RANSOMWARE DETECTION AND FORENSIC ANALYSIS

seminar report submitted
in partial fulfillment of the requirement for award of the degree of

Bachelor of Technology
in
Computer Science & Engineering

By

AKSHAYA K V (20UECS0423)
D HEMANSAKTHIVEL (20UECS0372)

Under the guidance of
Dr. MANU V T, M.Tech,PhD.,
Associate Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SCHOOL OF COMPUTING

VEL TECH RANGARAJAN Dr.SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University Estd u/s 3 of UGC Act, 1956)
CHENNAI 600 062, TAMILNADU, INDIA

June, 2022

BONAFIDE CERTIFICATE

It is certified that the work contained in the seminar report titled " RANSOMWARE DETECTION AND FORENSIC ANALYSIS " by " AKSHAYA K V (20UECS0423) D HEMANSAKTHIVEL (20UECS0372) " has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Signature of Supervisor

Dr. Manu V T

Associate Professor

Computer Science & Engineering

School of Computing

Vel Tech Rangarajan Dr.Sagunthala R&D

Institute of Science and Technology

June, 2022

Signature of Head of the Department

Dr. V. Srinivasa Rao

Professor & Dean

Computer Science & Engineering

School of Computing

Vel Tech Rangarajan Dr.Sagunthala R&D

Institute of Science and Technology

June, 2022

DECLARATION

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature)

AKSHAYA K V

Date: / /

(Signature)

D HEMANSAKTHIVEL

Date: / /

APPROVAL SHEET

This seminar report is entitled as RANSOMWARE DETECTION AND FORENSICS ANALYSIS by AKSHAYA K V (20UECS0423), D HEMANSAKTHIVEL (20UECS0372), is approved for the degree of B.Tech in Computer Science & Engineering.

Signature of Supervisor

Dr. Manu V T

Associate Professor

Computer Science & Engineering

School of Computing

Vel Tech Rangarajan Dr.Sagunthala R&D

Institute of Science and Technology

Signature of Seminar Handling Faculty

Dr. N R Rajalakshmi

Professor

Computer Science & Engineering

School of Computing

Vel Tech Rangarajan Dr.Sagunthala R&D

Institute of Science and Technology

Date: / /

Place: Chennai

ACKNOWLEDGEMENT

We express our deepest gratitude to our respected **Founder Chancellor and President Col. Prof. Dr. R. RANGARAJAN B.E. (EEE), B.E. (MECH), M.S (AUTO). DSc., Foundress President Dr. R. SAGUNTHALA RANGARAJAN M.B.B.S.,** Chairperson Managing Trustee and Vice President.

We are very grateful to our beloved **Vice Chancellor Prof. S. SALIVAHANAN, Ph.D.,** for providing us with an environment to complete our seminar successfully.

We record indebtedness to our **Professor & Dean, Department of Computer Science & Engineering Dr. V. SRINIVASA RAO, M.Tech., Ph.D.,** for immense care and encouragement towards us throughout the course of this seminar.

We take this opportunity to express our gratitude to Our Internal Supervisor **Dr. MANU V T, M.Tech.,PhD.,** for his/her cordial support, valuable information and guidance, he/she helped us in completing this seminar through various stages.

A special thanks to our **Seminar Coordinator Dr. G. TAMILMANI, Ph.D.,** for her valuable guidance and support throughout the course of the seminar.

We thank to our **Seminar handling Faculty Dr. N R RAJALAKSHMI ,M.E.,PhD.,** for the valuable information shared in proceeding with our seminar.

We thank our department faculty, supporting staff and friends for their help and guidance to complete this project.

AKSHAYA K V (20UECS0423)
D HEMANSAKTHIVEL (20UECS0372)

ABSTRACT

Ransomware is a type of malware that prevents its victims from accessing their own data until they pay a ransom.The Ransomware is secretly installed on our systems and locks the system down.That lockdown is inevitably accompanied by a message demanding payment if the systems owner ever wants to access the files again.Everything important on your hard drive will be effectively lost to you,unless you pay up.This type of malware has direct financial implication, which has promoted an ecosystem of cybercriminals.Ransomware as a service (RaaS) is a service that allows the easy acquisition of ransomware codes at a price.This indicates that cooperation exists among criminals.One party is responsible for developing and creating the ransomware code, while another party is responsible for organizing the dissemination of the infection or an attack campaign, and both parties enjoy the profit from a successful attack. Ultimately, this will promote specialist criminals that authorities will find difficult to tackle.

Keywords: Acquisition, Encryption, Malware, Ransonware

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

GPS	Global Positioning system
IPS	Intrusion Prevention System
OS	Operating System
RaaS	Ransomware as a service

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Introduction

Being in this generations it is a fashion to use computers connected via the Internet. Objective ransomware is to block its victim from accessing their own resources by locking the OS or encrypting targeted files that seem valuable to the victim. Basically, there are two types of ransomwares - locky and crypto. Locky ransomware locks the entire system from access by its user, but it is usually easy to resolve. Crypto ransomware uses encryption technology to lock selected files from user access; this is much more difficult to resolve and the damage caused may be irreversible.

1.2 Aim of the Seminar

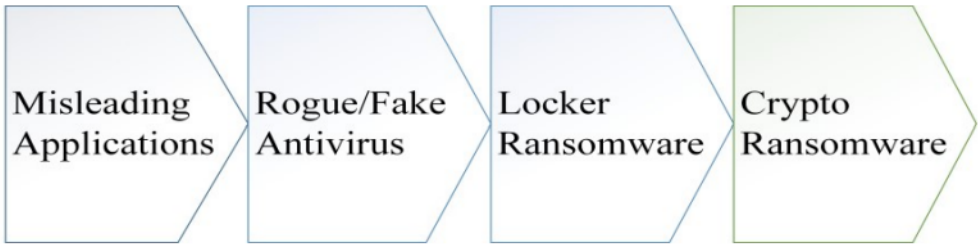
This seminar will help to know about ransomware attacks and to secure network. Prevent future ransomware attacks and present the current techniques used for the analysis and the detection of ransomware.

1.3 Scope of the Seminar

The scope of this seminar is to detect the Ransomware detection various types of Ransomware attacks we are facing now a days. In this seminar it explain detailed study of Ransomware attacks and how to detect the malware attacks. Main aim of this seminar is to protect our system from Ransomware attack.

1.4 Methodology

Ransomware evolution has been significantly influenced by a range of developments in technology, economics, security and culture. Similar to any real-life ecosystem, this threat has evolved and adapted to its surroundings to survive and even thrive. Those threats that cannot or do not adopt may eventually disappear. This Ransomware world is a significant example of evolution in action or Darwinian-style evolution, as shown in Fig 1.



1.4 Ransomware Evolution

Chapter 2

LITERATURE REVIEW

Giorgio valenziano Santangelo et al has proposed to prevention and detection of ransomware two relevant cases of ransomware . [1]

A.H.Mohammad has proposed system to ransomware evolution growth and recommendation for detection. [2]

Llker Kara et al has proposed the cyber fraud detection and behavior analysis of the crypto-ransomware attack . [3]

Kul prasad Subedi et al has proposed the forensic analysis of ransomware families using static and dynamic analysis. [4]

R. Richardson et al has proposed the ransomware evolution, mitigation, prevention and existing techniques to prevent and mitigate ransomware attacks. [5]

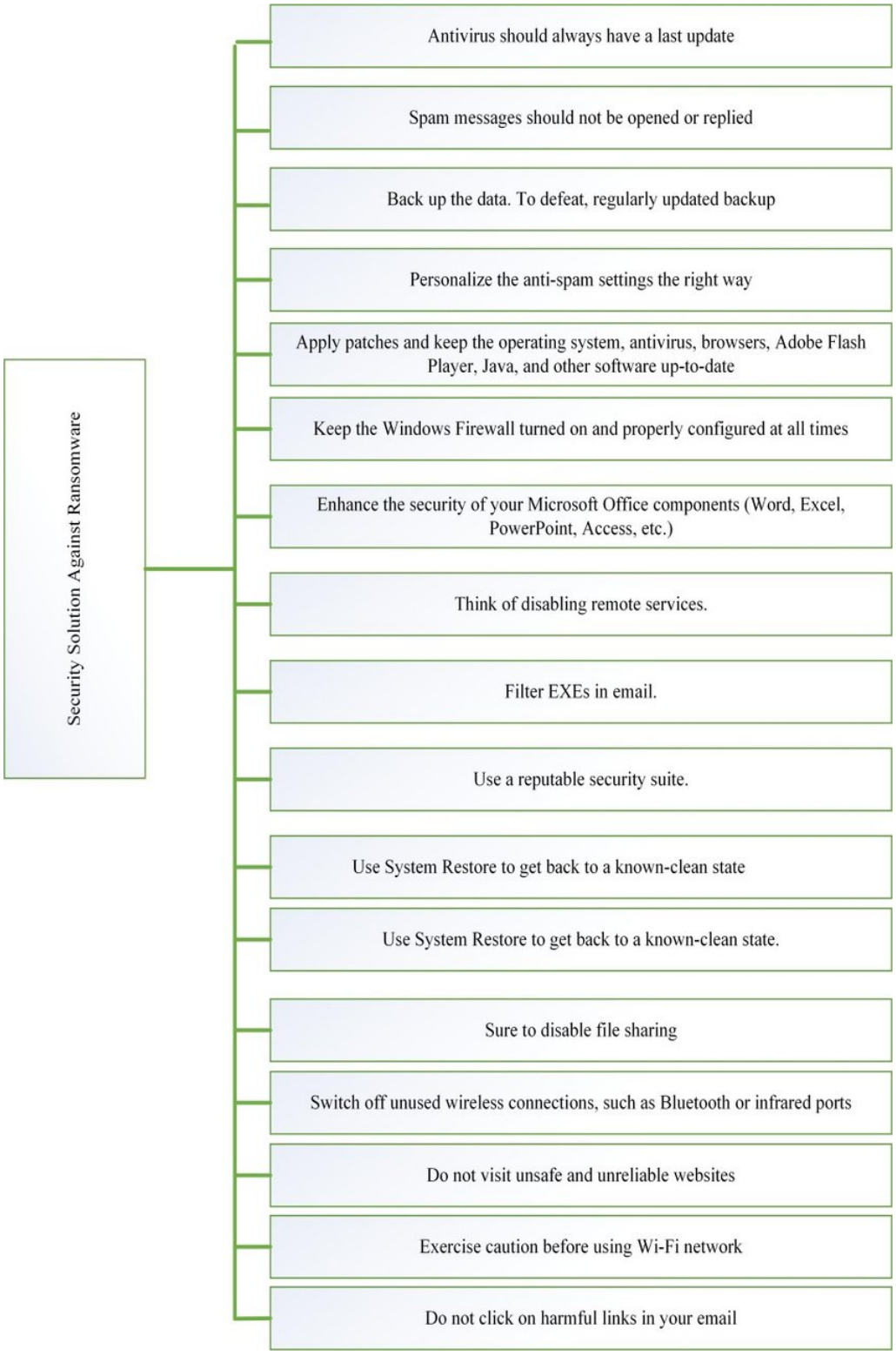
D. Gonzalez et al has proposed to detection and prevention of crypto-ransomware and safeguards are listed as well. [6]

Chapter 3

SEMINAR DESCRIPTION

3.1 Existing System

The most commom technique as a solution to prevent and mitigate the nightmare of Ransomware attack, which is the most critical attack in 2017. This attack has affect several large infrastructures in the world. If we survived the open position for the security developers and research till this time. It shows massively increased the marked security consultant and developer in world wide. That indicates something really critical happen in internet security world and need immediate action against it.



3.1 Current-Security-Solution-against-Ransomware

Advantages

- Ensures that our system is protected before the malware gets to destroy and encrypt all our files.
- Early Detection
- Risk mitigation
- Data protection
- Network Defenses to prevent ransomware from communicating with Command Control Centers.

Disadvantages

- Victims are at risk of losing their files, but also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications.
- Even when you pay ransomware, the tools provided by the ransomware hacker may not immediately recover your data.

3.2 Feasibility Study

Countermeasures that free victims of ransomware attacks from paying the cyber-criminals are discussed. These were achieved by exploiting the weakness of the working operation of the malware, and intercepting calls made to Microsoft's Cryptographic API respectively. Useful information can be obtained from system API packages. These packages can be used to define applications without any prior knowledge of user-defined content.

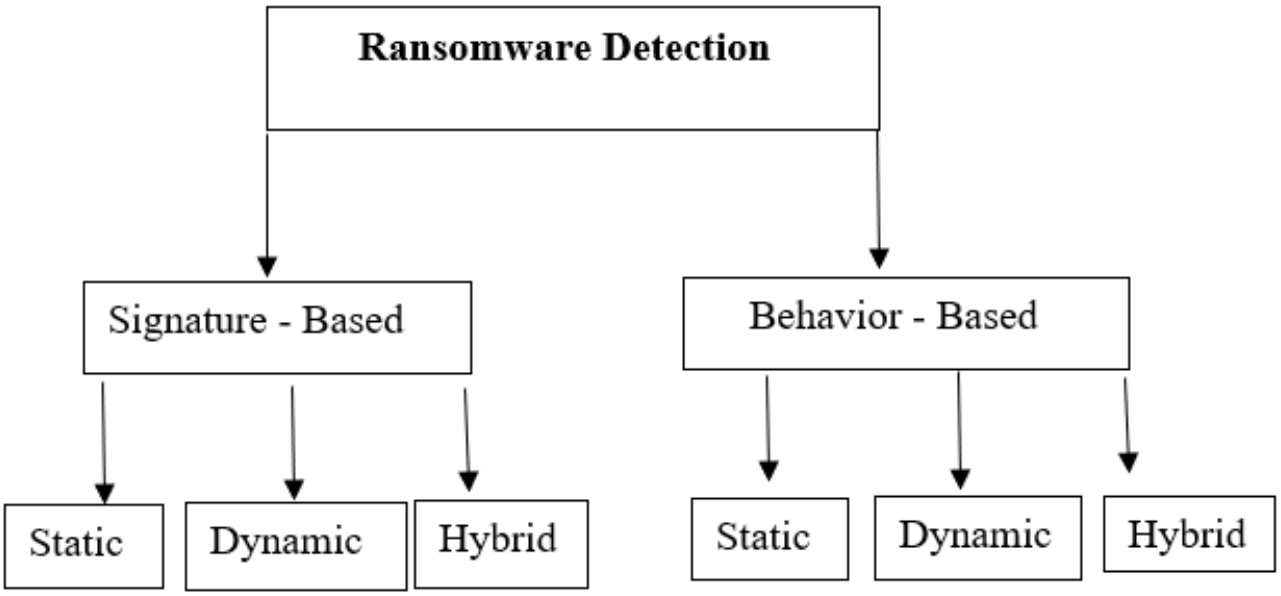
Chapter 4

METHODOLOGIES

4.1 Ransomware Detection Techniques

Signature-Based Detection Technique it is one of the commonly used counter measure. The unique feature of a malware executable such as a fingerprint. It has been used extensively by antivirus software. It is quite fast when compared to other techniques, but it cannot detect new malware(Unknown Malware).

Behavior-Based Detection Technique it is a Behavior-based malware detection techniques observe the behavior of the program to determine whether the program is malware or bengin. It looks for program behavior, not program code or code sequence. Even though the program codes are changed, the behavior of the program will be the same or similar, therefore, it can be still detected .



4.1 Ransomware Detection

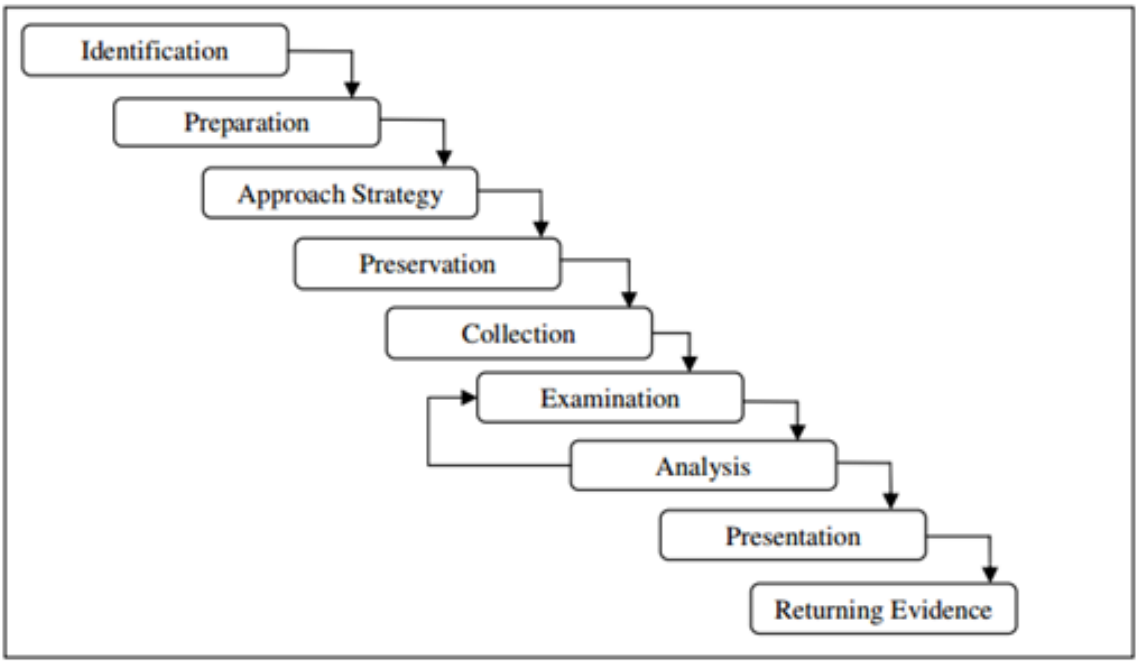
4.2 Forensic analysis

To provides comprehensive analysis techniques, because, there are various, or even a hundred, types of embedded systems in our environment. So, we can come up with each methodology responding to every digital device. So we focus on current issues about new emerging embedded systems. We separates two analysis phases, hardware analysis and software analysis. The hardware analysis focuses on hardware modification, through which a suspect has reconstructed embedded system for special purpose, like examples of the video game console.

The software analysis is based on installed software or firmware on an embedded system, such as operating systems, utilities, applications. The necessity of software analysis is connected with GPS navigation system analysis. Each GPS navigation system has its own particular file formats for saving plan routes, favorite destination, etc. So we need to analysis each file format and operation workflow to get vital information.

Ransomware Forensics includes the techniques and ways to investigate cybercrime. During this process, the digital evidence is preserved and later used to discover the actions taken by cybercriminals. Different methods take place that give insights to respond effectively to recover and decrypt your files and loss data. The whole process of ransomware forensics involves full-fledged investigation. In which forensics labs along with different law enforcement take steps and find their way back to recovery. The investigation usually relies on the digital evidence collected. Getting this evidence is one other process which is explained down below. There are cases in which this digital evidence is not properly collected, and that makes it quite hard to take steps to recover your files. After you have confirmed that a breach has occurred and the suspected ransomware attack is, in fact happening, a lot of things are going to start happening at once. It is

going to be stressful, and the forensics lab is going to be integral in performing root cause analysis. Some of the most important teams you will immediately want to connect with are your various Security teams—including but not limited to Network, Cloud, or Endpoint Security—so they can as quickly as possible isolate and quarantine infected end0points and servers, even network segments, to mitigate the spread of the ransomware attack.



4.2 Abstract forensic model

4.2.1 Operate an effective backup and restoration program

Make regular backups of all data files necessary to restore business operations in the face of loss of systems, applications, and data.Periodically restore systems from backup to ensure that backups are sufficient to re-

store operations quickly.Create offline backups that are separate from online backups to guard against the event that the ransomware reaches backup systems.

4.2.2 Prepare for an incident

Verify that suppliers have a documented and practiced incident response plan and that they have a ransomware-specific response playbook.

4.2.3 Educate employees on how to identify and respond to phishing emails

Cited earlier, 42 percent of ransomware attacks start with phishing. Ensure that suppliers are educating their personnel regarding the risk of phishing attacks and how to avoid becoming a victim. Employee security awareness companies such as KnowBe4, PhishMe, and Proofpoint, among others, actively engage employees in training programs with great results.

4.2.4 Expose authorized and hardened network services to the Internet

Sharing the lead with phishing, 42 percent of ransomware attacks start with exploiting an internet-accessible Remote Desktop Protocol Service. RDP services become more prominent during the pandemic as companies often hastily migrated employees to remote work. Re-

gardless of whether it is an employee's computer operating from home, or a server deployed in a data center or the cloud, ensure that suppliers restrict all internet-exposed network services to only those that are explicitly authorized and that are operated in a defensible manner. RDP, a very common and commonly exploited remote access service, should not be exposed to the Internet. Rather, a secure VPN service should be used that requires two-factor authentication.

4.2.5 Keep software patches current

According to Coveware, 14 percent of ransomware attacks started with exploiting vulnerable software in an internet-facing system. Demand that your suppliers operate a robust program for keeping software patches current, particularly the software of internet-facing systems.

4.2.6 Prevent malware from being delivered and spreading to devices

Filter malicious emails before delivery to mailboxes for malicious software, phishing content, and disreputable sources. Proxy all end-user Internet traffic through a proxy that automatically blocks access to malicious sites and dynamically detects and blocks malicious code and content. A stronger approach to protecting against web-native threats is allowing access to only safe browsing lists.

4.2.7 Prevent malware from running on devices

An ideal position to be in is one in which malware simply can't operate on endpoints. Suppliers can get part of the way there with endpoint protection platforms on every system. These stop identified threats before they install on the host system. However, they don't provide 100 percent protection. Two additional controls will greatly enhance the defensibility of systems. Remove administrator privileges from users and applications. This single action will render most ransomware from successfully operating on patched systems. Centrally administer systems and control what software can be installed and operated on systems. Application allow-list solutions can help manage this at scale.

4.2.8 Detect malicious network and endpoint activity

It is unreasonable to expect that the preventitive controls will block all threats. As such, it is essential to have robust network and endpoint activity and threat monitoring and blocking. This includes monitoring for intrusion attempts, sourcing from both outside and inside the network, data exfiltration attempts, known malicious, and abnormal communications.

Chapter 5

RESULTS AND DISCUSSIONS

Automatic depiction and prevention security engines are not enough indeed to prevent and mitigate. Recent reports from defect verities of the network security companies faced a big challenge how to prevent these kinds of attack. To prevent the user's data from getting into unrecoverable state, users should have an incremental online and offline backups of all the important data and images. Exposure to threats should be minimized, where ever possible the, site or IP address blocking and endpoint protection. Organizations and individuals should ensure that their electronic defense is as impenetrable as possible through the use of anti-virus, firewalls, IPS, web and mail filtering. A robust and incremental back-up system of business and personal-critical details should be implemented.

Chapter 6

CONCLUSION AND FUTURE ENHANCEMENTS

6.1 Conclusion

The goal of this seminar is to know more about Ransomware attacks. Ransomware assaults are exceptionally well known to the assailants as they are made or delivered income for aggressors. Additionally Ransomware assault become most impressive danger to individual and associations as they stop the working of frameworks by assaulting and encoding records or frameworks. While some systems are very effective at detecting Ransomware using a single detection technique,that technique will help to prevents the attacks.

6.2 Future Enhancements

Forensic analysis will become an area of increasing significance in the near future. Early detection may be difficult.To learn wellknown malware analysis and detection tools and compare the performance of these tools on existing and unknown malware.Kaspersky Lab and Intel have joined forces with Interpol and the Dutch National Police to set up a website aimed at helping people to avoid falling victim to ransomware.

Reference

[1] Giorgio valenziano Santangelo, Vincenz o Giuseppe Colacino, Mirco Marchetti (2021), “ Prevention and detection of ransomware attacks on Industrial Control Systems ”, p. 1-5.

[2] Mohammad, A. H. (2020), “ Ransomware evolution, growth and recommendation for detection ”. Modern Appl. Sci, 14(3), p. 144-150.

[3] Llker Kara , Murat Aydos (2020), “ Cyber Fraud: Detection and Analysis of the Crypto-Ransomware ” , 44(2), 1-42.

[4] KP Subedi, DR Budhathoki, D Dasgupta, (2018) , “ Security and Privacy Workshops (SPW) ”, 180-185.

[5] R. Richardson and M. North (2018), “ Ransomware: Evolution, Mitigation and Prevention,” International Management Review, vol. 13, p. 10-21 .

[6] D. Gonzalez and T. Hayajneh (2018) , “ Detection and prevention of cryptoransomware ”, pp. 472-478.