based on the social behaviour of spider monkey which implements the swarm intelligence method for foraging based on fission and fusion. Swarm is the living place of the spider monkeys and they comprise of 40-50 members. In a region, the leader decides to divide the strategy for food searching. Female leads create mutable small clusters and are the leads of the swarm. The cluster size is depending on the availability of food sources as well as the region.

The essential criteria of the SMO algorithm are swarm intelligence (SI), and it should comprise labour division and self-organization. The foraging works are divided by the Spider monkeys Labour division by creating smaller groups. To meet food availability principle of Self-organization is followed. The Swarm intelligence concept is described in figure 7.1. Thus, an SMO-based algorithm divides into a normal, swarm intelligence-based algorithm

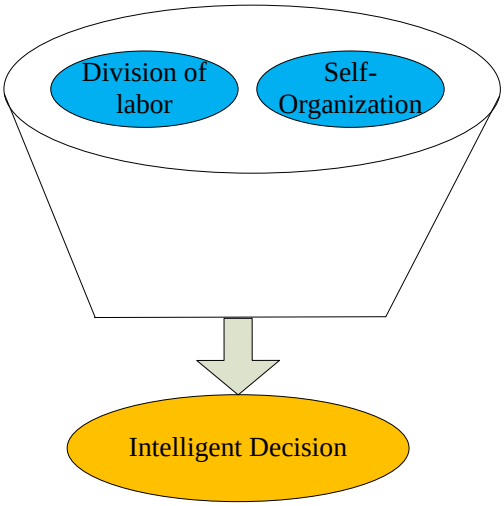

Figure 7.1: Swarm intelligence concept

7.2.1 Spider Monkey Optimization Process

The observations and intentions of spider monkeys are identified by the positions and posture at long distances. By particular sounds such as chattering or whooping, they interact with each other. Every monkey has its unique noticeable sound by which that monkey is identified by other group members. Figure 7.2 depicts the spider monkeys foraging behaviour.

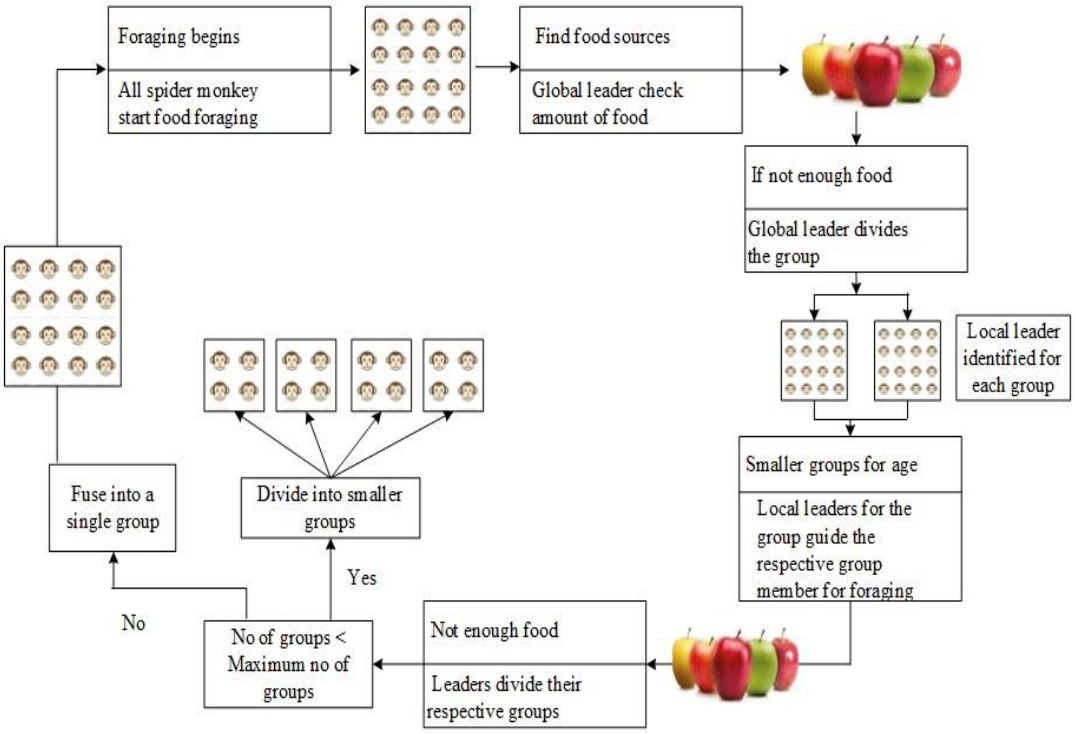

Figure 7.2: Foraging behaviour of spider monkeys

This algorithm is recognized as a metaheuristic method, and the concept of this algorithm is the social behaviour of spider monkey which implements the swarm intelligence method for foraging based on fission and fusion. Swarm is the living place of the spider monkeys and they comprise of 40 -50 members. In a region, the leader decides to divide the strategy for food searching. Female leads create mutable small clusters and are the leads of the

swarm. The cluster size is depending on the availability of food sources as well as the region. The essential criteria of the SMO algorithm are swarm intelligence (SI), and it should comprise labour division and self-organization. The foraging works are divided by the Spider monkeys Labour division by creating smaller groups. To meet food availability principle of Self-organization is followed. Thus, an SMO-based algorithm divides into a normal, swarm intelligence-based algorithm.

7.2.2 Implementation of SMO Algorithm

Implementation of this algorithm is done using six-stage such as local leader stage, local leader learning stage, local leader decision stage and global leader stage, global leader, learning stage and global leader decision stage. The workflow of the SMO is shown in figure 7.3. The procedure is described below:

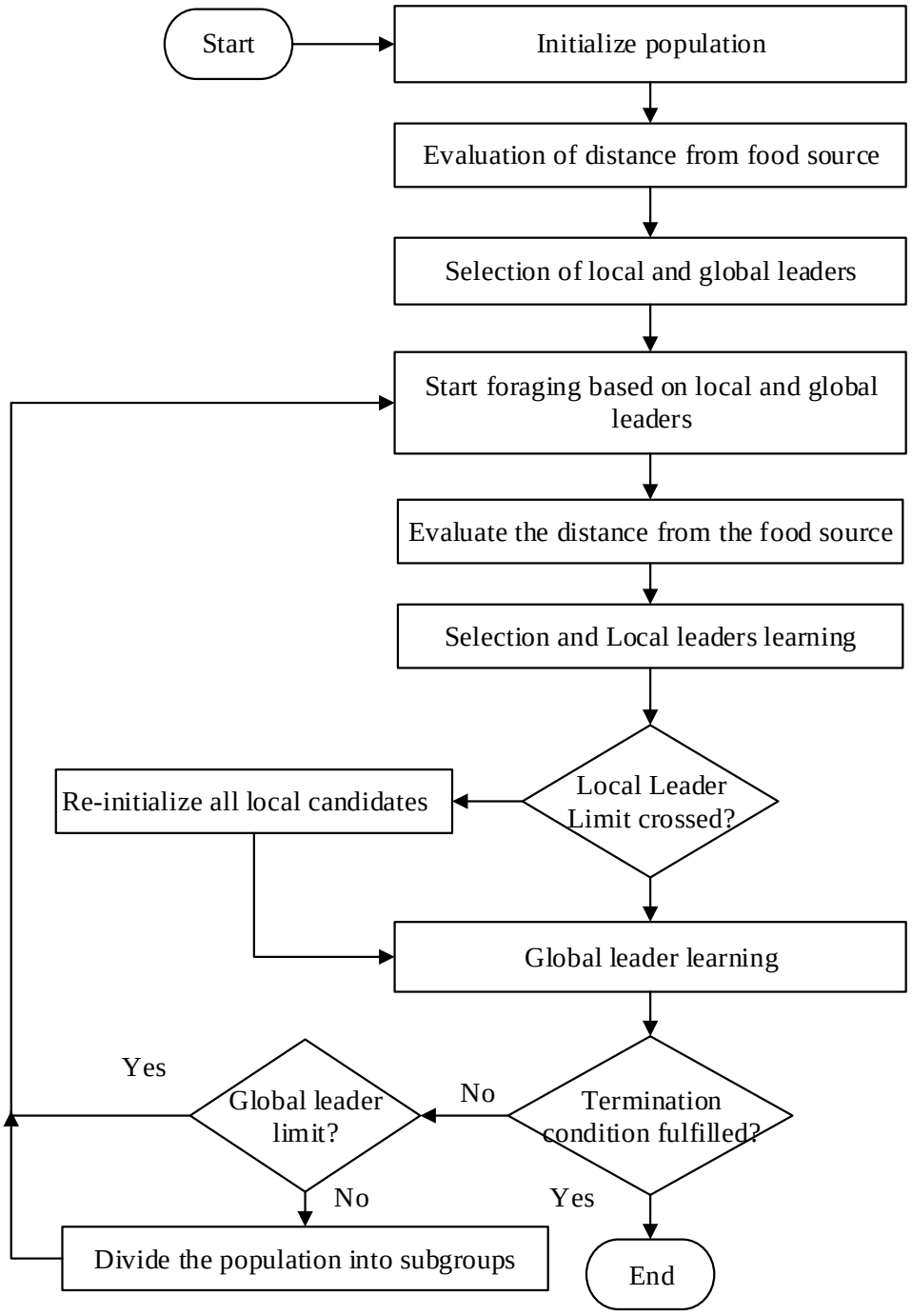

Figure 7.3: The Proposed workflow of the SMO algorithm

7.2.2.1 Population Initialization

The population of SMO is uniformly distributed the spider monkeys denoted as SMp .In which p =1, 2... P and in the population the pth monkey is signified as SMp. As M-dimensional vectors the Monkeys are identified where M determines the sum of problem

domain variables. Each spider monkey is related to an optimal solution for the provided problem. The following equation is used by SMO to initialize every SMp:

$$SMpq=SMminq+UR(0, 1) \times (SMmaxq – Smminq) \quad (7.1)$$

Where,

SMpq denotes qth dimension of the pth Spider Monkey.

SMminq denotes the lower bound of SM in q th direction

SMmaxq denotes the the qth direction upper bounds of SM p (where q =1, 2... M)

Random number is denoted by UR (0, 1) which is distributed over the range of [0, 1].

7.2.2.2 Local Leader Stage (LLS)

The next step is LLP. It uses the past events of both local leaders and local group members to modify SM's current location. The position of the SM is only upgraded to the new spot whenever the current locations fitness value is preferable to the former one. The Local group expression for the pth SM is shown below in Eqn 7.2:

$$SMnewpq=SMpq+ UR(0, 1) \times(LLlq- SMpq) +UR(-1, 1) \times (SMrq - SMpq) \quad (7.2)$$

Where, the qth length of the lth local group leader location is denoted as LLlq. The qth length of the arbitrarily chosen lth SM of the lth local group is denoted as SMrq, which meets the condition that $r \neq p$.

7.2.2.3 Global Leader Stage (GLS)

The third step of the implementation is GLS. In this step the experience of global leaders and the new location of SM is upgraded using the local group members.SM location of the equation is given below.

$$SMnewpq=SMpq+UR(0, 1) \times (GLlq- SMpq)+UR(-1, 1) \times (SMrq - SMpq) \quad (7.3)$$

The location of global leader in qth dimension is denoted as Where GLq and the q values are

assigned as 1, 2, 3, the arbitrarily designated index is termed as M. Fitness value of SM is utilized to determine prbp (probability) and the location also updated in such a way. The members at the proper position have access to more chances to develop itself. Estimation of the probability equation is:

$$prb_p = \frac{fnp}{\sum_{p=1}^{N} fn_p} \tag{7.4}$$

The fitness value of the pthSM is denoted as fnp. Then the new locations fitness value is assessed and compared with the previous location. Finally, the preeminent fitness value is chosen for further processing.

7.2.2.4 Global Leader Learning Stage

The global leader position is updated by adopting the greedy selection method. The position of the SM with the maximum fitness value in the community is updated to the leading global location. The global leader provides the best position. If there are no additional updates, GlobalLimitCount tends to add an increment of 1.

7.2.2.5 Local Leader Learning Stage

The greedy search approach all through the local group is used to upgrade the local leader position. The location of a local leader in a particular local group is updated by SM and the best fitness. The local leader has an optimal location. If no additional updates are found, then the Count of Local Limit increased by 1.

7.2.2.6 Local Leader Decision Stage

Within the limit of a local leader, if the local leader is not updated then the candidates of the local group, as per the step 1or by using the previous data from the local leader and the

global leader modify their locations, due to the pr through the following Eqn (7.5).

$$SMnewpq=SMpq+UR(0, 1) \times (GLlq- SMpq) + UR(0, 1) \times(SMrq -LLpq) \quad (7.5)$$

7.2.3 Brownout Based Energy Model

In data processing and migration, the real concern is the energy which is measured by the power utilized by each VM. The cloud domains energy is mainly relied on the power expended from several resources of the VM. This Brownout mechanism is adopted by the proposed model to reduce energy and carbon footprint. The resource usage is controlled by this approach by actively controlling the applications optional applied to microservices.

7.3 Blockchain Platforms

In a permission less blockchain, Ethereum is one of its kinds which works on PoW (Ethash) consensus appliance and uses ether currency. Whereas when it comes to permissioned Blockchain technology the Hyperledger is one of its type which works on PBFT (excluding Corda) appliance and doesn't use any currency. This particular type runs on validating and non-validating peers. Another specific distributed ledger platform is the R3 which works on exact knowledge of consensus i.e. notary nodes. The ether currency is used by the Ethereum to gift the nodes that aids to pay transaction fees and extent consensus, therefore monetary transactions based decentralized applications could be built for Ethereum. For the consensus mechanism, the R3 Corda and Hyperledger don't need cryptocurrency as they do not ensure the mining procedure. Still, using chain code in the Hyperledger using the inherent currency is feasible. For any sorts of application, the Ethereum prevails to be a generic platform. The permissionless mode and flexibility nature of it descends at the price of privacy, scalability and performance. The Hyperledger address these issues by the applications permission mode. Corda can be adopted in abundant applications and is sectional in structure. Primarily the Corda

emphases on transaction of financial services.

7.3.1 Categories of Blockchain

This section briefly presents the blockchain types. In blockchain there are two types of ledger:

(A) Private or Centralized ledger or (B) Public or Decentralized ledger. The blockchain is of two types based on permission they are (C) Permissioned and (D) Permission less.

A. Public or Decentralized:

This particular ledger is based on consensus algorithms which are not permission (pp) and source. Any person can write, read and send information. The block or the transaction is created by the buyer, later with the help of cryptographic hashing the transaction is distributed or validated. The miners are rewarded and the transaction is committed to blockchain in the distributed databases. Then the transaction is received by the seller via trustless peering. Some of the consensus mechanisms such as Proof of Stake, Proof of Work are used by the ledgers to secure them. Examples: Ethereum, Monero, Bitcoin, Dogecoin, Litecoin, Dash etc.

B. Private or Centralized:

In this particular ledger, the permission to write is consolidated to one establishment while the permission to read is restricted or available publicly. The benefits of the blockchain technology are grabbed by them where the transactions are verified by the end-users internally. The redundancy is minimised which leads to cost-effective transactions. In this system, the participant's known identities and are preapproved. In the present situation, these types of ledgers are comparatively outdated.

C. Permissioned:

One of the ideal examples of this particular blockchain is the Bitcoin. In this network, every node subsidizes in consensus method. This blockchain might be private-permissioned or public-permissioned. This particular approach works on the Proof of Work protocol in which

any person with assured predefined norms can validate the transactions and download the protocol but in permission private, the transactions are validated by the member of the consortium with the PBFT or multi-signature.

D. Permissionless:

This particular blockchain has apparent and public proprietorship and works on proof of work; anyone can validate transactions and access the protocol.

7.3.2 Resource Management Using Blockchain

This section discusses in brief about handling the VMs and requests using blockchain in cloud DCs.

Preliminary:

All member of a blockchain network has the blockchain which is a linked data structure. To handle the consensus issues of the Bitcoin network it was presented. The structure of the blockchain is illustrated in Figure 7.4.

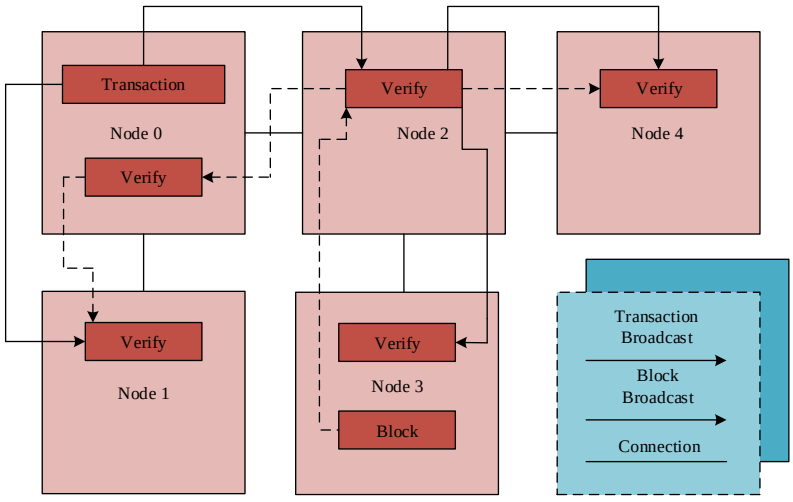

Figure 7.4: Structure of blockchain

As a single list, the blockchain is organized in which apart from the first block (genesis block) the remaining blocks comprises the previous block's hash. Initially, the former block is generated before the latter block and the records of blockchain actions are carried by every block, i.e., assets transferring. Figure 7.5 presents a detailed description of the generation

mechanism of the blockchain. The description of figure 7.5 states that:

1. A transaction is signed by the user using the private key while interrelating with Node0. Thus, using the user's public key the transaction possibly could be traced moreover the security and data integrity is reinforced by the digital signature. Then, to the one-hop neighbour of Node0 (i.e., Node1 and Node2) the transaction is made.

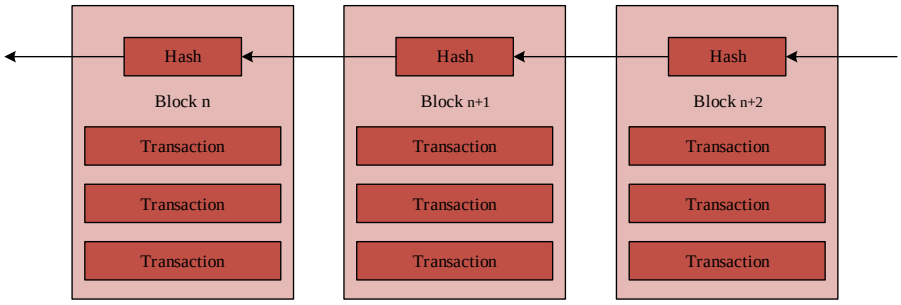

Figure 7.5: The blockchain network

2. The broadcast transaction is verified by the neighbouring nodes (i.e., Node1 and Node2) follows the transaction protocol and to prevent the falling of the transaction they are broadcasted to neighbours (Node3 and Node4). When designing the blockchain the determination of the transaction protocol is also done. The transaction protocol in the blockchain network prevents chaos. The entire blockchain network is spread by this transaction by repeating the above-mentioned procedures.

The network generated transactions by all participants at the time of a fixed time interval using the mining node are packaged into one block, then

1. The block to blockchain network are broadcasted by the miner (i.e., Node3). The block is also broadcast peer to peer like the transaction. As a result, the block is received by the Node2.

2. The Node2 which is the receiver validates

a. whether the transaction protocol is obeyed by all the transactions of the block; and

b. in the blockchain a correct hash is present in the block of the previous block.

Once the verification is passed the receiver combines it to the blockchain and extracts the block having transactions to update the transactions of the receiver, which is known as the "vision of

the world." Or else, the block is rejected. In the blockchain network, the consensus mechanism leverages the miner's choice.

To offer blockchains next block in Bitcoin, the random value of the nodes first found should be entitled. Mining is also called as the finding process, which is a sort of consensus mechanism. The entire participant of the blockchain network possesses a blockchain and the consensus process is very important. The public network blockchain which can be used by anyone commonly uses proof of stake (PoS) or proof of work (PoW) as its consensus process. Some of the prevailing consensuses approach for the network is Tangaroa and practical Byzantine fault tolerance which are accessible to white list members only (a private network).

7.4 Results and Discussion

In this chapter, two groups of simulations are carried out using CloudSim simulator. In the first part, the performance of SMO is attained by measuring the response time, makespan, and resource utility. The second part validates the efficiency of the approach proposed. The analysed factors are Execution time, Acceptance ratio, Resource Exploitation and Power Management.

7.4.1 Performance evaluation for Stage 1

Tables 7.1, 7.2, 7.3 and 7.4 demonstrate the simulation parameters used to evaluate the proposed SMO and compared the performance of the SMO with ABC-clustered, ABC, Firefly-CSA, and WOA algorithms. The scheduling process increases the locality rate by significantly reducing the processing period for tasks mapped by reducing network traffic, as it reduces tasks mapped to remote fetching. The efficiency of the SMO system is measured with dimensions such as response time which cover a varying number of tasks.

Table 7.1: Results for number of tasks=100

Algorithm	Response time (s)	Makespan (s)	Resource Utility(%)	Energy Consumption(Joule)
ABC-Clustered	321	56	68	40
ABC	313	56	69	30
Firefly-CSA	307	55	72	22
WOA	296	53	73	14
SMO	287	51	76	10

The response time of the proposed approach is validated using a varying number of tasks during processing. The estimated mean response time of the proposed approach under a contrasting number of tasks is depicted in Figure 7.6. Compared with other techniques, our proposed approach provides better results. The proposed algorithm responds within 287 seconds, which is 10.5 % greater than the other methods.

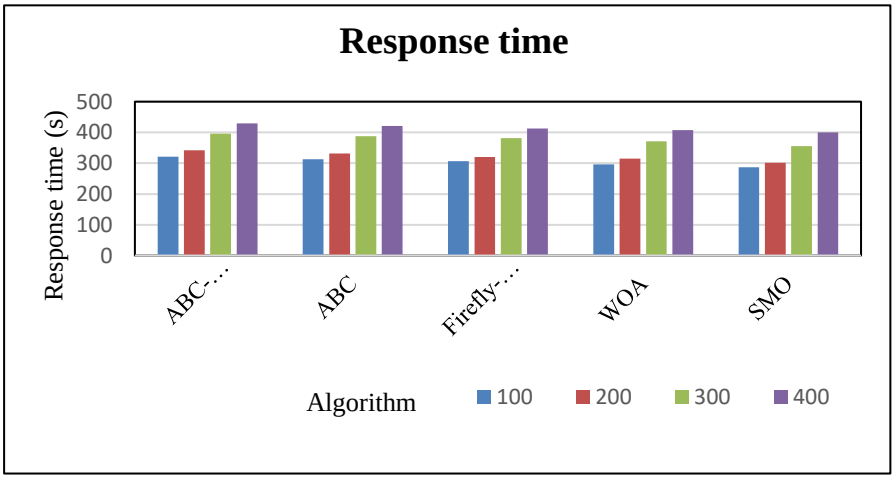

Figure 7.6: The comparison analysis of response time vs the number of tasks

Table 7.2: Results for number of tasks=200

Algorithm	Response time (s)	Makespan (s)	Resource Utility(%)	Energy Consumption(Joule)
ABC-Clustered	342	71	68	49
ABC	332	69	71	38
Firefly-CSA	320	67	73	30
WOA	315	66	74	25
SMO	301	65	77	18

Figure 7.7 illustrates the comparison of makespan response with other algorithms. Comparison of resource utility is depicted in figure 7.8. Compared to other makespan values, SMO provides better results in which the resource utility also better.

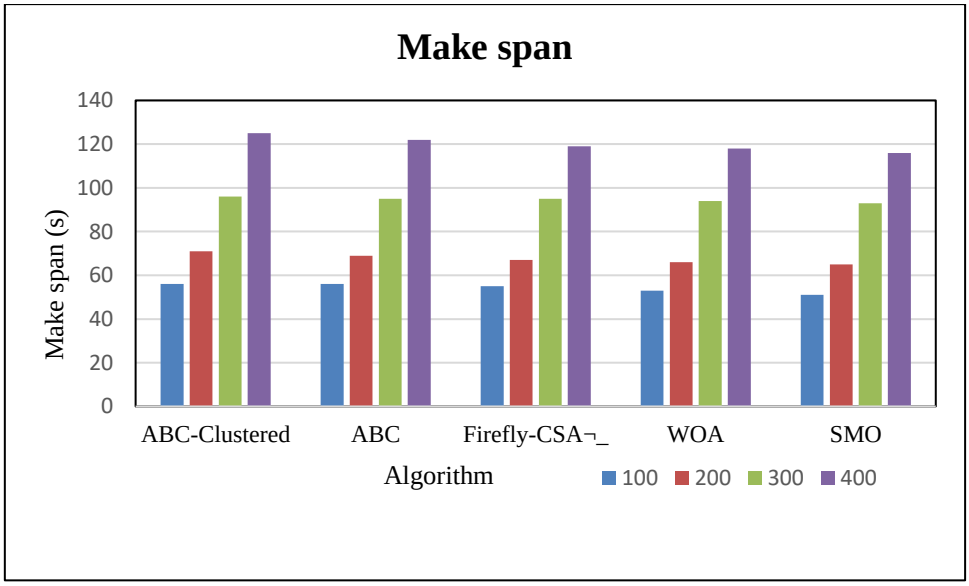

Figure 7.7: The comparison analysis of makespan response vs the number of tasks

Table 7.3: Results for number of tasks=300

Algorithm	Response time (s)	Makespan (s)	Resource Utility(%)	Energy Consumption(Joule)
ABC-Clustered	396	96	70	54
ABC	388	95	70	46
Firefly-CSA	382	95	70	37
WOA	371	94	72	31
SMO	356	93	75	27

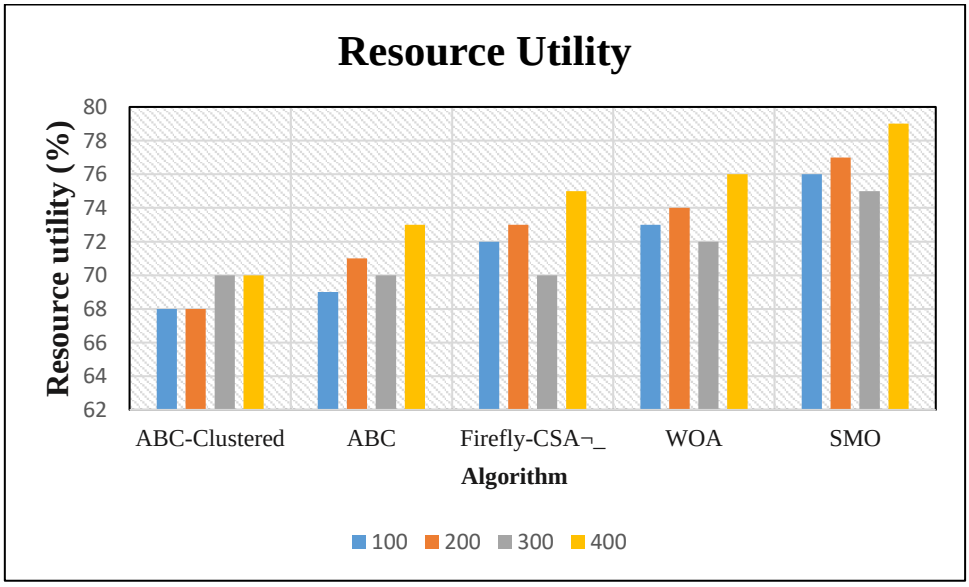

Figure 7.8: The comparison analysis of resource utility

Table 7.4: Results for number of tasks=400

Algorithm	Response time (s)	Makespan (s)	Resource Utility(%)	Energy Consumption(Joule)
ABC-Clustered	429	125	70	65
ABC	421	122	73	52
Firefly-CSA	413	119	75	45
WOA	408	118	76	39
SMO	400	116	79	33

The resource utility also increased up to 80 %, in which the other methods exhibited only 70%. Comparatively, resource utilization is increased by 10%.

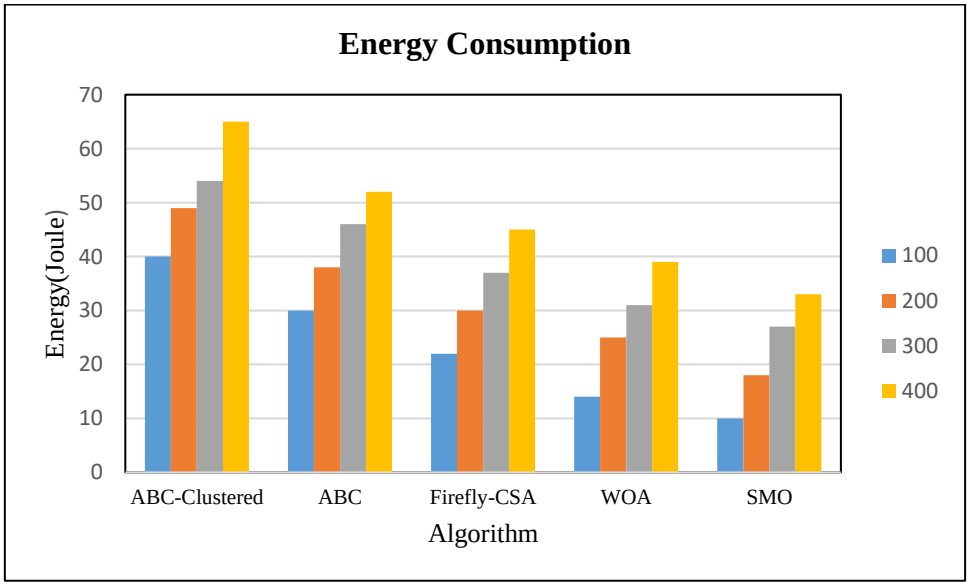

Figure 7.9: The comparison analysis of energy consumption

The energy consumption of the proposed approach is validated using a varying number of tasks during processing. The estimated energy consumption of the proposed approach under a contrasting number of tasks is depicted in Figure 7.9. Compared with other techniques, our

proposed approach provides better results. The proposed algorithm consumes 33 joules for 400 tasks, which is 18.2 % lesser than the other methods.

7.4.2 Performance evaluation for Stage 2

The cloud data center is comprised of several PM's. The resource agents in the Datacenters are initiated. A series of hosts in each datacenter with their equivalent VM's are initiated. The incoming tasks are scheduled by the cloudlet scheduler. The Hardware necessities are displayed in Table 7.5 and in Table 7.6 the specification of cloud sim are presented.

Table 7.5: Hardware requirements

Resources	Specifications
Processor	Intel Pentium CPU G2030@3.00GHZ
Hard Disk	1TB
RAM	4GB
OS	Windows (X86 ultimate)64 bit

Experimental validation is done using certain metrics like resource utilization, makespan, completion ratio, execution time and power consumption. The efficiency of the system is enhanced by the proposed approach and is compared with the prevailing approaches.

Table 7.6: Simulation parameters

Resources	Specifications	Values
VM	Host	4
Cloudlets	Length of task	1600-3400
	No of Tasks	30-3000

Physical machine	Bandwidth	25,00,00
	Memory	540
	MIPS/PE	500
	Storage	500GB

The graphical representation reveals the performance of the proposed approach. For Calculating the Resource Utilization the ratio of the consumed resources in the data center is analyzed. The tasks arrived as a batch in this approach. For job arrival, the batch processing concept is borrowed. Our approach is used for the allocation task. The task scheduling concept is applied to prioritize jobs. The tasks which are prioritized are given to the agents for allocating the available resources. Some of the existing approaches GA, PSO and ACO are used for comparison during this process and the parameters calculated are Bandwidth, acceptance ratio, execution time. Valuation of the performance is done with certain metrics i.e. resource utilization, makespan, task completion ratio, execution time, and power consumption.

7.4.2.1 Task response time (TRes)

Time taken from the arrival of the task to the execution of the task is called the Response time of a task. Let the task completion time be TCmp the task arrival time be and TStart the response time TRes can be denoted as follows,

$$T_{\mathrm{Res}} = T_{Cmp} - T_{Start} \qquad (7.6)$$

The response time as seen in figure 7.10 is very less when compared to the other algorithms

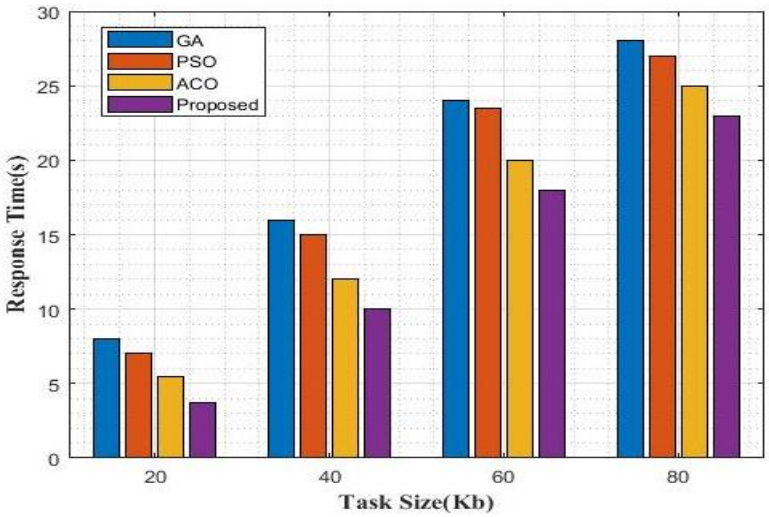

Figure 7.10: Comparison of response time

7.4.2.2 Makespan (Mspan)

The execution time taken for a set of tasks as of the start to the end of the task is called a Makespan. The time taken to accomplish all tasks be TC, the Mspan is denoted subsequently.

$$M_{span} = Max(T_C) \tag{7.7}$$

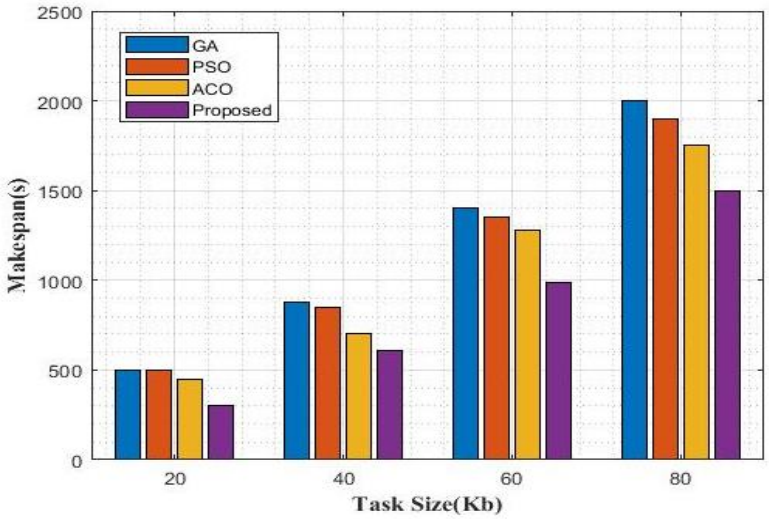

Figure 7.11: Comparison of makespan

Minimized makespan is provided by the results when validated with the other algorithms. Graphical representation in figure 7.11 offers a reduction in Makespan and a rise

in efficiency by about 30% than the existing methods.

7.4.2.3 Resource utilization (RU)

The volume of resources available exploited by the tasks to get fulfilled is called as resource utilization. The available resources are represented as Ravl and the resourced unused is represented as Run. The Resource utilization (RU) is denoted as

$$R_U = R_{avl} - R_{un} \tag{7.8}$$

Both memory and CPU and used in the proposed work. The proposed works utilization percentage is higher when with the other algorithms.

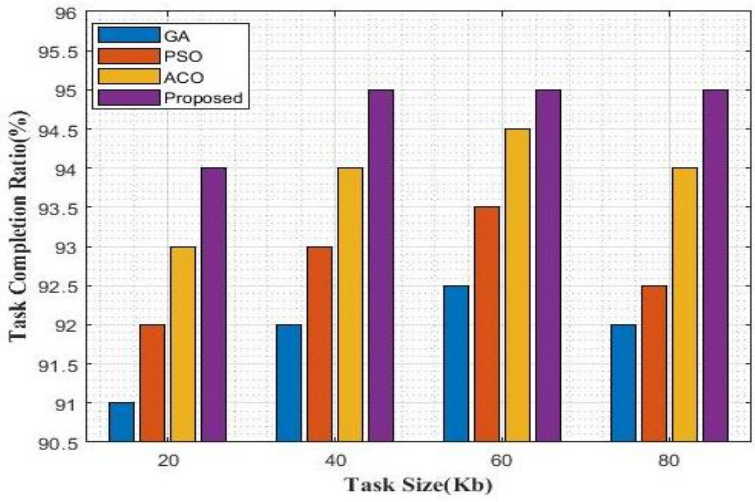

Figure 7.12: Comparison of resource utilization

The maximum utilization of resources is displayed in the graphical representation of Figure 7.12 The proposed approach makes the PM's which are idle in OFF state. It has a role in this method

7.4.2.4 Task completion ratio (TCR)

It is a ratio of effectively accomplished tasks to the tasks which are submitted at a definite time. The number of completed tasks be Nscc and the submitted tasks are Nsbt, the completion ratio

of the Task is denoted as subsequently

$$T_{CR} = {}^{N_{scc}}\!/_{N_{sbt}} \tag{7.9}$$

During the simulation, the completed tasks for a definite period of time are analysed. The improved performance ratio is given by the simulation result. The proposed approach is compared with the existing algorithms for testing the performance.

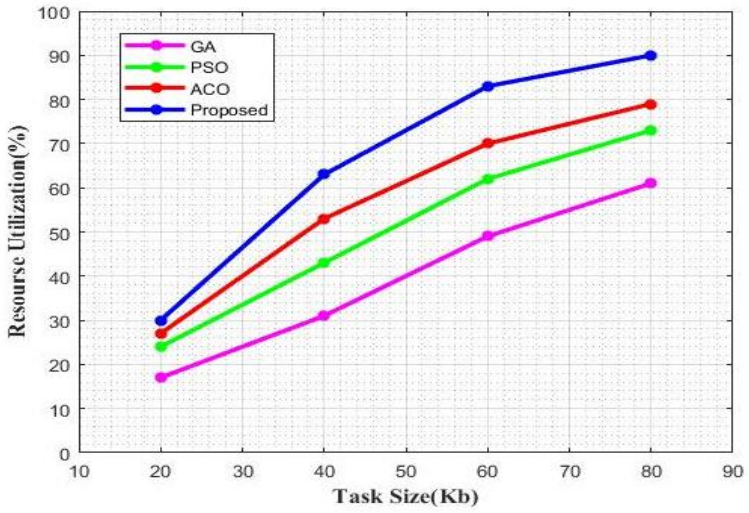

Figure 7.13: Comparison of task completion ratio

The graphical representation in Figure 7.13 reveals the dominance of the presented approach when compared with the other.

7.4.2.5 Power consumption

The power used during the resource allocation process by the PMs is defined as power consumption. It is clearly said as the total power utilized by all PMs. The Brownout approach is adopted in this proposed work to minimize energy utilization. In real-time data centers, there are a lot of technologies dealing with the consumption of power such as, Resource hibernation, Dynamic Voltage Scaling and Dynamic voltage Frequency scaling which doesn't sense the virtualized environment. The implemented approach for power minimization in this study is superior when compared to the existing methods.

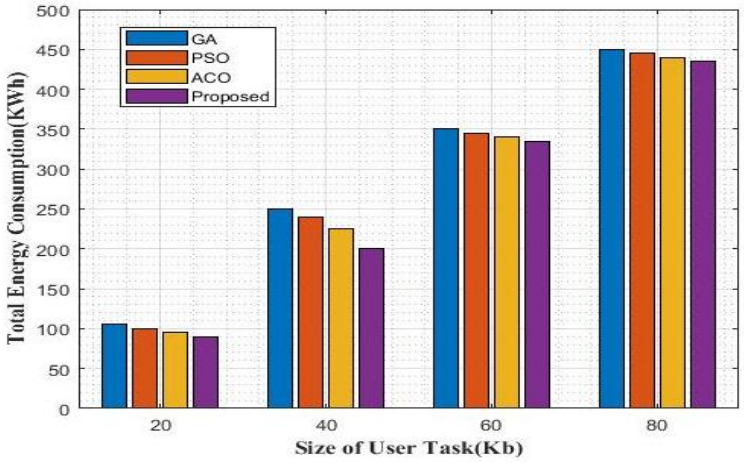

Figure 7.14: Comparison of power consumption

Figure 7.14 show that the proposed approach consumes minimum power than the existing methods. In this paper, the proposed power management approach diminishes the energy utilised by Idle VM, baseline energy used by PM and the energy used for internal and external communication.

CHAPTER VIII

QoS and Service Level Agreement Policy

The content of this chapter is published in-

1. **Materials Today: Proceedings, Elsevier, ISSN: 2214-7853. SCOPUS Indexed, (In Press)**

CHAPTER VIII

QoS AND SERVICE LEVEL AGREEMENT POLICY

8.1 Introduction

There is no precise meaning of cloud yet we can characterize cloud in different manners and by considering different methods. Cloud computing is an Internet-associated method of supercomputing. It is a sort of shared infrastructure, which just puts the colossal framework pools together by utilizing different methods; disseminated virtualization, and so on. It gives clients an assortment of capacity, systems administration, and computing assets in the cloud computing condition using the Internet, clients put a ton of data and access a great deal of computing power with the assistance of its own PC. Worldwide the Cloud computing is unique solid computing. Notwithstanding, the optimization of the utilization of cloud server farms has become an unmistakable issue. Task scheduling is momentous progress to improve the cloud computing general execution. Conventional observing and the board components are intended for big business conditions, particularly a bound together condition. Be that as it may, an enormous scope, heterogeneous asset provisioning places genuine difficulties for the administration and observing instrument in different server farms. As of late, this task scheduling issues in a circulated domain has grabbed the eye of scientists. Task scheduling is viewed as a basic issue because of various components like culmination time, the maximum expense for fulfilling every one of clients' tasks, usage of the asset like power utilization, and adaptation to non-critical failure. A cloud server farm ordinarily comprises of a huge gathering of servers associated with the Internet. To organize the task executions a task scheduler is required in a cloud server farm. To execute tasks, the task scheduler needs to effectively use cloud server farms assets. The exhibition matters of the scheduling calculation incorporate the vitality utilization and the makespan. To achieve task execution a decent scheduler can utilize

very less time and fewer assets. Less vitality is consumed when exploiting few assets. Reducing the makespan and vitality utilization is the main problem for creating an enormous scope of clouds.

"Cloud computing is anything but a polite paradigm for giving needed, the client required, adaptable approach to a set of computing assets which are configurable and might be immediately furnished and discharged with depleted consideration exertion or administration which examine the distinguishable scheduling of tasks for elite algorithms". Different virtual machines (VMs) in the Cloud computing settings share physical assets (memory, bandwidth and CPU) on a solitary physical host and by utilizing the system virtualization many VMs can share the bandwidth of a server farm. Since the framework assets are shared by numerous clients and applications, a legitimate plan for task-scheduling is hard to asset usage as well as framework execution. Numerous framework boundaries for example memory space, the bandwidth of the system and processor power influence the effectiveness of task scheduling. In the cloud, the principle point of task scheduling algorithms is to maintain the exact burden on processors by considering the bandwidth of the system and augment their productivity, utilization and to lessen the execution time of the task [151].

Cloud computing is an important technology for bulk data storage, resource mobilization and online access to computer services. In the cloud computing platform, there are plenty of resources, but the foremost challenge is to allocate tasks. The vital issue in scheduling is how the entire task could be allocated with maximized resource utilization to a resultant virtual machine, existing scheduling algorithms mainly focused on minimization of the task execution time while ignoring the SLA and QoS assurance [172,177]. This chapter thrives to accomplish the total task with eminent resource utilization, minimum migration cost, and minimum utilization of energy. For attaining these objectives, the proposed method utilizes the hybrid algorithm such as Fuzzy-TOPSIS and particle swarm optimization (PSO) approach. Initially,

the available task and the no. of VMs (virtual machines) are optimized by the PSO algorithm. In the cloud, the multi-objective SLA based task scheduling problem is solved by the Fuzzy TOPSIS which uses the weighted sum of energy, cost and execution time as an objective function. Fuzzy TOPSIS method is work positively for many applications and impacts liberally on real-world decision making concerns. The proposed approach is investigated based on distinct evaluation metrics. Our proposed algorithm outperforms the existing approaches and achieves better results in terms of QoS parameters. The implementation had done using JAVA with CloudSim simulator.

8.2 Problem Definition

In cloud computing, Task scheduling is a vital approach, which is the systematic utilization of available resources by organizing the inbound requests (tasks) in a specific style. Many techniques have been used in the existing method, but there are several problems. Some of the problems are listed below,

1) Task scheduling is not very accurate, considering additional constraints, such as the budget of work providers and the deadline of workflow implementation.
2) Task scheduling is a crucial topic for attaining high efficiency. Though, this is a major dispute for the execution of efficient planning algorithms. In cloud computing most existing work-planning approaches only judge the workflow, not just the bandwidth requirements, but also the requirements for CPU and memory.
3) In the existing system, it is more difficult in allotting the associated computing sources to tasks that could improve the weight of the tasks precisely by improving the consistency ratio.
4) The complexity and time will get increased when tasks are rescheduled to perform load balancing.

This motivates us to develop a new method in cloud computing for effective task scheduling.

8.3 Proposed Methodology

In the emerging paradigms, cloud computing is a platform that offers different administrations for both enterprises and users. In the cloud, the provoking issue is the scheduling of user tasks between Host, Virtual Machines and Data Centers owing to the association of colossal users. To deal with such issues, the effective task scheduling algorithm is suggested here. The principle aim of the study is to plan the task in cloud productively with the assistance of Fuzzy TOPSIS and PSO algorithm [143,177].

This study intends to reduce energy depletion and migration cost. In this study, a hybridization of PSO and Fuzzy TOPSIS is made for task scheduling to achieve the multi-objective function. Initially, the PSO algorithm optimizes the available task and the number of VMs. Here the Fuzzy TOPSIS solves the multi-objective task scheduling problem using the weighted sum of energy, cost and execution time as an objective function. Figure 8.1 depicts the diagrammatic representation of proposed task scheduling using Hybrid Fuzzy TOPSIS-PSO.

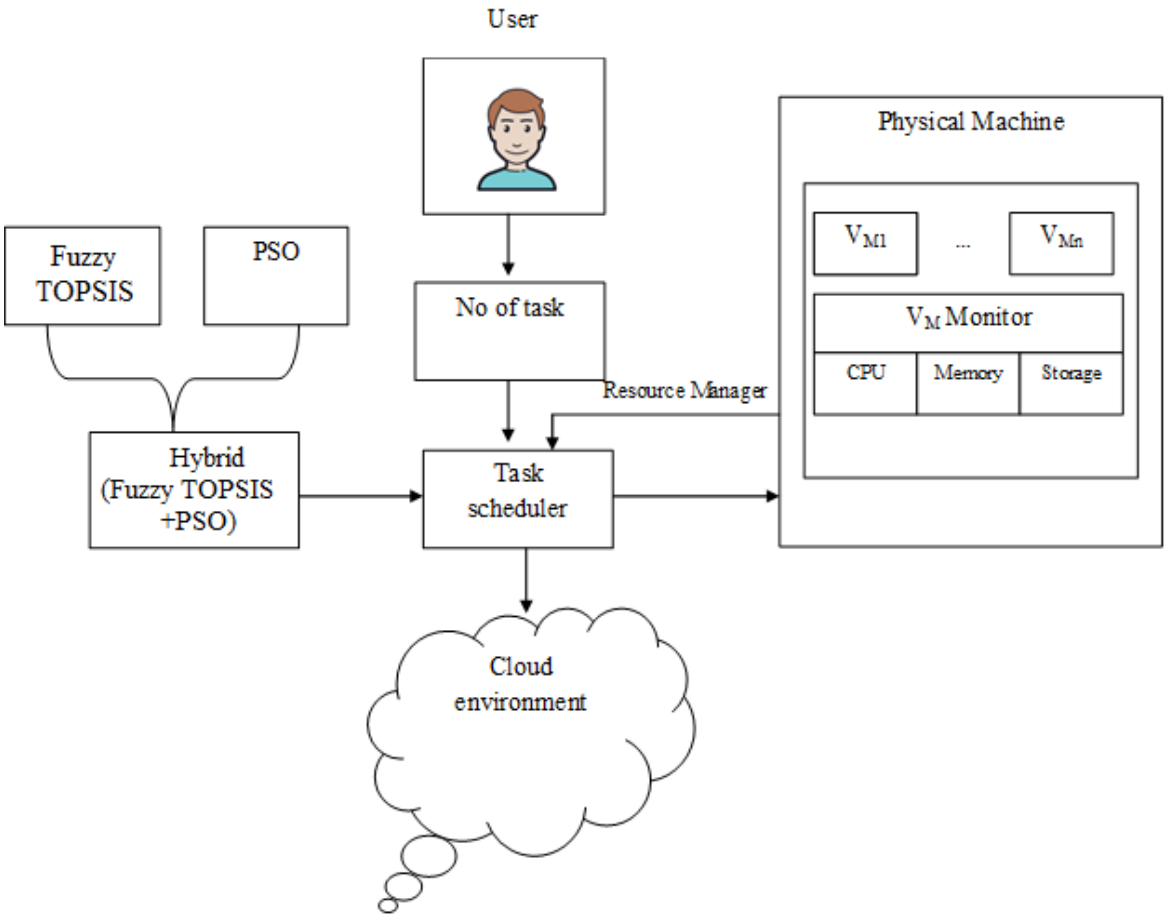

Figure 8.1: Proposed Block diagram of Task scheduling

In this study, every task that is submitted comprises of various odd and self-ruling sub-tasks. Every task should remain actualized in one VM occurrence type. Let a set of cloud PMs be represented as $P_M = \{P_{M1}, P_{M2}, ..., P_{Ma}\}$. The VM's are represented as $V_{Mi} = \{V_{M1}, V_{M2}, ..., V_{Mb}\}$ and $T = \{T_1, T_2, ..., T_c\}$ is a set of task. Every VM has separate execution time T_i, memory M_i, energy consumption E_i, and cost migration C_i. Every task has the dissimilar cost C_j, energy E_j and size S_j. In this study, the multi-objective function depends

on the two boundaries, for example, migration cost and energy consumption. The objective function can be planned by utilizing equation (8.1).

$$Objective\ \ function = \sum_{i=1}^{m} \min(C_i, E_i) \tag{8.1}$$

The objective function is determined in condition (1). The objective function is minimized by the proposed algorithm. The principal boundary of effective task scheduling is migration cost (M_C). To achieve the objective function minimum migration cost must be attained. By condition (2) the overall migration cost is determined.

$$M_C = \frac{F_M + F_C}{2} \tag{8.2}$$

Here, $$F_M = \frac{1}{P_M}\left[\sum_{i=1}^{V_{Mi}}\left(\frac{Number\ of\ movements}{Total V_M}\right)\right] \tag{8.3}$$

$$F_C = \sum_{i=1}^{V_{Mi}}\left(\frac{Cost\ to\ run \times Memory\ of\ task}{V_M \times P_M}\right) \tag{8.4}$$

To find the minimum migration cost value the Cost factor *(F_C)* and Movement factor *(F_M)* is calculated. Likewise, energy consumption E_i is the second factor for task scheduling. The energy utilized E_i is computed by using equation (8.5).

$$E_i = \frac{1}{P_M \times V_M}\left[\sum_{i=1}^{P_M}\sum_{j=1}^{V_M} A_{ij}\ E_{\max} + \left(i - A_{ij}\right)\delta_{ij\ E_{\max}}\right] \tag{8.5}$$

$$\delta_{ij} = \frac{1}{2}\left[\left(\frac{CPU\ utilized_{ij}}{CPU_{ij}}\right) + \left(\frac{memory utilized_{ij}}{memory_{ij}}\right)\right] \tag{8.6}$$

$$E_{\max=1};\ A_{ij} = 0.1 \tag{8.7}$$

Here the proposed algorithm minimized the above objective function. For that, the suggested method utilizes a Hybridization of Multi-objective PSO and Fuzzy TOPSIS is introduced here. The detailed explanation of the presented approach is explained subsequently.

8.3.1 Hybrid Fuzzy TOPSIS and Particle Swarm optimization (HTOPSISPSO)

PSO is an optimization algorithm based on a populace, which is introduced with a gathering of self-assertive elements and next scans for optima by reexamining groups. There are two sorts of variants utilized according to PSO. Primarily is "individual best" and the Next is "global best". Every individual situation of the particle is determined by the individual best algorithm by assessing its own best position. The global information is determined by the global best algorithm by making the development of the particles from the entire swarm. All particles fly during a multi-dimensional inquiry space where each particle is altering its position consent to its own understanding and the neighbours. The PSO algorithm comprises of only three stages:

1. Evaluate every particles fitness
2. Updating the individual and global bests
3. Updating the position and velocity of every particle

Until a condition is satisfied these steps are repeated. The upside of the conventional PSO calculation is the easiest optimization strategy which functions admirably for worldwide optimization issue. The fitness function is calculated using TOPSIS owing to its less productivity of obtaining ideal solutions for local optimum. Henceforth the TOPSIS acts like a fitness assessment apparatus. Two segments are considered in this study i.e. VMs and tasks. From the start, the strategy arbitrarily allocates the respective task to any of the VM. Here the technique thinks about an initial particle as the number of VM. The purpose of this study is to correspondingly schedule the tasks to VMs built on its functioning.

8.3.1.1 Evaluate the fitness of each particle

When the initial particle is produced, every individual's fitness value is stored and assessed for future use. The TOPSIS approach determines the fitness function and impacts liberally on

certifiable dynamic issues and function decidedly for some appliances. The TOPSIS-PSO algorithm does the Task scheduling process which maps the tasks of the client to VM by thinking about numerous generous elements. Contribution of TOPSIS algorithm supports different objective functions to boost the effectiveness of task scheduling. The general technique of TOPSIS calculation is delineated in underneath,

8.3.1.2 Fuzzy Logic

Fuzzy logic is a powerful process for representing and handing uncertainty problem. In this logic, a membership function is signified $\mu\tilde{A}(x)$ with the values in the closed interval of [0, 1].

If $\mu\tilde{A}(x)$ =0, the number x is not a member of the set;

If $\mu\tilde{A}(x)$ =1, the number x is a member of the set;

The attendance of x in other instances in the set is represented as fuzzy. The triangular membership function is followed in this study, $\tilde{A}$ is the triangular fuzzy number which is represented using three real numbers i.e. $\tilde{A} = (m1, m2, m3)$. The triangular membership function of a fuzzy number is shown is Figure 8.2.

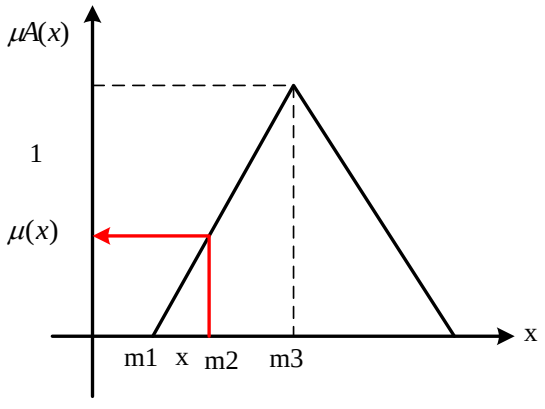

Figure 8.2: Triangular fuzzy set of number Ã = (m1, m2, m3).

Among these factors (m1, m2, m3), m1 denotes the minimum value, m2 denotes the most

possible value, and m3 denotes the biggest possible value. The fuzzy set intervals minor limits are denoted as m1 and m3, whereas m2 has the full membership with the single number, and the triangular fuzzy numbers membership function is represented below.

$$\mu A(x) = \begin{cases} 0, & x < m1 \\ \dfrac{x - m1}{m2 - m1}, & m1 \le x \le m2 \\ \dfrac{m3 - x}{m3 - m2}, & m2 \le x \le m1 \\ 0, & x > m1 \end{cases} \tag{8.8}$$

The linguistic and equivalent fuzzy depiction is presented in Table 8.1. The linguistic values of the membership function are displayed in Figure. 8.3.

Table 8.1: Membership functions of linguistic values

Linguistic Values	Fuzzy Numbers
Very Low(VL)	(0.00, 0.00,0.20)
Low(L)	(0.00,0.20, 0.40)
Medium(M)	(0.20, 0.40, 0.60)
High(H)	(0.40, 0.60, 0.80)
Very High(VH)	(0.60,0.80,1.0)
Excellent(E)	(0.80,1.0, 1.0)

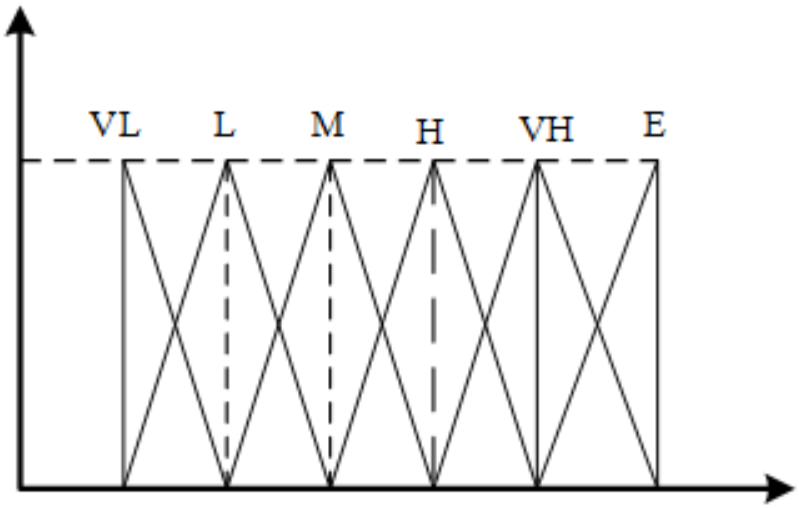

Figure 8.3: Linguistic values and fuzzy numbers

8.3.1.3 TOPSIS algorithm

Evaluate the decision matrix with the size a*b.

$$DM = \begin{bmatrix} EX_{T11} & T_{T11} & MC_{T11} \\ EX_{T21} & T_{T21} & MC_{T21} \\ : & : & : \\ EX_{TK1} & T_{TK1} & MC_{TK1} \end{bmatrix}$$

Where, E- Energy T- Time, MC- Migration cost

1. Normalize the decision matrix.

$$ND_{mn} = \frac{S_{mn}}{\sqrt{\sum S_{mn}^2}}$$

Where, m= {1,2,…i} and n= {1,2,…j}and S_{mn} represents the element of decision matrix.

2. Generate weighted normalized decision matrix.

$$E_T = E_{TK} \times W_E$$

$$T_T = T_{TK} \times W_T$$

$$MC_T = MC_{TK} \times W_{MC}$$

$$W_E + W_T + W_{MC}$$

Where, $0 < W_E, W_T, W_{MC} \leq 1$

3. Find the positive and negative impact of the initial solution.

$$P^+(Positive) = (S_1^+, S_2^+, ...S_m^+)$$

$$N^-(Negative) = (S_1^-, S_2^-, ...S_m^-)$$

4. Determine the separation measures from positive and negative for each alternative.

$$Sep^* = \sqrt{\sum_{n=1}^{3} (S_{mn} - S_n^+)^2}$$

$$Sep^{'} = \sqrt{\sum_{n=1}^{3} (S_{mn} - S_n^-)^2}$$

5. Evaluate the relative closeness of the initial solution.

$$RC_K = \frac{Sep^{'}}{Sep^{'} + Sep^*}$$

Here relative closeness is considered as the fitness function. In the population, the particles at every iteration move towards the optimal solution and based on fitness function computed from the TOPSIS algorithm their velocity is updated. The VM which gains the optimal fitness function is considered as the best solution. To find the best solution the residual VMs are

updated based on these functions.

8.3.1.4 Update Individual and Global Bests

In the beginning, among the fitness value, the best one is chosen as $gbest$ and $pbest$ value. Ensuing to that iteration, the overall best fitness value is selected as $gbest$ and the present optimal fitness value is selected as the $pbest$.

8.3.1.5 Update Each Particle's Velocity and Position

The particle velocity and position, changed by the equation as follows.

$$v_m^{new} = v_m + \psi_1.\xi_1.(pbest_m - p_m) + \psi_2.\xi_2.(gbest_m - p_m)$$

$$p_m{}^{new} = p_m + v_m{}^{new}$$

Where, ψ_1, ψ_2 - Learning rates, ξ_1, ξ_2 - Random numbers in the range [0, 1], v_m - specifies the current velocity and p_m - specifies the current position. The selected task is allocated when the proposed method achieves the best fitness. For each user task, this process is accomplished which is scheduled to VM. There is a major drop in the energy and migration cost when each task are allotted to VM. The task scheduling process based on HTOPSISPSO decreases the tasks makespan without any feature of effective resource usage.

8.4 Result and Discussion

The results obtained are discussed in this section. Java (jdk 1.8) with cloud Sim devices are used as a simulation tool for the task scheduling at 2 GHz dual-core processor with 4 GB RAM in a Windows OS 2007 64-bit version.

8.4.1 Performance Analysis:

This study aims to schedule the task through HTOPSISPSO algorithm. Evaluation of the proposed approach is done by no of resource utilization, migration cost, allocation time and execution time. Using three different task configurations the analysis of results is accomplished

with VM=35 and PM=10. Here the number of tasks varies from 100, 200 and 300.

A) PM=10, VM=35 and Task=100

Here, the method schedules the task based on ten physical machines and 35 virtual machines on cloud computing. In this work, the method considers the input task for scheduling is 100. Here the efficiency of the proposed methods is matched with the existing PSO and GA. The results are plotted below.

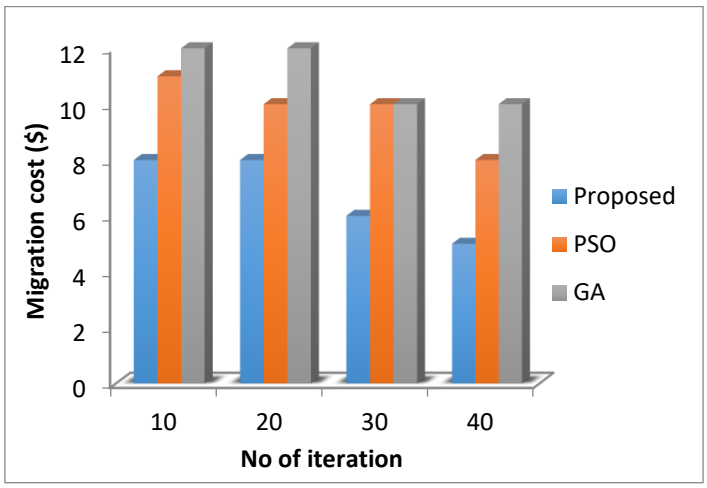

Figure 8.4: Comparison of migration cost of the proposed against existing methods

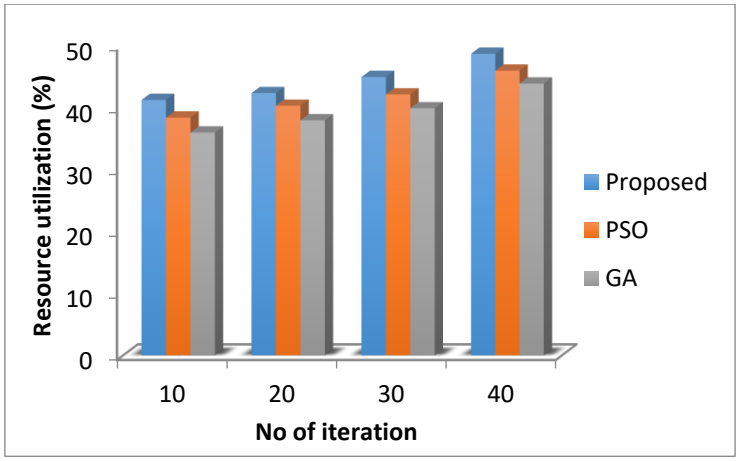

Figure 8.5: Comparison of resource utilization of proposed against existing methods.

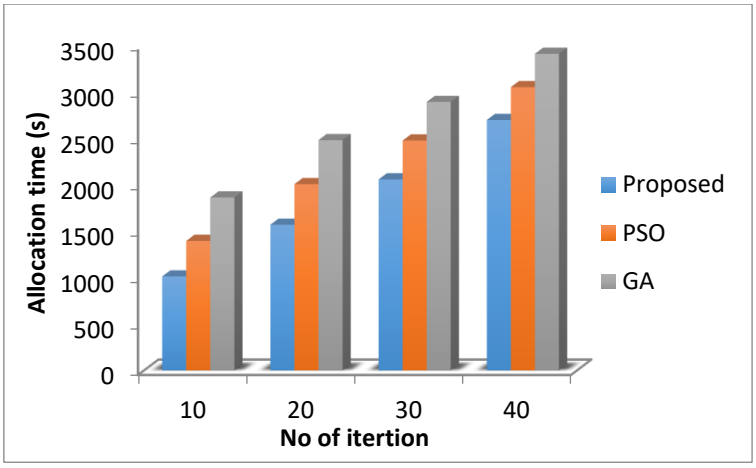

Figure 8.6: Comparison of the allocation time of the proposed against existing methods.

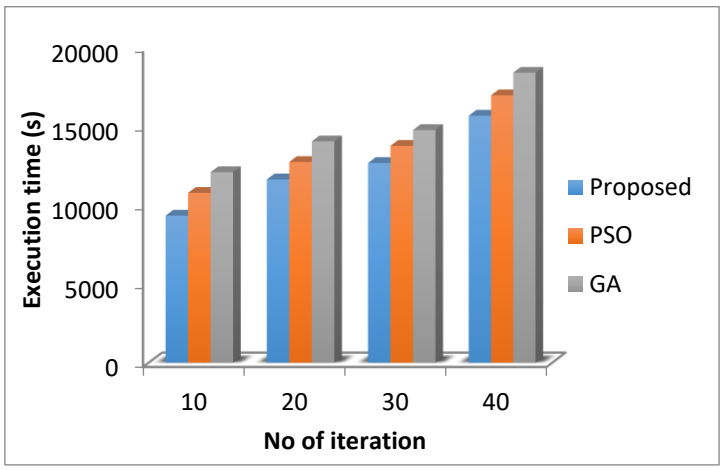

Figure 8.7: Comparison of the execution time of the proposed against existing methods.

Above in figure 8.4 to 8.7 displays the performance of the methods using 100 tasks, ten PMs and 35 VMs. Comparison graph of migration cost of the proposed against existing methods is displayed in figure 4. In which, the x-axis is shown the iteration and y-axis shown the migration cost. The good systems minimize the migration cost. Figure 8.5 shows the Minimum migration cost of 6.75$ obtained by the proposed approach when matched with the existing algorithm PSO and GA. The resource utilization graph of proposed against the existing is shown in Figure 8.3 which clearly displays the amount of effectively utilized resources. Maximum resource utilization of 44.31% is achieved by the proposed approach. The comparison graph of allocation time of the proposed against the existing is shown in Figure 8.6

in which the minimum allocation time is achieved by the proposed method. The execution time graph is illustrated in Figure 8.7.

B) PM=10, VM=35 and Task=200

Figure 8.8 to 8.11 displays the performance of the presented approach using ten PMs, 35 VMs with 200 tasks. Here, the method schedules the task based on ten PMs and 35 VMs on cloud computing. In this study, the method considers the input task for scheduling is 200. The graphical representation of the proposed performance analysis shown below,

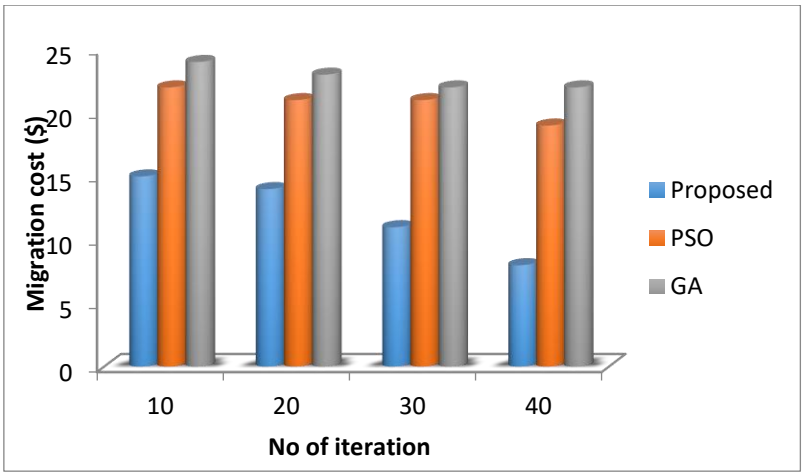

Figure 8.8: Comparison of migration cost of proposed against existing methods.

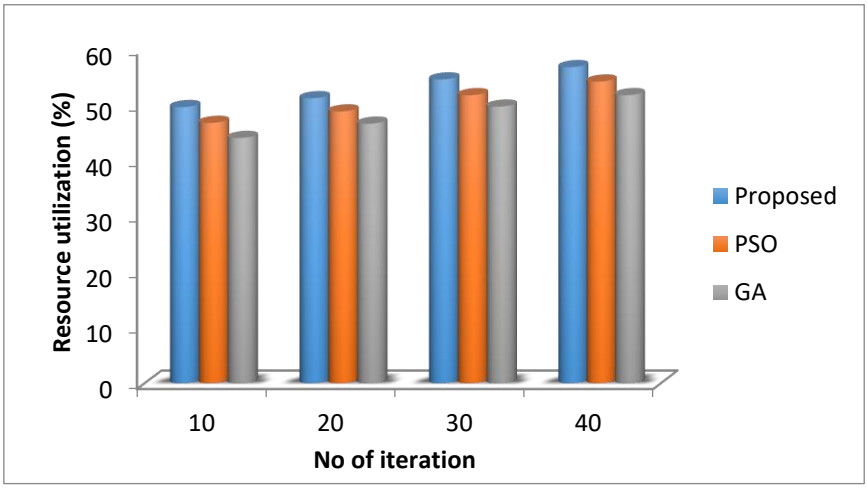

Figure 8.9: Comparison of resource utilization of proposed against existing methods.

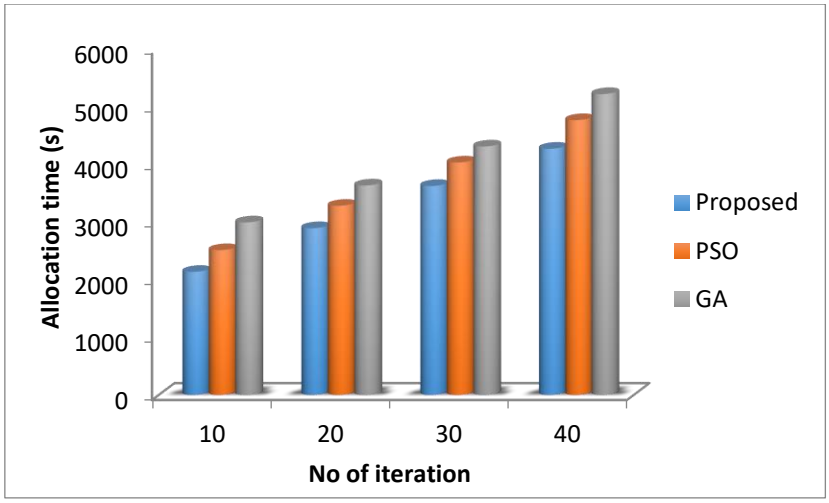

Figure 8.10: Comparison of allocation time of proposed against existing methods.

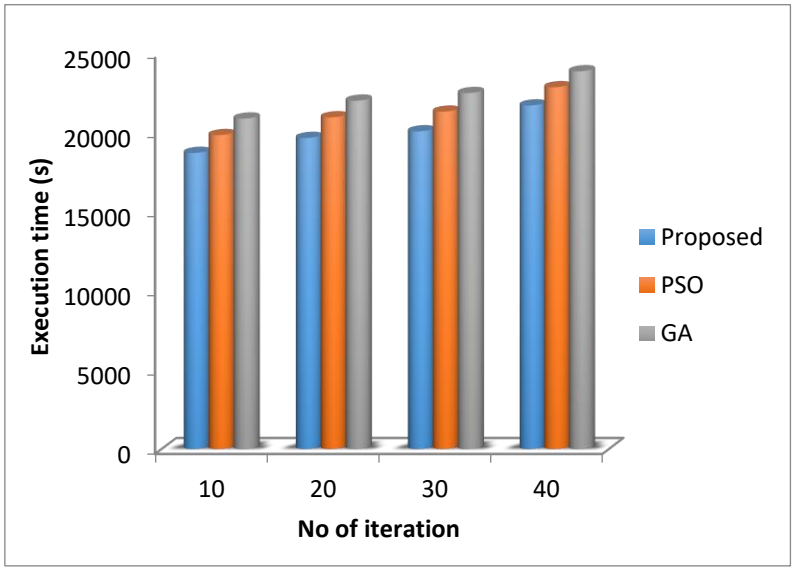

Figure 8.11: Comparison of the execution time of proposed against existing methods.

With the PSO and GA techniques, the proposed results are matched for calculating migration cost, resource utilization values, allocation time and execution time for task 200. Hence the graph, clearly exposes that the proposed approach has maximum resource utilization value, minimum migration cost, allocation time and execution time. During the 40th iteration process, the maximum resource utilization value is 56.84% and the minimum migration cost is 8$ compared to the existing PSO and GA model. The overall allocation time and execution time of the proposed approach are 3232s and 20018s which is very less when matched with the

existing ones. Therefore, as of the observations, it has been exposed that the proposed approach is effective than other methods.

C) PM=10, VM=35 and Task=300

The above figure 8.12 to 8.15 presents the performance of the proposed approach using ten PMs, 35VMs and 300 tasks. Now the method schedules the task based on ten PMs and 35 VMs on cloud computing. In this study, the method considers the input task for scheduling is 300.

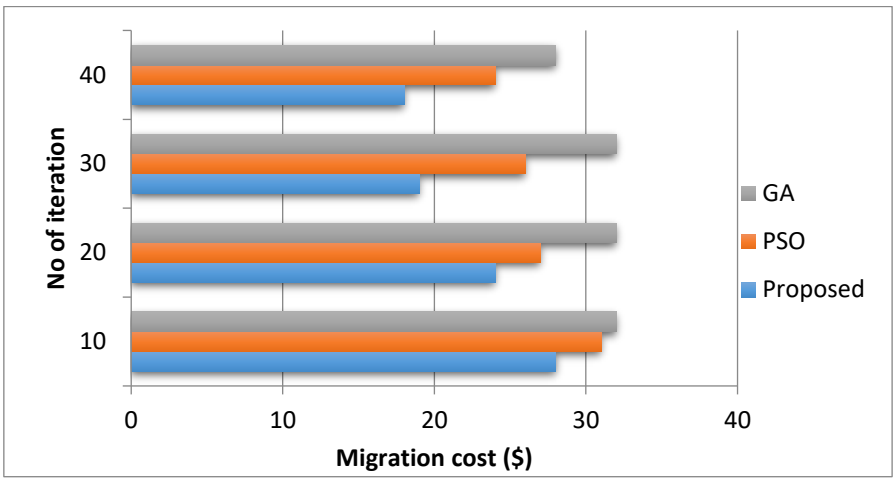

Figure 8.12: Comparison of Migration cost of proposed against existing methods.

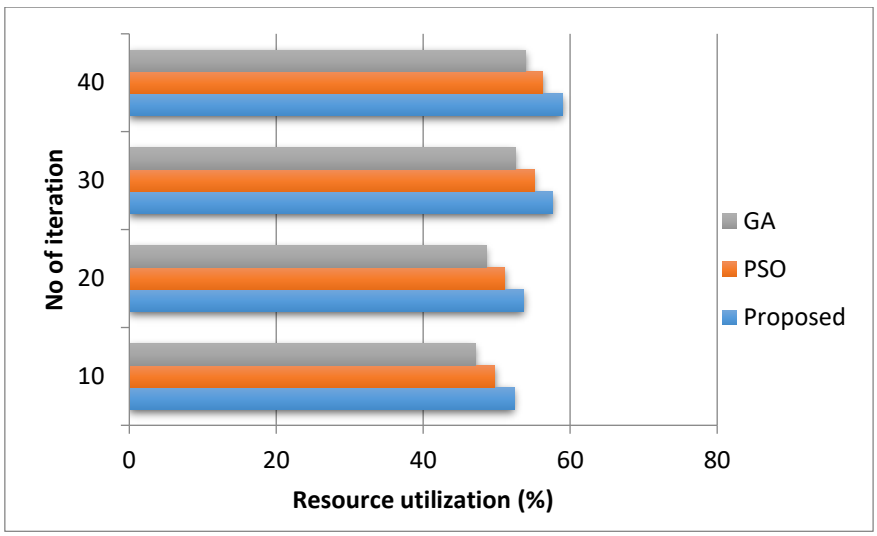

Figure 8.13: Comparison of resource utilization of proposed against existing methods.

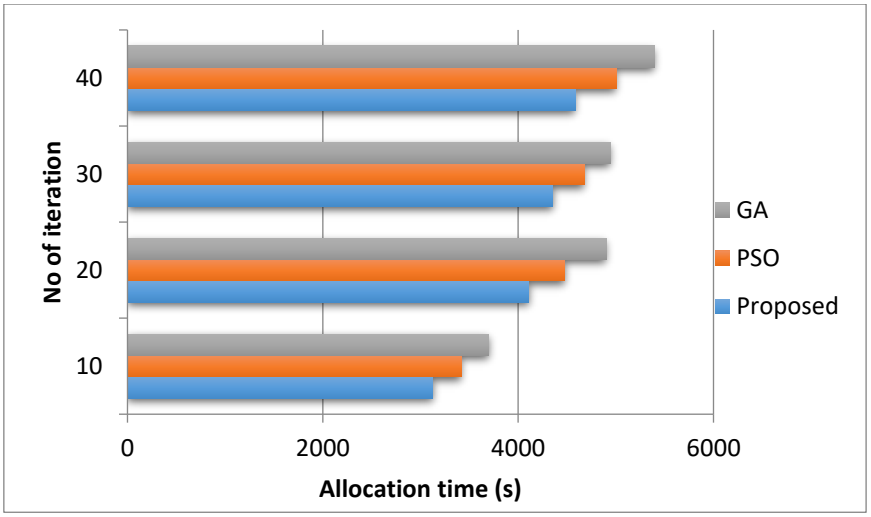

Figure 8.14: Comparison of allocation time of proposed against existing methods.

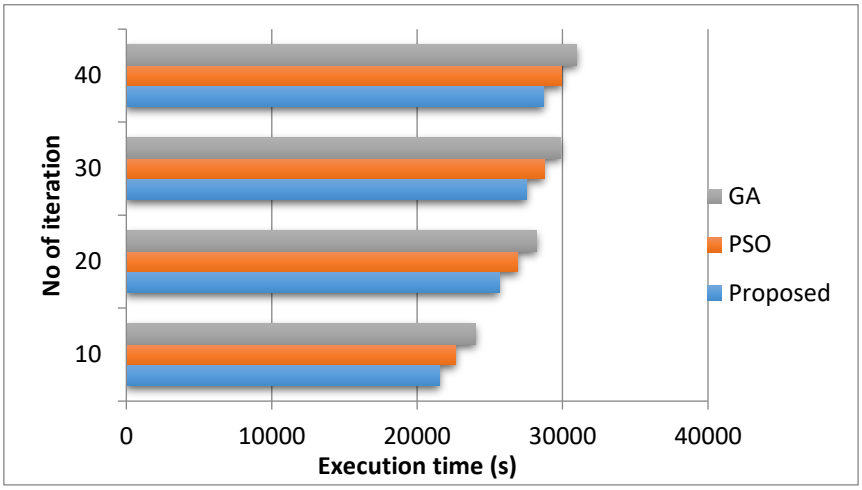

Figure 8.15: Comparison of the execution time of proposed against existing methods.

With the existing PSO and GA techniques, the proposed results are compared for calculating migration cost, resource utilization values, allocation time and execution time for task 200. From the graph, it is obvious that the intended method has better-quality result when matched with the existing ones. The overall percentage of resource utilization value is 55.65% and the overall migration cost of the proposed approach is 22.25$. The overall allocation and execution time of the proposed approach is 4043s and 25856s which is very less than the existing ones.

CHAPTER IX

Conclusions and Future Perspectives

CHAPTER IX

CONCLUSIONS AND FUTURE PERSPECTIVES

Cloud computing (CC) offers a new generation of internet-based computing which is highly scalable and distributed moreover it provides computing resources in the form of service. Elegantly cloud computing is flourishing from an initial notion frame to the significant modern formation. CC has recently emerged as the "Next-Best-Thing" in Information and Communications Technology. In industry and academia wise the CC as a utility paradigm is attaining momentum. By adding modern principles has reinstated the traditional computing technology and it is now the next mutative step of distributive computing. CC offers its providers and user a modern business infrastructure with considerable cost reductions. A lot of organizations with the intension to enlarge their plan at marginal cost and to gain rapid access in the business applications are dependent on the cloud.

Plentiful benefits are provided in the cloud, includes metered services, quick provisioning and stationing, conspicuous elasticity, scalability, flexibility, reasonable catastrophic restoration, rampant network access, data storage solutions, fast renovation of services etc. Multi-tenancy and flexibility are the two key components of the cloud model. Among various tenants Multi-tenancy consents to the allocation of similar service instances. Flexibility in the cloud ability for increasing up and down the resources based on the requirements of the current service. These benefits attract new users from industries to encourage the use of the cloud. When these kinds of services are provided, the cloud offers certain challenges in adapting these services. Considering several aspects of cloud computing, the researchers have done their research in this particular context. In this thesis, several sub-

problems of cloud resource management are carried out along with the approach for solving them.

In this research work, several sub-problems related to cloud security have been studied and various mechanisms have been developed to solve the security issues in the cloud computing environment.

The first chapter gives the introduction to cloud computing and issues in terms of cloud security and the second chapter provides a review of literature. In the third chapter, a novel intrusion detection technique and Authentication process is thoroughly discussed along with its analysis and design of protocol which able to handle security hurdles in terms of the authentication process.

The following points are the main highlights of the third chapter.

- A fake user is avoided by using an OTP based computational process and the proposed policy or mechanism used 3-ways verification scheme which provides a better security policy for the cloud environment.
- A new hybridization approach for the intrusion detection system is proposed to improve the overall security of cloud based computing environment.
- This approach achieved optimal values while tested with certain parameters such as accuracy, precision, recall, TP rate, FN rate and F-1 score under several attacks

To prevent unauthenticated access and the hijacking, a better security scheme is presented in chapter four. The following points explain to minimize the cyber fraud even cyber-crime as well as traffic hijacking.

- A Traffic Hijacking Prevention through Prime Number and Character Stuffing Mechanism is a solution to deal with cyber fraud even cyber-crime as well as traffic hijacking.
- The RSA with character stuffing (RSA-CS) using prime numbers is effectively used to Prevent Hijacking of Cloud Data in which a cryptographic approach named.
- RSA algorithm is modified for better outcomes in perspectives of the cloud environment and comparing the existing stuffing approach, used for network security.

In the fifth chapter, there is a need to ensure secured validation and access control of data/user should be protected during transmission for users in a public IoT-cloud environment. Existing security measures failed by their single level of security, adaptability for a large amount of data and reliability. Therefore, to overcome these issues, a better solution for vulnerable data is suggested.

- To ensure a secured validation of user and to protect data during transmission for users in a public IoT-cloud environment, the KP-ABE with Ban Logic Techniques presented.
- The user authentication is verified. Then the user data is encrypted with the help of KP-ABE algorithm. Finally, data validation and privacy preservation are done by Burrows-Abadi-Needham (BAN) logic.
- The proposed approach attains the high IoT-cloud data security and increases the speed for validation and transmission with high accuracy and used for cyber data science processing.

In Chapter six, an efficient task scheduling and load balancing approach is presented which prevails to be a concern because of the characteristic features of tasks and resources. An enhanced fuzzy ant-bee colony approach is presented to provide better QoS and user preferences.

- An FTOPSIS approach is employed for effective task scheduling and WOA is introduced for load balancing.
- This model controls the admittance of the requests by achieving target QoS in terms of response time. Hence, the admittance is controlled so that the requests which are accepted do not face a delay greater than the time limit stated in the SLA.
- This method increases the throughput of the cloud system by reducing the make span of the cloud scheduling process.
- For security aware scheduling, a Fuzzy Ant Bee Colony (FABC) algorithm is presented. In this approach, it is observed that a task is allocated to the ideal VM based on the QoS and security level of the users. A hive table helps in minimizing the cost, makespan, task migration and security risk moreover the load in the VM is balanced.

As resource management and energy consumption over the cloud data centre recently is becoming a challenging task. Several algorithms for resource allocation and minimization of energy in cloud computing environment which are presented in Chapter Seven.

- The key parameters considered to regulate the performance of SMO are its application time, migration time, and resource utilization.
- Energy consumption is another key factor in cloud computation, and this work adopted the Green Cloud Scheduling Model (GCSM) for the energy utilization of the resources
- Considering the energy consumption and make span optimization models, the SMO approach successfully optimizes resource allocation when evaluated with the prevailing resource allocation algorithms.
- In addition to this, the energy depletion of the resources is minimized by applying a Brownout based Energy model.

Finally, Chapter Eight concentrated on the vital issue in the cloud, i.e. the scheduling for user tasks between Host, Virtual Machines and Data Centers owing to the association of colossal users to fulfill SLA requirement in the cloud computing environment.

- SLA based task scheduling problem is solved by Fuzzy TOPSIS PSO, which considers the weighted sum of energy, cost and execution time as an objective function. Based on these three patterns, the experimental results are attained.
- The proposed approach works positively for many applications and impacts liberally on real-world decision making concerns.
- The experimental outcomes confirmed that the Hybrid Fuzzy TOPSIS-PSO based scheduling approach is apt for task scheduling problems and delivers the higher QoS in contrast to other algorithms.

The future perspectives of the present work in cloud resource management lead to many directions.

- The people in the future will access and share their software applications via online and uses the remote server networks to access information instead of depending on fundamental tools and information present in their personal computers.
- One of the leading research topics is the security issues in cloud computing which is always investigated by the researchers and developers to find appropriate solutions consistently.
- There is a chance to put forward the strategies to deal with specific future challenges like espionage, physical security, data ownership, hypervisor viruses, malicious insiders and transparency in cloud security.

Future of cloud security will witness a boom up in communication technology through the cloud environment. However, it is the people will depend on daily needs and use the cloud

services for their survival. The present research work purely fit to attain best and suitable solutions for the security issues in the cloud. Hence, in the projected domain, the present research work finds an efficient framework for security solutions in the cloud environment.

References

REFERENCES

1. Zhang, Ni, Di Liu, and Yunyong Zhang. “A research on cloud computing security.” In International Conference on Information Technology and Applications, pp: 370-373, 2013.
2. Alqahtani, S.M., Al Balushi, M. and John, R. “An intelligent intrusion detection system for cloud computing (SIDSCC)”, Computational Science and Computational Intelligence (CSCI), International Conference on. pp.135–141, 2014.
3. Alam, Md Imran, Manjusha Pandey, and Siddharth S. Rautaray. “A comprehensive survey on cloud computing.” International Journal of Information Technology and Computer Science, vol. 2, pp: 68-79, 2015.
4. Shahzad, Farrukh. “State-of-the-art survey on cloud computing security challenges, approaches and solutions.” Procedia Computer Science, vol. 37, pp: 357-362, 2014.
5. Zafar, Faheem, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Masoom Alam, and Fuzel Jamil. “A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends.” Computers & Security, vol. 65, pp: 29-49, 2017.
6. Kamboj, Sheenam, and Navtej Singh Ghumman. “A survey on cloud computing and its types.”In 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp: 2971-2974. IEEE, 2016.
7. Ezema, Modesta, and Christian Izuchukwu Nwafor. “Enhancing Cloud Computing Security in the 21st Century Using Advanced Web Technologies”.,2020.
8. Bahram, S., Jiang, X., Wang, Z., Grace, M., Li, J., Srinivasan, D., Rhee, J. and Xu, D., October. “Dksm: Subverting virtual machine introspection for fun and profit”. In 29th IEEE symposium on reliable distributed systems, pp: 82-91, 2010.

9. S. Pisharody, J. Natarajan, A. Chowdhary, A. Alshalan and D. Huang, “Brew: A Security Policy Analysis Framework for Distributed SDN-Based Cloud Environments,” in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp: 1011-1025, 2019.
10. Mall, Shalu, and Sushil Kumar Saroj. “A new security framework for cloud data.” Procedia computer science, vol. 143, pp: 765-775, 2018.
11. Kumar, P. Ravi, P. Herbert Raj, and P. Jelciana. “Exploring data security issues and solutions in cloud computing.” Procedia Computer Science, vol. 125, pp: 691-697, 2018.
12. Barrow, Preeti, Runni Kumari, and R. Manjula. “Security in cloud computing for service delivery models: Challenges and solutions.”Journal of Engineering Research and Applications, vol.6, no. 4, pp: 76-85, 2016.
13. Gibson, Joel, Robin Rondeau, Darren Eveleigh, and Qing Tan. “Benefits and challenges of three cloud computing service models.” In Fourth International Conference on Computational Aspects of Social Networks (CASoN), pp: 198-205. IEEE, 2012.
14. Islam, Sadeka, Jacky Keung, Kevin Lee, and Anna Liu. “Empirical prediction models for adaptive resource provisioning in the cloud.” Future Generation Computer Systems, vol. 28, no. 1,pp: 155-162, 2012.
15. Weingärtner, Rafael, Gabriel Beims Bräscher, and Carlos Becker Westphall. “Cloud resource management: A survey on forecasting and profiling models.” Journal of Network and Computer Applications, vol. 47, pp: 99-106, 2015.
16. Garrison, Gary, Sanghyun Kim, and Robin L. Wakefield. “Success factors for deploying cloud computing.” Communications of the ACM, vol. 55, no. 9,pp: 62-68, 2012.
17. Luong, Nguyen Cong, Ping Wang, Dusit Niyato, Yonggang Wen, and Zhu Han.

"Resource management in cloud networking using economic analysis and pricing models: A survey." IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp: 954-1001, 2017.

18. Johnsen, Einar Broch, Ka I. Pun, and S. Lizeth Tapia Tarifa. "A formal model of cloud-deployed software and its application to workflow processing."In 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp: 1-6. IEEE, 2017.
19. Sridhar S., and S. Smys. "A hybrid multilevel authentication scheme for private cloud environment." International Conference on Intelligent Systems and Control (ISCO), pp. 1-5. IEEE, 2016.
20. Wazid, Mohammad, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, and Joel JPC Rodrigues. "Authentication in cloud-driven IoT-based big data environment: Survey and outlook." Journal of Systems Architecture, vol. 97, pp: 185-196, 2019.
21. Achbarou, Omar, My Ahmed El Kiram, Outmane Bourkoukou, and Salim Elbouanani. "A new distributed intrusion detection system based on multi-agent system for cloud environment. "International Journal of Communication Networks and Information Security, vol. 10, no. 3, pp: 526, 2018.
22. Mishra, Preeti, Emmanuel S. Pilli, Vijay Varadharajan, and Udaya Tupakula. "Intrusion detection techniques in cloud environment: A survey." Journal of Network and Computer Applications, vol. 77, pp: 18-47,2017.
23. Mishra, Preeti, Emmanuel S. Pilli, Vijay Varadharajan, and Udaya Tupakula. "Efficient approaches for intrusion detection in cloud environment." International Conference on Computing, Communication and Automation (ICCCA), pp. 1211-1216, 2016.
24. Islam, Tariqul, D. Manivannan, and Sherali Zeadally. "A classification and characterization of security threats in cloud computing." Int. J. Next-Gener. Comput,

vol. 7, no. 1, pp: 268-285,2016.

25. Amara, Naseer, Huang Zhiqui, and Awais Ali. “Cloud computing security threats and attacks with their mitigation techniques.” International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 244-251, 2017.
26. Subashini, Subashini, and Veeraruna Kavitha. “A survey on security issues in service delivery models of cloud computing.” Journal of network and computer applications, vol. 34, no. 1, pp: 1-11, 2011.
27. Ayak, Suvendu Chandan, Sasmita Parida, Chitaranjan Tripathy, and Prasant Kumar Pattnaik. “An enhanced deadline constraint based task scheduling mechanism for cloud environment.” Journal of King Saud University-Computer and Information Sciences, 2018.
28. Panda, Sanjaya K., Indrajeet Gupta, and Prasanta K. Jana. “Task scheduling algorithms for multi-cloud systems: allocation-aware approach.” Information Systems Frontiers, vol. 21, no. 2,pp: 241-259,2019.
29. Vakilinia, Shahin, Behdad Heidarpour, and Mohamed Cheriet. “Energy efficient resource allocation in cloud computing environments.” IEEE Access, vol. 4,pp: 8544-8557,2016.
30. Usman, M., A. Ismail, H. Chizari, A. Gital, and A. Aliyu. “A conceptual framework for realizing energy efficient resource allocation in cloud data centre.” Indian Journal of Science and Technology, vol. 9, no. 46, pp: 73-82, 2016.
31. Kulshrestha, Sudhanshu, and Sanjeev Patel. “A Study on Energy Efficient Resource Allocation for Cloud Data Center.” In Twelfth International Conference on Contemporary Computing (IC3), pp. 1-7, 2019.
32. Choudhary, Anita, M. C. Govil, Girdhari Singh, and Lalit K. Awasthi. “Energy-efficient resource allocation approaches with optimum virtual machine migrations in

cloud environment." In Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 182-187, 2016.

33. Alsarhan, Ayoub, Awni Itradat, Ahmed Y. Al-Dubai, Albert Y. Zomaya, and Geyong Min. "Adaptive resource allocation and provisioning in multi-service cloud environments." IEEE Transactions on Parallel and Distributed Systems, vol. 29, no. 1, pp: 31-42, 2018.
34. Zhang, Zhenling, Lejian Liao, Hai Liu, and Guoqiang Li. "Policy-based adaptive service level agreement management for cloud services." In IEEE 5th International Conference on Software Engineering and Service Science, pp. 496-499, 2014.
35. Yaghoubi, Mohamadali, and Ali Maroosi. "Simulation and modeling of an improved multi-verse optimization algorithm for QoS-aware web service composition with service level agreements in the cloud environments." Simulation Modelling Practice and Theory, vol.103, pp: 102090, 2020.
36. Zhang, N., Liu, D. and Zhang, Y. (2013) "A research on cloud computing security", Information Technology and Applications (ITA),International Conference On. pp:370 373,2013.
37. Alqahtani, S.M., Al Balushi, M. and John, R. "An intelligent intrusion detection system for cloud computing (SIDSCC)", Computational Science and Computational Intelligence (CSCI), International Conference on. pp:135–141,2014.
38. Alam, Md Imran, Manjusha Pandey, and Siddharth S. Rautaray. "A comprehensive survey on cloud computing." International Journal of Information Technology and Computer Science, vol. 2, pp: 68-79, 2015.
39. Namasudra, Suyel. "An improved attribute-based encryption technique towards the data security in cloud computing." Concurrency and Computation: Practice and Experience, vol. 31, no. 3, pp: e4364, 2019.

40. Sajay, K.R., Babu, S.S. & Vijayalakshmi, Y. “Enhancing the security of cloud data using hybrid encryption algorithm”. J Ambient Intell Human Comput, pp: 1-10, 2019.
41. Awan, Ijaz Ahmad, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, and Allah Ditta. “Secure Framework Enhancing AES Algorithm in Cloud Computing.” Security and Communication Networks, 2020.
42. Manish M. Party, Dr C. A Dhote, Deepak H. Sharma, “ Secure Authentication for Data Protection in CloudComputing using Color Schemes”, International Conference on Computational Systems and Information Systems for Sustainable Solutions, pp. 424-427, 2016.
43. Zeeshan, Imaran Ijaz, “Secure User Authentication in Cloud Computing.”, IEEE, 2013.
44. Chen Chin-Ling, Yang Tsai-Tung, Leu Fang-Yie, Huang Yi-Li, “Designing A Health Care Authorization ModelBased On Cloud Authentication”, Intelligent Automation & Soft Computing; Taylor & Francis,vol.20,no.3, pp. 365-379, 2014.
45. Rabbani, Mahdi, Yong Li Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao, and Peng Hu. “A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing.” Journal of Network and Computer Applications, vol. 151, pp: 102507, 2020.
46. Kavin, Balasubramanian Prabhu, Sannasi Ganapathy, U. Kanimozhi, and Arputharaj Kannan. “An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA.” Wireless Personal Communications, vol.115, pp: 1107-1135, 2020.
47. Sremath Sreenivas Tirumala, Hira Sathu, Vijay Naidu, “Analysis and Prevention of Account Hijacking based incidents in Cloud Environment”,14th International Conference on Information Technology:IEEE, pp. 124-129, 2015.
48. Maghrabi A. Loauai, “The Threats of Data Security over the Cloud as Perceived by

Experts and University Students": IEEE, pp: 1-6, 2014.

49. M. Ali, K. Bilal, S. U. Khan, B. Veeravalli, K. Li and A. Y. Zomaya, "drops: Division and Replication of Data in Cloud for Optimal Performance and Security," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 303-315, 2018
50. Bijayalaxmi Purohit, Pawan Singh, "Data leakage analysis on cloud computing", International Journal of Engineering Research and Applications, vol.3, no.3, pp: 1311-1316, 2013.
51. Sheetal Kalra, Sandeep Sood, "ECC-based anti-phishing protocol for cloud computing services", International Journal of Security and Networks, vol.8, no.3, pp: 130-138, 2013.
52. Y. Chen, L. Wang and C. Liao, "Eavesdropping Prevention for Network Coding Encrypted Cloud Storage Systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 8, pp. 2261-2273,2016.
53. Karuppiah, Marimuthu, Ashok Kumar Das, Xiong Li, Saru Kumari, Fan Wu, Shehzad Ashraf Chaudhry, and R. Niranchana. "Secure remote user mutual authentication scheme with key agreement for cloud environment." Mobile Networks and Applications, vol. 24, no. 3, pp: 1046-1062,2019.
54. Selvarani, P., Annamalai Suresh, and N. Malarvizhi. "Secure and optimal authentication framework for cloud management using HGAPSO algorithm." Cluster Computing, vol. 22, no. 2, pp: 4007-4016, 2019.
55. Kumari, Adesh, M. Yahya Abbasi, Vinod Kumar, and Akber Ali Khan. "A secure user authentication protocol using elliptic curve cryptography." Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, no. 4, pp: 521-530, 2019.
56. Besharati, Elham, Marjan Naderan, and Ehsan Namjoo. "LR-HIDS: logistic regression host-based intrusion detection system for cloud environments." Journal of Ambient

Intelligence and Humanized Computing, vol. 10, no. 9, pp: 3669-3692,2019.

57. Jaber, A.N., Rehman, S.U. FCM–SVM based intrusion detection system for cloud computing environment. Cluster Computing, vol.23, pp: 3221–3231, 2020.
58. Namasudra, Suyel, Rupak Chakraborty, Seifedine Kadry, Gunasekaran Manogaran, and Bharat S. Rawal. "FAST: Fast Accessing Scheme for data Transmission in cloud computing." Peer-to-Peer Networking and Applications, pp: 1-13, 2020.
59. Mishra, Kamta Nath. "Supervising Data Transmission Services Using Secure Cloud Based Validation and Admittance Control Mechanism." In Internet of Things (IoT), pp. 129-149, 2020.
60. Han, Yi, Jeffrey Chan, Tansu Alpcan, and Christopher Leckie. "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing." IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 1, pp: 95-108, 2015.
61. B. Kranmai, Prof. A. Damodaram, "Extenuate DDoS Attacks in Cloud",2nd International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT):IEEE, pp. 235-238,2016.
62. Yan, Qiao, and F. Richard Yu. "Distributed denial of service attacks in software-defined networking with cloud computing." IEEE Communications Magazine, vol. 53, no. 4, pp: 52-59, 2015.
63. Rossi D, Miguel G. Xavier, Rajkumar Buyya, "E-Eco: Performance-aware energy-efficient cloud data center orchestration", Journal of network and Computer Applications: Elsevier, vol. 78, pp. 83-93, 2017.
64. Ehsan Arianyan, Hassan Taheri, Vahid Khoshdel, "Novel Fuzzy multi objective DVFS-aware consolidation heuristics for energy and SLA efficient resource management in cloud data centers", Journal of network and computer applications:Elsevier,vol.78, pp. 43-61, 2017.

65. Zhang Yingjie, “Energy efficiency techniques in machining process: A review”, International journal of Adv Manuf. Technology: Springer, vol.71, pp. 1123-1132, 2014.
66. Fan Yuqu, Hongli Ding, Lusheng Wang, Xiaojing Yuan, “Green latency-aware data placement in data centers”, Computer Networks: Elsevier, vol. 110, pp. 46-57, 2016.
67. Praveenchandar, J., and A. Tamilarasi. “Dynamic resource allocation with optimized task scheduling and improved power management in cloud computing.” Journal of Ambient Intelligence and Humanized Computing, pp: 1-13, 2020.
68. Hanini, Mohamed, Said El Kafhali, and Khaled Salah. “Dynamic VM allocation and traffic control to manage QoS and energy consumption in cloud computing environment.” International Journal of Computer Applications in Technology, vol. 60, no. 4, pp: 307-316, 2019.
69. Hammami Ali, Simoni Noemie and Salman Rasha, “Ubiquity and Quality for Cloud Security”, 41st International conference on parallel processing Workshops, pp. 277-278, 2012.
70. Tao Chen, Xiaofeng Gao and Guihai Chen, “The features, hardware, and architectures of data center networks, A Survey”, Journal of Parallel Distributing Computing: Elsevier,vol. 96, pp. 45-74, 2016.
71. Bansidhar Joshi, Bineet Joshi and Kritika Rani, “Mitigating Data Segregation and Privacy Issues in Cloud Computing”, Proceedings of International conferences on communication and networks, Advances in Intelligent systems and computing: Springer”,vol. 508, pp. 175-182, 2017.
72. M. Durairaj and A. Manimaran, “A Study on Security issues in Cloud based E-Learning”, Indian journal of Science and Technology, vol.8, no.8, pp. 757-765, 2015.
73. D. Aruna Kumari, M. Chandrika and B. Surekha Ratnam Bhardwaj, “Magnified Cipher

Block Chaining Mode using DES to Ensure Data Security in Cloud Computing" Indian journal of Science and Technology,vol.9,no.17,pp:1-7,2016.

74. Abo-alian, A., Badr, N.L., Tolba, M.F. "Authentication as a service for cloud computing". In: Proceedings of the International Conference on Internet of things and Cloud Computing, no.5, pp: 1-7, 2016.
75. Kalra, Sheetal, and Sandeep K. Sood. "Secure authentication scheme for IoT and cloud servers." Pervasive and Mobile Computing, vol. 24, pp: 210-223, 2015.
76. Jana, B., Poray, J. "Performance analysis on elliptic curve cryptography in network security".International Conference on Computer, Electrical & Communication Engineering, pp: 1-7, 2016.
77. Jain, G., Sejwar, V.: "Improving the security by using various cryptographic techniques in cloud computing".International Conference on Intelligent Computing and Control Systems (ICICCS).pp:23-28, 2017.
78. Velásquez, Ignacio, Angélica Caro, and Alfonso Rodríguez. "Authentication schemes and methods: A systematic literature review." Information and Software Technology, vol. 94, pp: 30-37, 2018.
79. Reddy, Alavalapati Goutham, Ashok Kumar Das, Vanga Odelu, Awais Ahmad, and Ji Sun Shin. "A privacy preserving three-factor authenticated key agreement protocol for client–server environment." Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 2, pp: 661-680, 2019.
80. Rifaqat Ali, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah and Mauro Conti. "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring." Future Generation Computer Systems, vol. 84, pp: 200-215, 2018.
81. Limbasiya, Trupil, Mukesh Soni, and Sajal Kumar Mishra. "Advanced formal

authentication protocol using smart cards for network applicants." Computers & Electrical Engineering, vol. 66.pp: 50-63, 2018.

82. Cheng, Long, Dinil Mon Divakaran, Aloysius Wooi Kiak Ang, Wee Yong Lim, and Vrizlynn LL Thing. "FACT: A framework for authentication in cloud-based IP traceback." IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp: 604-616, 2016.
83. Huszti, A., Oláh, N, "A simple authentication scheme for clouds". IEEE Conference on Communications and Network Security (CNS). IEEE, USA, pp: 565-569, 2016.
84. Fang, X., Yang, G, Wu, Y. "Research on the Underlying Method of Elliptic Curve Cryptography". 4th International Conference on Information Science and Control Engineering (ICISCE). IEEE, China, pp: 639-643, 2017.
85. Will, Mark A., Ryan KL Ko, and Silvino J. Schlickmann.: Anonymous Data Sharing Between Organisations with Elliptic Curve Cryptography. IEEE Trustcom/BigDataSE/ICESS, IEEE, Australia, pp: 1024-1031, 2017.
86. Tuan, Dang Minh, and Nguyen Anh Viet. "A new multi-proxy multi-signature scheme based on elliptic curve cryptography." 4th Nafosted Conference on Information and Computer Science, pp: 105-109, 2017.
87. Shaikh, Javed R., Maria Nenova, Georgi Iliev, and Zlatka Valkova-Jarvis. "Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications." IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), pp: 1-4, 2017.
88. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan and W. Li, "SecSDN-Cloud: Defeating Vulnerable Attacks through Secure Software-Defined Networks," in IEEE Access, vol. 6, pp: 8292-8301, 2018.

89. B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu and T. Qiu, “An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing,” in IEEE Access, vol. 4, pp:7899-7911, 2016.
90. M. Al-Fayoumi, S. Aboud, M. Al-Fayoumi and J. A. Saraireh, “An Efficient E-Coin Scheme under Elliptic Curve Cryptography,” International Conference on New Trends in Computing Sciences (ICTCS), Amman, pp: 185-190, 2017.
91. Aujla, Gagangeet Singh, Rajat Chaudhary, Neeraj Kumar, Ashok Kumar Das, and Joel JPC Rodrigues. “SecSVA: secure storage, verification, and auditing of big data in the cloud environment.” IEEE Communications Magazine, vol. 56, no. 1,pp: 78-85,2018.
92. Khajuria, Samant, and Henrik Tange. “Implementation of diffie-Hellman key exchange on wireless sensor using elliptic curve cryptography.” 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, pp: 772-776, 2009.
93. A.N. Jaber and S.U. Rehman, “FCM–SVM based intrusion detection system for cloud computing environment”. Cluster Computing, pp: 1-11, 2020.
94. S.R.K. Tummalapalli and A.S.N. Chakravarthy, “Intrusion detection system for cloud forensics using bayesian fuzzy clustering and optimization based SVNN”. Evolutionary Intelligence, pp: 1-11,2020.
95. R. Vijayanand and D. Devaraj, “A Novel Feature Selection Method Using Whale Optimization Algorithm and Genetic Operators for Intrusion Detection System in Wireless Mesh Network”. IEEE Access,vol. 8,pp:56847-56854,2020.
96. Chen, Junwen, Xuemei Qi, Linfeng Chen, Fulong Chen, and Guihua Cheng. “Quantum-inspired ant lion optimized hybrid k-means for cluster analysis and intrusion detection.” Knowledge-Based Systems, vol. 203,pp: 106167,2020.
97. Ghosh, Joydev, Divya Kumar, and Rajesh Tripathi. “Features Extraction for Network

Intrusion Detection Using Genetic Algorithm (GA).” In Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough, pp: 13-25, 2020.

98. E. Mugabo and Q.Y. Zhang, Intrusion Detection Method Based on Support Vector Machine and Information Gain for Mobile Cloud Computing. IJ Network Security, vol. 22, no.2, pp: 231-241, 2020.
99. Debnath, S., Nunsanga, M. V., & Bhuyan, B. “Study and Scope of Signcryption for Cloud Data Access Control”. In Advances in Computer, Communication and Control Springer, Singapore, pp. 113-126, 2019.
100. Islam, Thouhedul, Rashidah Funke Olanrewaju, and Othman O. Khalifa. “MotionSure: A cloud-based algorithm for detection of injected object in data in motion.” 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA), pp: 1-6, 2017.
101. Lad, Mohit, Ricardo Oliveira, Beichuan Zhang, and Lixia Zhang. “Understanding resiliency of internet topology against prefix hijack attacks.” In 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), pp: 368-377, 2007.
102. Liu, Yujing, Wei Peng, and Jinshu Su. “Study on IP Prefix Hijacking in Cloud Computing Networks Based on Attack Planning.” International Conference on Trust, Security and Privacy in Computing and Communications, pp: 922-926, 2011.
103. Zhang, Daojuan, Yuanfang Guo, Dianjie Guo, and Guangming Yu. “Privacy Leaks through Data Hijacking Attack on Mobile Systems.” In ITM Web of Conferences, vol. 12, pp: 04011, 2017.
104. Casas, Pedro, Alessandro D'Alconzo, Giuseppe Settanni, Pierdomenico Fiadino, and Florian Skopik. “POSTER: (Semi)-Supervised Machine Learning Approaches for Network Security in High-Dimensional Network Data.” In Proceedings of the ACM

SIGSAC Conference on Computer and Communications Security, pp: 1805-1807, 2016.

105. Baitha, Anuj Kumar, and Smitha Vinod. “Session Hijacking and Prevention Technique.” International Journal of Engineering & Technology, vol. 7, no. 2.6, pp: 193-198, 2018.
106. Christina, A. Annie. “Proactive measures on account hijacking in cloud computing network.” Asian Journal of Computer Science and Technology, vol. 4, no. 2, pp: 31-34, 2015.
107. Badr, Aymen Mudheher, Yi Zhang, and Hafiz Gulfam Ahmad Umar. “Dual authentication-based encryption with a delegation system to protect medical data in cloud computing.” Electronics, vol. 8, no. 2, pp: 171, 2019.
108. Kumar, B. Ravi, P. R. K. Murti, and B. Hemantha Kumar. “An Authenticated Bit Shifting and Stuffing (BSS) Methodology for Data Security.” Computer Engineering and Intelligent Systems, vol. 2, no. 3, pp: 94-103, 2011.
109. Liu, Jingwei, Ailian Ren, Lihuan Zhang, Rong Sun, Xiaojiang Du, and Mohsen Guizani. “A Novel Secure Authentication Scheme for Heterogeneous Internet of Things.” International Conference on Communications (ICC), pp. 1-6,2019.
110. Liu, Zhen, Yanbin Pan, and Zhenfei Zhang. “Cryptanalysis of an NTRU-based proxy encryption scheme from ASIACCS’15.” In International Conference on Post-Quantum Cryptography, pp. 153-166, 2019.
111. Mumme, Dean C., Brooke Wallace, and Robert McGraw. “Cloud Security via Virtualized Out-of-Band Execution and Obfuscation.” 10th International Conference on Cloud Computing (CLOUD), pp. 286-293, 2017.
112. Cheema, Rupinder, and Aayush Gulati. “Improving the Secure Socket Layer by modifying the RSA algorithm.” International Journal of Computer Science,

Engineering and Applications, vol. 2, no. 3, pp: 79, 2012.

113. Elrawy, Mohamed Faisal, Ali Ismail Awad, and Hesham FA Hamed. “Intrusion detection systems for IoT-based smart environments: a survey.” Journal of Cloud Computing, vol. 7, no. 1, pp: 21, 2018.
114. Shereek, B. M. Improve Cloud Computing Security Using RSA Encryption With Fermat's Little Theorem. IOSR Journal of Engineering, vol.4, pp: 1, 2014.
115. Alsaleh, M., Mannan, M., & Van Oorschot, P. C. “Revisiting defenses against large-scale online password guessing attacks”. IEEE Transactions on dependable and secure computing, vol. 9, no.1, pp: 128-141, 2012.
116. Elrawy, Mohamed Faisal, Ali Ismail Awad, and Hesham FA Hamed. “Intrusion detection systems for IoT-based smart environments: a survey.” Journal of Cloud Computing, vol. 7, no. 1, pp: 21, 2018.
117. Zhu, Hui, Qing Wei, Xiaopeng Yang, Rongxing Lu, and Hui Li. “Efficient and privacy-preserving online fingerprint authentication scheme over outsourced data.” IEEE Transactions on Cloud Computing, 2018.
118. Abd Latiff, Muhammad Shafie, Syed Hamid Hussain Madni, and Mohammed Abdullahi. “Fault tolerance aware scheduling technique for cloud computing environment using dynamic clustering algorithm.” Neural Computing and Applications, vol. 29, no. 1, pp: 279-293, 2018.
119. Kesavamoorthy, R., and K. Ruba Soundar. “Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system.” Cluster Computing, vol. 22, no. 4, pp: 9469-9476, 2019.
120. Muthurajkumar, S., M. Vijayalakshmi, A. Kannan, and S. Ganapathy. “Optimal and energy efficient scheduling techniques for resource management in public cloud networks.” National Academy Science Letters, vol. 41, no. 4, pp: 219-223, 2018.

121. Thanka, M. Roshni, P. Uma Maheswari, and E. Bijolin Edwin. “An improved efficient: Artificial Bee Colony algorithm for security and QoS aware scheduling in cloud computing environment.” Cluster Computing, vol. 22, no. 5, pp: 10905-10913, 2019.

122. Pang, Shanchen, Wenhao Li, Hua He, Zhiguang Shan, and Xun Wang. “An EDA-GA hybrid algorithm for multi-objective task scheduling in cloud computing.”IEEE Access, vol. 7, pp: 146379-146389, 2019.

123. Gąsior, Jakub, and Franciszek Seredyński. “Security-aware distributed job scheduling in cloud computing systems: a game-theoretic cellular automata-based approach.” In International Conference on Computational Science, pp: 449-462, 2019.

124. Dhamija, Ankit, and Vijay Dhaka. “A novel cryptographic and steganographic approach for secure cloud data migration.” International Conference on Green Computing and Internet of Things (ICGCIoT), pp: 346-351. IEEE, 2015.

125. Thilagavathy.R and Murugan.A, “Secure the Cloud Data Transmission Using an Improved RSA Algorithm”, Indian Journal of Science and Technology, vol.10, no.12, 2017.

126. Dongre, Kirti A., Roshan Singh Thakur, and Allan Abraham. “Secure cloud storage of data.” International Conference on Computer Communication and Informatics, pp: 1-5, 2014.

127. Khare, Mayank Deep, and Chandra Shekhar Yadav. “Secure data transmission in cloud environment using visual cryptography and genetic algorithm: A review.” International Conference on Innovations in Control, Communication and Information Systems (ICICCI), pp: 1-4, 2017.

128. Lin.H.Y, Hsieh.M.Y and Li.K.C, ‘Researches on secure data transmission mechanisms in cloud Internet of Things architectures’, IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing &

Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 2017.

129. Alzubi.J.A, Manikandan.R, Alzubi.O.A, Qiqieh.I, Rahim.R, Gupta.D and Khanna.A, "Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud", Measurement, vol.150, pp: 107077, 2020.
130. Porwal.A, Maheshwari.R, Pal.B.L and Kakhani.G, "An approach for secure data transmission in private cloud", International Journal of Soft Computing and Engineering (IJSCE), pp:2231-2307, 2012.
131. Neela.K.L and Kavitha.V, "Enhancement of data confidentiality and secure data transaction in cloud storage environment", Cluster Computing, vol.21, no.1, pp: 115–124, 2018.
132. Tanweer Alam. "Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework". Journal of Telecommunication, Electronic and Computer Engineering, vol. 12, no.1, 2020.
133. Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A., Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, vol. 7, no.1, pp: 1-29, 2020.
134. Pham, Xuan-Qui, and Eui-Nam Huh. "Towards task scheduling in a cloud-fog computing system." 18th Asia-Pacific network operations and management symposium (APNOMS), pp. 1-4, 2016.
135. Lin, W., Liang, C., Wang, J.Z. and Buyya, R. "Bandwidth-aware divisible task scheduling for cloud computing". Software: Practice and Experience, vol. 44, no. 2, pp.163-174, 2014.
136. Ergu, Daji, Gang Kou, Yi Peng, Yong Shi, and Yu Shi. "The analytic hierarchy process: task scheduling and resource allocation in cloud computing environment." The Journal

of Supercomputing.vol. 64, no. 3, pp: 835-848, 2013.

137. Wang, Tingting, Zhaobin Liu, Yi Chen, Yujie Xu, and Xiaoming Dai. “Load balancing task scheduling based on genetic algorithm in cloud computing.” 12th International Conference on Dependable, Autonomic and Secure Computing, pp. 146-152, 2014.
138. Panda, S.K. and Jana, P.K. “Efficient task scheduling algorithms for heterogeneous multi-cloud environment”. The Journal of Supercomputing, vol. 71, no.4, pp: 1505-1533, 2015.
139. Singh, P., Dutta, M. and Aggarwal, N. “A review of task scheduling based on meta-heuristics approach in cloud computing”. Knowledge and Information Systems, vol.52, no. 1, pp.1-51, 2017.
140. Tawfeek, Medhat A., Ashraf El-Sisi, Arabi E. Keshk, and Fawzy A. Torkey. “Cloud task scheduling based on ant colony optimization.” 8th international conference on computer engineering & systems (ICCES), pp. 64-69, 2013.
141. Jena, R.K. “Multi objective task scheduling in cloud environment using nested PSO framework”. Procedia Computer Science, vol. 57, pp: 1219-1227, 2015.
142. Xavier, VM Arul, and S. Annadurai. “Chaotic social spider algorithm for load balance aware task scheduling in cloud computing.” Cluster Computing, vol. 22, no. 1, pp: 287-297, 2019.
143. Panwar, Neelam, Sarita Negi, Man Mohan Singh Rauthan, and Kunwar Singh Vaisla. “Topsis–pso inspired non-preemptive tasks scheduling algorithm in cloud environment.” Cluster Computing, vol. 22, no. 4, pp: 1379-1396, 2019.
144. Abualigah, Laith, and Ali Diabat. “A novel hybrid antlion optimization algorithm for multi objective task scheduling problems in cloud computing environments.” Cluster Computing, pp: 1-19, 2020.
145. Alazzam, Hadeel, Esraa Alhenawi, and Rizik Al-Sayyed. “A hybrid job scheduling

algorithm based on Tabu and Harmony search algorithms." The Journal of Supercomputing, vol. 75, no. 12, pp: 7994-8011, 2019.

146. Valarmathi, R., and T. Sheela. "Ranging and tuning based particle swarm optimization with bat algorithm for task scheduling in cloud computing." Cluster Computing, vol. 22, no. 5, pp: 11975-11988, 2019.
147. Boutkhoum, Omar, Mohamed Hanine, Tarik Agouti, and Abdessadek Tikniouine. "A decision-making approach based on fuzzy AHP-TOPSIS methodology for selecting the appropriate cloud solution to manage big data projects." International Journal of System Assurance Engineering and Management,vol. 8, no. 2,pp: 1237-1253,2017.
148. L. Shen, J. Li, Y. Wu, Z. Tang and Y. Wang. "Optimization of Artificial Bee Colony Algorithm Based Load Balancing in Smart Grid Cloud". IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Chengdu, China,pp: 1131-1134,2019.
149. Goyal, Tarun, Ajit Singh, and Aakankasha Agrawal. "Cloudsim: simulator for cloud computing infrastructure and modelling". Procedia Engineering, vol. 38, no. 4, pp: 3566-3572, 2012.
150. Senthil Kumar Avinashi Malleswara and Bhaskararao Kasireddi. "An Efficient Task Scheduling Method in a Cloud Computing Environment Using Firefly Crow Search Algorithm (FF-CSA)". International Journal of Scientific & Technology Research, vol. 8, no. 12, 623-627, 2019.
151. Xuan Chen, Long Cheng , Cong Liu , Qingzhi Liu, Jinwei Liu, Ying Mao, and John Murphy. "A WOA-Based Optimization Approach for Task Scheduling in Cloud Computing Systems". IEEE Systems Journal, pp: 1-12, 2019.
152. Mohit Kumar and S.C.Sharma. "Load balancing algorithm to minimize the makespan time in cloud environment". World Journal of Modelling and Simulation, vol.14, no. 4, pp: 276-288, 2018.

153. Karthiban, K., and Jennifer S. Raj. “An efficient green computing fair resource allocation in cloud computing using modified deep reinforcement learning algorithm.” Soft Computing,pp: 1-10,2020.

154. Usman, Mohammed Joda, Abdul Samad Ismail, Hassan Chizari, Gaddafi Abdul-Salaam, Ali Muhammad Usman, Abdulsalam Yau Gital, Omprakash Kaiwartya, and Ahmed Aliyu. “Energy-efficient Virtual Machine Allocation Technique Using Flower Pollination Algorithm in Cloud Datacenter: A Panacea to Green Computing.” Journal of Bionic Engineering, vol. 16, no. 2, pp: 354-366, 2019.

155. Vhatkar, Kapil Netaji, and Girish P. Bhole. “Particle swarm optimisation with grey wolf optimisation for optimal container resource allocation in cloud.” IET Networks, vol. 9, no. 4, pp: 189-199, 2020.

156. Xu, Chenhan, Kun Wang, and Mingyi Guo. “Intelligent resource management in blockchain-based cloud datacenters.” IEEE Cloud Computing, vol. 4, no. 6, pp: 50-59, 2017.

157. Yu, Chunxia, Luping Zhang, Wenfan Zhao, and Sicheng Zhang. “A blockchain-based service composition architecture in cloud manufacturing.” International Journal of Computer Integrated Manufacturing, vol. 33, no. 7, pp: 701-715, 2020.

158. Zhou, Ao, Qibo Sun, and Jinglin Li. “BCEdge: Blockchain-based resource management in D2D-assisted mobile edge computing.” Software: Practice and Experience, 2019.

159. Akintoye, Samson Busuyi, and Antoine Bagula. “Improving quality-of-service in cloud/fog computing through efficient resource allocation.” Sensors, vol. 19, no. 6, pp: 1267, 2019.

160. Devarasetty, Prasad, and Satyananda Reddy. “Genetic algorithm for quality of service based resource allocation in cloud computing.” Evolutionary Intelligence, pp: 1-7, 2019.

161. Remesh Babu, Kaippilly Raman, and Philip Samuel. “Service-level agreement–aware scheduling and load balancing of tasks in cloud.” Software: Practice and Experience, vol. 49, no. 6, pp: 995-1012, 2019.

162. Wei, Jing, and Xin-fa Zeng. “Optimal computing resource allocation algorithm in cloud computing based on hybrid differential parallel scheduling.” Cluster Computing, vol. 22, no. 3, pp: 7577-7583, 2019.

163. Muthulakshmi, B., and K. Somasundaram. “A hybrid ABC-SA based optimized scheduling and resource allocation for cloud environment.” Cluster Computing, vol. 22, no. 5, pp: 10769-10777, 2019.

164. Kumar, AM Senthil, and M. Venkatesan. “Task scheduling in a cloud computing environment using HGPSO algorithm.” Cluster Computing, vol. 22, no. 1, pp: 2179-2185, 2019.

165. Manasrah, Ahmad M., and Hanan Ba Ali. “Workflow scheduling using hybrid GA-PSO algorithm in cloud computing.” Wireless Communications and Mobile Computing, 2018.

166. Tian, Yuan. “A QoS-aware resource allocation framework in virtualised cloud environments.” International Journal of Networking and Virtual Organisations, vol 21, no. 3, pp: 336-350, 2019.

167. Kumari, V. Valli, and P. Ravi Kiran Varma. "A semi-supervised intrusion detection system using active learning SVM and fuzzy c-means clustering." In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 481-485. IEEE, 2017.

168. Sunita, Swain, Badajena J. Chandrakanta, and Rout Chinmayee. "A hybrid approach of intrusion detection using ANN and FCM." European Journal of Advances in Engineering and Technology, vol 3, no. 2, pp.6-14, 2016.

169. Poojitha, G., K. Naveen Kumar, and P. Jayarami Reddy. "Intrusion detection using artificial neural network." In 2010 Second International conference on Computing, Communication and Networking Technologies, pp. 1-7. IEEE, 2010.

170. Liu, Yuan & Wang, Licheng & Shen, Xiaoying & An, Dezhi. “Space-Efficient Key-Policy Attribute-Based Encryption from Lattices and Two-Dimensional Attributes” Security and Communication Networks pp.1-11.2020.

171. Jang, Sung Ho, Tae Young Kim, Jae Kwon Kim, and Jong Sik Lee. "The study of genetic algorithm-based task scheduling for cloud computing." International Journal of Control and Automation, vol 5, no. 4 ,pp. 157-162 ,2012.

172. Al-Maamari, Ali, and Fatma A. Omara. "Task scheduling using PSO algorithm in cloud computing environments." International Journal of Grid and Distributed Computing, vol 8, no. 5, 245-256,2015.

173. Kumar, R. Sathish, and S. Gunasekaran. "Improving task scheduling in large scale cloud computing environment using artificial bee colony algorithm." International Journal of Computer Applications, vol 103, no. 5, 2014.

174. Sheetal, A. Phani, and K. Ravindranath. "Priority based resource allocation and scheduling using artificial bee colony (ABC) optimization for cloud computing systems." International Journal of Innovative Technology and Exploring Engineering” vol 8, no. 6,39-44, 2019.

175. Portaluri, Giuseppe, Stefano Giordano, Dzmitry Kliazovich, and Bernabé Dorronsoro. "A power efficient genetic algorithm for resource allocation in cloud computing data centers." In 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet), pp. 58-63. IEEE, 2014.

176. Zhu, Linan, Qingshui Li, and Lingna He. 147"Study on cloud computing resource scheduling strategy based on the ant colony optimization algorithm." International

Journal of Computer Science Issues (IJCSI), vol 9, no. 5,2012.

177. Mohit Agarwal, and Gur Mauj Saran Srivastava. "A PSO Algorithm Based Task Scheduling in Cloud Computing." International Journal of Applied Metaheuristic Computing (IJAMC), vol.10, no. 4, pp.1-1, 2019.