Analysis and Design of Security Framework for Cloud Computing

SUMMARY OF 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

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.