A Study and Implementation of Fuzzy Cryptographical Techniques Across Distributed Network

SUMMARY

of

THESIS

SUBMITTED TO

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

LUCKNOW

BABASAHEB
BHIMRAO
AMBEDKAR
UNIVERSITY

LUCKNOW

प्रज्ञा शील करुणा

ESTABLISHED 1996

FOR THE DEGREE OF

Doctor of Philosophy

IN

COMPUTER SCIENCE

Submitted by

Rashmi Singh

Enrollment No. – 955/13

Under the Supervision of

Prof. Vipin Saxena

DEPARTMENT OF COMPUTER SCIENCE
SCHOOL FOR INFORMATION SCIENCE & TECHNOLOGY
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY; NAAC- 'A' GRADE)
VIDYA VIHAR, RAEBARELI ROAD, LUCKNOW-226 025 (U.P.), INDIA

2018

SUMMARY

In routine life of human being and due to E-commerce applications, the usage of internet is very common over worldwide. The rapid growth in electronic transactions has result a great desire for fast and valid user identification as well as authentication. In this aspect, data security is the most critical and important issue for the safety of information through the internet. Network security related issues are now becoming most important because the society is moving towards the digital information age. Network security and cyber crimes are reversible to each other as more users connect to the internet, it attracts a lot of cyber crime. The network information is controlled by the network administrator. The task of network security is not only to secure the end systems but also to provide the security to the entire network.

In the present era, cryptography is used to provide the security of digital data across the distributed network. The purpose of data security is to provide secure data transmission over the unreliable network. Network security involves authentication of access to the data which is controlled by the network administrator. Fuzzy logic and cryptography together provide the security in the field of network security. The key formed by fuzzy logic is in the form of a function which is hard to break. Therefore, content data would be used as an input data for cryptography so that the data become unreadable for the unauthorized users and the data will remain same from them. Network security covers a variety of computer networks, both private and public that is used in routine transactions and communications.

The use of fuzzy logic provides more accurate results as compare to boolean algebra. The applications of fuzzy logic are implemented at every step of fuzzy transportation mechanism which is employed for optimized data flow across the distributed network.

Fuzzy inference system is employed for effective decision making in data distribution process and other applications. Fuzzy logic deals with vague, ambiguous and unclear nature of sophisticated system. Fuzzy logic also provides an alternative to the mechanism of probability, probably which is suitable for software credibility.

In this present study, the concept of network security and cryptography is introduced and discussed the state of art in real life applications using cryprographic applications. We have analyzed few noval and efficient cryptographic security techniques, fuzzy set and fuzzy inference system techniques while facilitating new modified algorithms. The main focus of the present study is to provide cryptographic security in real life applications across distributed networks in such a way that enhance security level can be achieved while providing optimal cost.

This work is also related to propose a model which is based upon the object-oriented technology for occurring of cyber crime across the distributed network. A well known Unified Modeling Language is used and one can easily write the code for implementation of model in any object-oriented programming language. The chapter-wise summary of the present work is given below in brief:

CHAPTER I INTRODUCTION

An approach of cryptography and fuzzy logics is described in the present work. Therefore this chapter deals with the concept of cryptography and tools that are needed for implementing the system. The confidentiality of the files was maintained while providing the access to the trusted user in any organization. By this, the data has been accessed only through authorized person. The confidentiality, availability and integrity of the data were maintained through trusted users but the unauthorized person attacks the security network

like data manipulation, retransmission of data, service malfunction, simulation etc. So, the use of cryptography techniques, fuzzy inference system and fuzzy logic, is to make the process secure and efficient while in some cases maintaining the optimal cost across distributed network.

CHAPTER II REVIEW OF LITRATURE

The present chapter described the review of literature related to fuzzy rule based systems and cryptographical techniques in distributed network. In this specific area, very few works are described therefore the present work is an attempt in the direction of fuzzy cryptographical techniques and fuzzy rule based systems. The relevant literature review on cryptographical techniques and fuzzy rule based systems for various aspects in distributed network are summarized in this chapter. Fuzzy cryptography is very useful technique and the few advantages of fuzzy cryptographic techniques are supply chain management, transportation and software security in distributed networks. All the important research papers, review papers, book chapters and books are described in this chapter in brief.

CHAPTER III FUZZY RULE-BASED INFERENCE SYSTEM

In this chapter, fuzzy rule based inference system was implemented on naval military mission. On a military mission, the choice of changing unit requires complicated judgments like data about the well being status of the hardware and natural conditions. The fuzzy rule based inference system help in the choice about changing a unit to a mission using the methods of fuzzy concepts. A numerical application is also introduced to demonstrate the validity of above said approach. The contents of this chapter have been

published in International journal of Computer Network and Information Security (IJCNIS), Vol.10, No.4, pp. 28-37, 2018.

CHAPTER IV FUZZY DATA TRANSFER APPROACH IN DISTRIBUTED NETWORK

In this chapter, a new data transfer approach using fuzzy Vogel's Approximation Method (VAM) was introduced along with a new ranking based approach for fuzzy transportation problem. The fuzzy VAM gives the optimal solution while taking less number of iterations for fuzzy transportation in comparison to Vogal's Approximation Method (VAM). On the other side a fuzzy ranking based approach was used to solve the fuzzy transportation problem in which the trapezoidal fuzzy numbers were represented the transportation cost, availability and demand of the product. The contents of this chapter have been published in Computer Modelling &New Technologies, Vol. 21, No. 4, 2017, and International Journal of Advance Research in Computer Science, Vol. 8, No. 3, 2017.

CHAPTER V CRYPTOGRAPHIC SECURITY FOR MAC ADDRESS IN DISTRIBUTED ENVIRONMENT

In this chapter, an approach for secure transfer of information along with MAC address is depicted with well known algorithm Rivast, Shamir and Adleman (RSA). In this study, the algorithm is tested on various MAC address through object oriented JAVA programming language. UML approach was also introduced for the making of cryptosystem model. The contents of this chapter have been published in International journal of Computer Applications Vol. 131, No. 12, 2015.

CHAPTER VI A UML MODEL FOR OCCURRENCE AND RESOLVING OF CYBER CRIME

In this chapter, the model is proposed which is based upon the object oriented technology for occurring and resolving the cyber crime approach through Unified Modeling Language (UML) across distributed network. UML is used for this purpose by which one can easily write the code for implementation of this model in any object oriented programming language. The contents of this chapter have been published in Information Systems Design and Intelligent Systems and Computing, Vol. 433, Springer proceedings, 2016.

CHAPTER VII MINIMIZATION OF CYBER ATTACKS THROUGH OPTIMIZATION TECHNIQUES

In this chapter, a technique was presented which enumerates the minimization of cyber crime through optimization technique. An algorithm named Hungarian technique with state transition deterministic finite automation is used and different test cases were provided for the evaluation and validation of the results using UML. The contents of this chapter have been published in International journal of Computer Applications, USA, Vol. 99, No.1, 2014.

CHAPTER VIII CONCLUSIONS AND FUTURE SCOPE

This thesis includes data related to fuzzy cryptography in distributed network. Fuzzy logic and UML were also used. This work has been done for transportation problem, naval military system, MAC address security in data transfer, minimize the cyber crime and in future this work can be implemented for real life applications such as biometric based cryptographic security, supply chain management, communication, E-commerce applications, etc. In future by implementing other cryptographic techniques we can secure

the data across the distributed network. The above work can be further extended in the field of data mining, where the huge amount of database of different kinds is available on the system.