ANALYSIS AND DESIGN OF EFFECTIVE HYBRID CRYPTOGRAPHICAL 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

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

BY

Pawan Kumar

ENROLLMENT NO. 737/13

UNDER THE SUPERVISION OF

Prof. Vipin Saxena

DEPARTMENT OF COMPUTER SCIENCE

SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

(A CENTRAL UNIVERSITY) (NACC-A++ AECREDATED)

LUCKNOW-226025, UTTAR PRADESH(INDIA)

2024

SUMMARY

Recently, online business has been grown up tremendously and due to appearance of corona virus across the globe, many of the business organizations have shifted the business in the online mode. Further, due to evolution of the bit coin in the year 2009, digital transactions also increased and presently many people are using the transfer of digital currency in the online mode. But, daily, stolen of digital currency by the hackers are also reported by hacking the network or stealing the One Time Password (OTP) or by using the other techniques. Hence, it is a big challenge for secure transfer of digital currency and confidential information in the form of text, audio and video form from one device to another via cloud servers. The cloud data may also be hacked by the hackers through the trapdoor entries or by developing the softwares. Therefore, the present study is based upon the study of different kinds of security algorithms based upon the symmetric or asymmetric techniques and proposed the hybrid-based algorithms for cryptography which may be used for secure transactions of the digital currency. The proposed algorithms have been validated through the concepts of the Finite State Machine (FSM) by developing the security model through Unified Modelling Language (UML). The primary goal of the present work is to keep information in the hidden form from the public and cyber attackers. A key which may be exchanged between the sender and the receiver even in the symmetric encryption is kept hidden from the unwanted party while in the asymmetric cryptography, messages are encrypted and decrypted using a pair of keys. A mathematical process is applied by mixing the various kinds of the algorithms and by proposing the mathematical functions that mixes the data and renders it unintelligible. The present work is based upon the hybrid cryptography which is combination of the two or more cryptographical algorithms and fuzzy concept is also used and entire work is based upon the integration of the Triangular

Membership Function (TMF), Pseudo Random Number Generator (PRNG), Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), Elliptic Curve Integrated Encryption Scheme (ECIES), DNA, Paillier cryptography, Elgamal cryptography and concept of XOR logic gate. The research work provides authentication security such that mutual authentication, fingerprint authentication, session key agreement and two factor authentication. Based on the said security areas, the entire work bounds in the eight chapters in which five important problems have been considered and solved which can certainly increase the security levels in the digital era and chapter-wise summary details are given below in briefs:

Chapter I Introduction

The Chapter I is related to the discussions over the important features used to solve the various problems related to cryptographical techniques which are reported in the present work. The basics of the tools used and development of current technologies, etc are described in brief. The chapter consists of the brief introduction of the symmetric and asymmetric cryptography, hash cryptography, fuzzy logic, pseudo random generator, FSM and UML. Since the entire work is tested through the Python programming language, hence it is also described in brief.

Chapter II Review of Literature

Chapter II deals with the information about the important and useful literature available on the different kinds of the cryptographical techniques. For selection of the research problem, exhaustive review of literature is one of the major tasks, hence this chapter describes all the research papers reported in the literature during the last ten years. From the literature, it is observed that many researchers have done work on cryptographical techniques, but limited work is available on the hybrid cryptography. Based on literature review, the present research work is an attempt to propose the hybrid cryptographical techniques.

Chapter III Fuzzy Rule Based Enhancement of Patten Lock Security System

The Chapter III is related to the study of the Pattern Lock Security System (PLSS) which is used by many customers to lock the digital devices. For the security purpose of the smart device, pattern lock is the most popular security aspect for identification of the valid user. It contains the graphical pattern which may be simple in which all nodes may or may not covered and complex pattern in which all nodes must be covered. In this chapter, a fuzzy based PLSS is proposed which is more secure than the normal PLSS. It is based upon the pseudo random number generator and Elgamal cryptography is used for the security of the proposed PLSS.

Chapter IV Secure Transaction of Indian Currency Through Biometric Technique

Chapter IV deals with the secure transaction of the currency across the network connected with high-speed internet facilities. It is a very crucial tasks and many researchers provide many solutions but there are many loopholes for theft of currency. For the security purpose, fingerprint authentication and cryptography technique based on Indian Aadhar card are used for currency transaction.

Chapter V Secure Transaction of Digital Currency Through Fuzzy Based Cryptography

Internet technology is growing at a very fast rate around the globe and many of the countries are performing currency transaction through online mode. Due to increment of transaction of currency in an exponential manner, there is a need to include proper security features so that hackers or intruders could not hack the digital transaction carrying out between the two parties. A new model using Unified Modeling Language (UML) has proposed, which is developed in the hybrid mode with a combination of fuzzy rule-based computation, fingerprint authentication, Hash and Elgamal cryptography. The hybrid method is applied for secure transaction of the digital currency. The fuzzy rule based computation is used

with Triangular Membership Function (TMF), which is based on current date and time. Fuzzy value creates a secret key and encrypts through Hash algorithm. Elgamal cryptosystem is used for encryption and decryption. The results obtained through hybrid method are tested through the concept of Finite State Machine (FSM) by generating the various test cases. The results obtained through hybrid method are tested through the concept of FSM by generating the various test cases. In this work, mutual authentication as well as time stamp is also considered and the presented hybrid approach is based upon two-way authentication between client and user which is found to be very effective and may be used by the software industries for the customers especially related to the banking sectors.

Chapter VI Information Exchange via Hybrid Cryptography

Due to rapid growth of digital communication in the recent days, it is important to secure the confidential information in the form of text, audio and video files from the intruders, therefore, the Chapter VI is based upon the new concept of hybrid cryptographical algorithm which is explored by combining the Advance Encryption Standard (AES), Rivest, Shamir, Adleman (RSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) for digital communication of confidential information passed from one device to another device and computed results are presented in the form of tables and graphs.

Chapter VII Hybrid Cryptography for Security Key Exchange through AES and Paillier

Chapter VII deals with the information and key exchange over the internet communication channel with the help of hybrid cryptography. The cloud computing is gaining popularity among the users as the cloud servers are arranged through the dynamic topological structures. The main aim of every user is to transmit secure information from one device to another device via using high speed internet connectivity. The key is an important component for any cryptography algorithms. If the key is breached by the cyber attacker,

then the cyber attacker encrypts the confidential message. In symmetric cryptographic, only one key is used for encryption and decryption, and it has weakness of symmetric cryptography. So, the problem can be solved by proposing Advanced Encryption Standard (AES) which is symmetric cryptography and Paillier system which is a asymmetric cryptography are used. The private key of AES is encrypted by Paillier cryptography. The message is encrypted by private key of AES cryptography and the private key of AES is encrypted by the public key of Paillier cryptography.

Chapter VIII Nested Level of Hybrid Cryptographical Technique for Secure Information Exchange

The multi-level security is provided by DNA and Paillier cryptography. In the multi-level security, the proposed methodology performs two times encryption and two times decryption. Hybrid cryptography provides better solution than single type of cryptographical techniques. In this chapter, nested level of hybrid cryptographical technique is investigated with the help of Deoxyribonucleic Acid (DNA) and Paillier cryptographical techniques. In the first level, information will be encrypted by DNA and at the second level, the ciphertext of DNA will be encrypted by Paillier cryptography. At the decryption time, firstly Paillier cryptography will be processed then DAN cryptography will be processed to get the original text. The proposed algorithm follows the concept Last Encryption First Decryption (LEFD) at the time decryption. It is observed that the proposed methodology provides high efficiency and number of bits more than previous algorithm. The computed results are depicted in terms of tables and graphs.

Chapter IX Conclusions and Future Scope of Work

The last chapter i.e., Chapter IX is related to the major findings of the proposed work and future directions to further extension of the work. From the above major work reported in the four chapters, it is concluded that the UML is a powerful modelling language used to

propose object-oriented system model. The hybridization of the various kinds of cryptographical algorithms produce excellent efficiency in comparisons of the existing algorithms available in the literature. It is proved through comparisons with the previous work. In the recent days, cloud security is one of the major concerns, hence it is recommended to apply various cryptographical algorithms to form new hybrid algorithms which may be used to save the data of cloud servers from the intruders.