ENHANCING CLOUD BASED DATA SECURITY THROUGH TRUSTED SECURITY TECHNIQUES

A Summary of Thesis

Submitted to the

Babasaheb Bhimrao Ambedkar University, Lucknow

in Fulfillment of Requirement for the Award of Degree of

Doctor of Philosophy

IN

COMPUTER SCIENCE

BY

Jaydip Kumar

ENROLLMENT NO.- 732/18

UNDER THE SUPERVISION OF

Prof. Vipin Saxena

DEPARTMENT OF COMPUTER SCIENCE

SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

(A CENTRAL UNIVERSITY)

LUCKNOW, UTTAR PRADESH-226 025

2023

SUMMARY

Due to evolution of Amazon Web Services (AWS) in the year 2000, more than 100 applications were developed and later on shifted over the cloud in the year 2006. Further National Institute of Standards and Technology (NIST) introduced the term "Cloud Computing" in the 2011. It is a large and continuously growing technology that has an effect on everyone's daily lives. Additionally, it provides consumers with flexible and affordable on-demand web services, including servers, networks, storage, and software. It is a method that enables storage capacity to be scale up or down as needed without the need to invest in new infrastructure. Cloud computing provides four layers of architecture such as storage layer, which stored data in the cloud data centre; the management layer, which ensures cloud storage privacy and security; the application interface layer, which provides a platform for cloud application services; and finally, the cloud access layer, which gives users access to the cloud. Cloud computing provides security to all the services provided by cloud. But due to technology changes on daily basis and the personal or professional data are generated exponentially. It is a big challenge to provide security to the cloud data. Data owners lose control of their data when transfer it to a cloud data center, it creates a security issue. Security and privacy for cloud data are major issues that need to be solved for cloud computing. Unauthorized access, data loss, and the leakage of user-sensitive data are a few examples of cloud security problems. Data security in the cloud cannot be guaranteed by cloud data encryption. Authentication, encryption, integrity checking, access control, fraud detection, and data masking are security measures that are applicable to cloud data. The

cloud service providers and cloud clients must deal together with a variety of critical matters, including secret key leakage, illegal access, cloud data hiding, password protection, etc.

According to the literature review, the majority of techniques are used to improve the security of cloud data which have not used hybridization of cryptography, the BB84 protocol known as Quantum Key Distribution (QKD) for key exchange, or genetic algorithms for data encryption and decryption. The present work uses keystroke and location-based fuzzy techniques to improve the security of the credit/debit card PIN and One Time Password (OTP) for online transactions.

Data encryption and decryption, data search over large storage, insecure arithmetic operations on data, secrete key exchange, transaction access control using PIN, and transaction access control using OTP are the six security areas are studied in the present work where security solutions can be implemented in cloud computing. Based on these security areas, the current work is divided into eight chapters, each of which contains the solutions to six significant issues that can definitely increase the level of security for cloud data across network channels. Chapter wise summary is given below in brief:

Chapter 1 Introduction

This chapter provides an introduction to cloud computing technology and its importance as a new paradigm of computing. The evolution of the cloud and its classified services are described in detail. It also highlights the important attributes of cloud computing, its strengths, and its weak points. A number of widely accepted and most cited definitions of cloud computing are also given. Cloud computing is a special type of distributed computing in which any type of resource, physical or virtual, can be made available to users, worldwide,

by the use of powerful technology. To provide security of user's or organization's data in cloud storage. The security issues related to cloud computing are identified and elaborated in this chapter.

Chapter 2 Review of Literature

In this chapter previous available research works on cloud data security is deeply discussed. According to the literature, multiple researchers have worked on cloud data security. For understanding the new research problems, a number of reputable magazines, e-books, Wikipedia, books etc. are reviewed. More than one hundred eighty references are used in the present work. Many research articles were reviewed at the initial stages of this research work, and this chapter contains a discussion of more than ten years of research. Different kinds of comprehensive literature have been discussed with respect to every issue resolved in the present work.

Chapter 3 Asymmetric Encryption Scheme to Protect Cloud Data Using Paillier-Cryptosystem

The use of large shared resources is enabled in cloud computing which allows for the storing of information. Major cloud data security issues must be fixed in order to prevent data theft. A cloud security service offers a variety of data encryption methods to secure cloud data in order to prevent data leakage. The calculations on financial information and the security of financial data in cloud storage remain challenging. In the present work, Paillier cryptosystem is used to encrypt financial cloud data in order to increase the security of data. The Paillier cryptosystem uses a homomorphic encryption method and applies mathematical operations on encrypted data. Researchers also use the Paillier cryptosystem to protect decimal digits. In

this chapter, a more advanced Paillier cryptosystem has been proposed for hiding the cloud financial information. The proposed approach improves the security of cloud data. C++ and Python, two separate object-oriented programming languages, are used to implement the technique. The simulated result provides better security for cloud data transfer and also offers the ciphertext with the shortest bit length possible. Additionally, we have examined the two elements of space complexity and time complexities are examined which are represented in the form of tables and graphs.

Chapter 4 Hybridization of Cryptography for Security of Cloud Data

Multiple online security systems used by banks, financial institutions, and other businesses and shifting user's or administrators personal or professional information from servers to the cloud. The different security services are offered by a number of cloud service providers. The fundamental question is data transformation which may be very secure or not. The primary goal of this chapter is to present a hybrid framework which improves the security of cloud data transfer over the internet. The proposed hybrid model combines several extremely secure methods, including the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and DNA Genetic Algorithm. The hybridization of these techniques offers to the cloud users with high integrity, faster computation, and confidentiality.

Chapter 5 Rule-Based Credit Card Fraud Detection Using User's Keystroke Behavior

Online shopping security is one of the most crucial areas for research in the current digital era, for both consumers and business people. Currently, text-based authentication using one-time passwords is unreliable and unable to protect user's transactional information since hackers can quickly compromise it via remote browsing with handheld devices, using hidden

cameras, cloned credit and debit cards, and other methods. In this chapter, keystroke dynamics are used to reduce credit card theft during user online transactions. A rule-based expert system is used to verify the user's identification, and keystroke dynamics are used to monitor activities Personal Identification Number (PIN). The keystroke algorithm allows the service provider to record user activity such as typing speed, time, and pattern without the user's knowledge. No hardware devices need to be installed. The proposed system increases the security of online transactions while still being very cost-effective. The proposed experimental model proved that it reduces credit card theft and increases security when making online purchases.

Chapter 6 Cloud Data Security through BB84 Protocol and Genetic Algorithm

In the current digital world, the virtualization of computing resources has found an effective solution in cloud computing. Even while transferring an organization's data to the cloud has several advantages, the main advantage of cloud computing is its high level of security. The identity theft becomes a crucial element of computing data security. The intruders attack the organization or user's data throughout this process, violating security protocols. When using the cloud platform, the user experiences a feeling of anxiety due to the disclosure of cloud data. The various encryption techniques currently in use cannot defend against such attacks. This chapter introduces the BB84GA security systems, which depend on trustworthy cryptographic methods such attribute-based authentication, the BB84 protocol, and genetic algorithms. The BB84 protocol is used to distribute quantum key between the two parties, and finally the concept of genetic algorithms is utilized to encrypt and decrypt sensitive data between the cloud users. Attribute-based authentication is applied first for identity-based

access control. Hybrid algorithm is a very safe and technically feasible idea. It is a unique algorithm that can be used to reduce the security threats related to cloud computing.

Chapter 7 Fraud Detection through Fuzzy Authentication System for Online Transaction

The purpose of this chapter is to avoid online fraud, especially in the financial industry, by adopting different authentication and authorization protocols at different levels. Using a One Time Password (OTP) that is securely communicated, the proposed authentication method in this chapter uses user authentication. Before the transaction is complete, the GPS location data of both the phone which received the OTP and the location from which it was performed is recorded. Distance was calculated using both GPS coordinates and then utilized as an authentication factor. While the transaction is in progress, the distance, transaction time, and other factors are authenticated using a fuzzy rule-based expert system. Online transactions are authenticated, approved, or rejected based on account status of the Client Financial Control Application (CFCA).

Chapter 8 Secure Data Storage and Retrieval over the Encrypted Cloud Computing

The security of cloud data is used to protecting personal or professional information stored in the cloud storage. Due to the rapid growth of real-time data, the data size in the current digitalized world is increasing from Gigabytes to Terabytes or even Petabytes.

While using cloud computing, the security of cloud data is also an important element. The amount of data in the cloud is increasing significantly, making it difficult to extract the desired or necessary data from the huge amount of storage that is kept online. Our goal is to offer safe authentication while also allowing users to search through encrypted data. To

provide security to the cloud data, we have used fuzzy encrypted keywords search techniques are used to find the desired data from the cloud. The SHA256 hashing technique is used to store the encrypted keyword

Chapter 9 Conclusions and Future Scope of Work

The main objective of each solution provided in the above research work has been achieved by providing the cloud computing environment with a certain level of security. The use of cloud computing increases, demanding the development of new technologies and/or algorithms for various aspects of its security characteristics in order to successfully and gracefully increase both the quality and quantity. This research work, which attempts to provide perfect in the different interconnected areas of cloud computing security while improving existing research and laying the path for future improvements is described.

In the future work, reduction in execution time by using GPU scheduling techniques for the encryption and decryption processes. May be challenging areas for improving the population of genetic sequences to avoid local minima which will improve the fitness function to increase the security of cloud computing data storage.