ANALYSIS AND DESIGN OF SECURITY MANAGEMENT TECHNIQUES IN CYBER ENVIRONMENT

SUMMARY

of

THESIS

SUBMITTED TO

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

LUCKNOW

BABASAHEB
BHIMRAO
AMBEDKAR
UNIVERSITY

FOR THE DEGREE OF

Doctor of Philosophy

IN

COMPUTER SCIENCE

Submitted by

Priyanka Chaudhary

(Enrollment No. 949/13)

Supervisor

Dr. Narander Kumar

DEPARTMENT OF COMPUTER SCIENCE
SCHOOL FOR INFORMATION SCIENCE AND TECHNOLOGY
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
VIDYA VIHAR, RAE BARELI ROAD, LUCKNOW-226 025

2018

SUMMARY OF THESIS

The Information and Communication Technology (ICT) industry has emerged and evolved in last five decades. The technology is gaining popularity and becoming essential to each and every one. The Information and Communication Technology (ICT) device and parts are usually related and disturbance of one might also have an impact on several others. In the course of recent years, specialists and policy makers have expressed their concerns to cyber-attacks and suggest protecting ICT frameworks from such attacks, which numerous specialists worry that it may recur and seriously threaten the industry at large.

A cyber security can be a valuable term but there are still ambiguities regarding its definition. It is also sometimes improperly conflated with different ideas, for example, security, data sharing, insight social occasion, and surveillance. Be that as it may, cyber security can be a vital tool in ensuring security and averting unapproved observation and data sharing.

The study of risk to management of data is essential to an effective cyber security. The risk associated to any attack depends upon three factors: threat, vulnerabilities and impacts. Almost all cyber-attacks have limited impact, but a successful attack on a few aspects of critical infrastructure, most of which is held by the private sector and the livelihood and safety of individual citizens. Alleviating such threats often include reducing risk sources, acknowledging vulnerabilities, and reducing impacts.

CHAPTER I

INTRODUCTION

This chapter provides an introduction of cyber security and its importance in the cyber environment. Research motivation, scope, problem of statement, cyberspace and attribute of cyberspace is described in detail. The essential feature of cyber security and challenges of security is elicited. We have explored different types of broadly accepted definitions of cybercrime and categorizations of cybercrime are also given. A detailed discussion on the importance of security management in cyber environment is given and main objectives of the research work are explained.

CHAPTER II

REVIEW OF LITERATURE

This chapter describes the literature surveyed on security issues in the cyber world. Various software professionals and researchers are using the cryptography algorithm created for solving the complex security problems. There is a great deal of research on the cryptographic algorithm, but very few consider unified modeling system. A structured approach is taken to search various journals, e-books, Wikipedia, online journals, etc. are consulted for finding prior works in this area.

CHAPTER III

AWARENESS ABOUT CYBER CRIME AND PREVENTION TECHNIQUE

This chapter presents an overview of cybercrime i.e. how to make people aware of cybercrime through technology it also examines different issues of cybercrime through personal interaction, as well as emphasizes the severity of this problem.

Finally, it also discusses the prevention techniques by which we can minimize the cybercrime.

CHAPTER IV

MINIMIZE LOSSES OF DATA DUE TO CYBERCRIME

In this chapter, we present an enumeration technique by which we have reduced cyber losses during the cybercrime in the cyber environment. In this approach, we have obtained an optimal result. This is based on the primary data and personal interaction. We have also discussed Hungarian and Branch and Bound algorithm with state transitions and deterministic finite automation. Various test cases are generated to assess and validate the results of the algorithm that calculate the total cost of cybercrime.

CHAPTER V

REDUCING IDENTIFIED THEFT

In this chapter, we have proposed an algorithm which is established on the ASCII value to encode a plain text. In this algorithm we have generated a key in randomly manner for a person which is length equivalent to that of the plaintext. A dynamic modification using randomly generated number is done in the randomly modified key through substitution of position of the key and it is used to decrypt original plaintext message. We have used Java Net Beans IDE 8.0 to develop the GUI for this purpose. A computer having Intel Core i3 CPU and 1GB RAM has been used to obtain the outcomes.

CHAPTER VI

PREVENTION AND DETECTION OF ONLINE TRANSACTION FRAUDS

This chapter provides the prevention technique to safeguard from Hackers and Trackers while transaction online. Detection of fraud on credit cards as well as

other online facilities which are provided by the different companies or organizations is a high importance for the organization and their customers. If such fraudulent transactions are prevented, companied will benefit by mitigating huge penalties and associated with unauthorized accesses. We have come with a changed RSA algorithm with the use of bit stuffing whose main objective is to enhance the level of security in on-line transaction.

CHAPTER VII

AVOIDANCE CYBER STALKING

Cyber Stalking is an example of a pattern in which a stalker looks to access, or control over a victim. Such activities range from the favorable to the harmful and should induce enthusiastic misery or harm to the victim. This chapter focuses on aspects of upgradation of the security, diminishing the issues of cyber stalking. We have proposed technique using BCRYPT algorithm with Rail Fence Technique and BCRYPT with AES algorithm. We have used Java Net Beans IDE 8.0 to develop the GUI for this purpose. A computer having Intel Core i3 CPU and 1GB RAM has been used to obtain the outcomes.

CHAPTER VIII

PREVENTION AGAINST PHISHING ATTACK

The Phishing attack is a well-known cyber-attack which is becoming popular with the growth of mobile industry. Thus, protecting cell phone users from phishing attack is very crucial particularly in mid-range cell phone users because these users are easy targets of attackers while mid-range cell phones device do not assist feature like mobile antivirus anti-phishing software. This chapter intends to

develop computer learning based mobile phishing detection system on mobile to become aware of malware applications. This main objective of this work is to detect mobile phishing and prevent data loss and sensitive information leakage.

CHAPTER IX

CONCLUSION AND FUTURE WORK

This chapter is devoted to present the conclusions of the research work and future work in the area of cyber security management. Efficient management in cyber world is an interesting area of research. In the present work, several sub-themes in the cyber security management have been studied and different frameworks are developed for solving them. They are

- Awareness about Cybercrime and Prevention Technique
- Minimize Losses of Data Due to Cybercrime
- Reducing Identified Theft
- Prevention and Detection of Online Transaction Frauds
- Prevention against Phishing Attack
- Avoidance Cyber Stalking

The techniques used in the frameworks are scalable and dynamic in nature and may efficiently manage the cyber environment as suggested by the results. This work can be extended in the direction of security management for interoperable cyber world where users can increase the security level using other different types of algorithm present in today's cyber environment.