M. Mohanedova *et al*, International Journal of Advances in Agricultural Science & Technology,
Vol.11 Issue.4, April 2024, pg. 98-105

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

Crypto-Ransomware Analysis and Detection: Strengthening Security Measures

Ms.G.Naga Rani [1] , Kokkira Sudharma Kiran [2], Bheemala V G E Swamy Ganesh [3], Sudarsanam Aditya [4], Gunnam Saranya [5], Boddu Naina Sri [6] , [1] Assistant Professor, [2, 3, 4, 5, 6] B.tech Students Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India
Email: nagarani.g@pragati.ac.in

Abstract:

Since the advent of the wide adoption of virtual currency (such as Bitcoin, Ethereum, Ripple, and Litecoin), some with ill intents have become interested in this space and have created and sold ransomware to make easy access to virtual currency. Using cunning techniques, this ransomware enters the victim's computer and encrypts all of the files on it. Following the procedure for encryption, the intruder leaves a notice threatening to prevent entry to the encrypted data unless a virtual currency ransom is paid. The biggest threat to information technology security at the moment is this kind of ransomware, which is growing in popularity over time. Numerous studies about the identification and examination of this cyberbullying can be found in the literature. In this study, we looked closely at a forensic investigation of a recent attack example with an emphasis on crypto-ransomware. In this instance, the attack technique and the crypto-ransomware's behaviour were examined, and it was found that the attacker's data was available. Given this aspect, we believe our research will make a substantial contribution to the fight against this danger.

Keywords: Ransomware Analysis, Crypto-Ransomware, Cybersecurity

I. Introduction

New risks have surfaced in addition to the convenience brought about by the quick advancements in information and technology [1]. Attackers have altered their target, technique, and type of attack due to their fast adaptation to new technologies [2]. A new generation of safety precautions must be used by public institutions and organizations, commercial businesses, and regular internet users to combat these dangers [3].

Despite all safety measures, the number of cyberattacks has increased. At the moment, ransomware is the most often reported type of cyberattack [4]. Malicious software, also known as ransomware, encrypts a victim's private data and folders and then wants a ransom [5]. Cryptographic-ransomware and cryptographic locker ransomware are the two forms of ransomware that are typically examined [6]. It is acknowledged that crypto-ransomware was the first type of ransomware in use today [7, 8].

The victim's computer's OS or system entry is blocked by this malware until a ransom is paid. Usually, a prepaid card system code, an electronic card system, or a phone message are used to demand money transfer in exchange for ransom. By encrypting a specific portion of the files, crypto-ransomware blocks access and requires a code key to unlock the files.

The most common malware seen lately is crypto-ransomware. Attackers now have a focus on virtual money use due to its widespread use worldwide. The foundation of the malware is the ease of use of virtual currency and their untrace ability. Files encrypted by crypto-ransomware can be removed from the victim's computer. A notification indicating that the documents are encrypted and purchase is necessary appears on the screen when the user tries to access the requested files. The files with encryption are removed from the victim's computer and kept in an area controlled by the

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

attacker, with the understanding that sharing of the information will resume after a ransom is paid. Examined cases demonstrate that it is nearly challenging to gain access to the encrypted files, even after the ransom is paid.

II. LITERATURE SURVEY

Numerous methods have been employed up to this point in order to identify and analyse ransomware. Algorithms utilizing signature-based detection logic are the ones that are receiving the most attention [11]. This strategy's effectiveness is questionable because of its flaws. New-generation (fileless) ransomware cannot be identified using traditional signature-based methods. To address these shortcomings, novel strategies are still being explored. These methods include methods for examining ransomware's operational behaviour (dynamic analysis).

A ransomware identification technique based on signatures and visual mining was introduced by Fatemah et al. According to the study's findings, their successful detection rate was 96.6% [12].

A dynamic analysis method utilizing machine-learning reasoning for ransomware was created by Daniele et al. [13]. Dong Hyun et al. (2015) suggested a digitalized strategy for recognizing and preventing crypto-ransomware [14].

A novel method for identifying and analysing crypto-ransomware was created by Amin et al. This method defines the encryption technique and distinctive behavioural traits of the crypto-ransomware that is infecting the victim's system [15].

A workable technique for detecting and analysing crypto-ransomware was presented by Boldt et al. [16]. The method's greatest flaw is that it lacks a case study to evaluate its applicability and prohibits the usage of the approach's applications for free. We made the case study of crypto-ransomware that was studied in this paper available to anyone. Furthermore, consideration was given to utilizing trial versions of the statistical tools included in the suggested procedure. Our goal was to determine whether the suggested technique algorithm could be used to various investigations.

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

The current technology offered a workable strategy for analyzing and detecting crypto-ransomware. The primary shortcoming of this strategy is that neither the programs utilized in it nor the case study used to evaluate its applicability are free of charge. We made the case study of crypto-ransomware that was studied in this paper available to anyone. Furthermore, consideration was given to utilizing free versions of the statistical tools included in the suggested procedure. Our goal was to determine whether the suggested technique algorithm could be used to various investigations.

In a computer's virtualization setting, Shaid evaluated Maarof [17] malware, gathered user-level API requests, and categorized. Forensic Toolkit (FTK) program tools were utilized by Kara et al. [18] in 2019 for ransomware investigation and detection. Through their research, Akbanov et al. [19] have created a methodology for identifying ransomware on cloud-hosted virtual computers. Hwang et al. [20] presented a method combining machine learning and dynamic analysis in 2020. Hwang also tested the accuracy of the API categorization using 1176 ransomware files on the dataset, reporting 97.3%.

DISADVANTAGES OF THE EXISTING SYSTEM

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

Signature-Based Detection Limitations:
Traditional antivirus solutions often rely on signature-based detection, which involves recognizing known patterns of malware. This approach may struggle to detect new or sophisticated variants of crypto-ransomware that frequently evolve to bypass signature-based defenses.

False Positives and Negatives:
Many detection systems face challenges in achieving a balance between false positives and false negatives. False positives can lead to unnecessary alerts, while false negatives can result in undetected threats. Striking the right balance is a continuous challenge.

Encrypted Traffic Challenges:
With an increasing use of encryption, attackers may use encrypted channels to communicate and deploy ransomware. This makes it difficult for traditional network-based detection systems to inspect the content of encrypted traffic, potentially allowing malicious activity to go undetected.

Polymorphic Ransomware:
Polymorphic ransomware can change its code and appearance while maintaining its core functionality. This adaptability makes it challenging for signature-based detection systems to keep up.

Zero-Day Exploits:
New, previously unknown vulnerabilities, known as zero-day exploits, pose a significant challenge. Existing systems may not have signatures or rules to detect and prevent attacks exploiting these vulnerabilities until they are discovered and addressed.

Resource Intensiveness:
Some advanced detection methods, such as behavioral analysis and machine learning, can be resource-intensive. Implementing these technologies may require significant computing power and can impact system performance.

Lack of Standardization:
The lack of standardized protocols for sharing threat intelligence and indicators of compromise (IoCs) can hinder the effectiveness of collaborative defense efforts. Improved information sharing could enhance the ability to detect and respond to threats.

User Awareness and Training:
Human factors, such as social engineering and phishing attacks, remain a common vector for ransomware. Existing systems may not address the need for continuous user awareness and training to recognize and avoid these threats.

Ransomware-as-a-Service (RaaS):
The rise of RaaS models allows even individuals with limited technical skills to deploy ransomware attacks. This dynamic landscape poses challenges for traditional security measures.

B. PROPOSED SYSTEM

For a proposed system focused on the detection and analysis of crypto-ransomware, advancements should be made to overcome the limitations of existing solutions. The proposed system integrates cutting-edge technologies such as machine learning, behavioural analysis, and threat intelligence sharing to enhance the detection and mitigation capabilities. By employing machine learning algorithms, the system aims to dynamically adapt to evolving ransomware threats, identifying patterns and anomalies in real-time, even those associated with polymorphic variants. Behavioural analysis components will focus on monitoring system activities, identifying deviations from normal behaviour, and

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

swiftly flagging potential ransomware activities. The system will also incorporate advanced threat intelligence sharing mechanisms, allowing organizations to collaboratively combat emerging threats collectively. Emphasis will be placed on encrypted traffic inspection, addressing the challenge of concealed communication channels that attackers exploit. Additionally, user awareness and training modules will be integrated to fortify defences against social engineering and phishing attacks. The proposed system aims not only to detect and neutralize ransomware threats effectively but also to minimize false positives, optimize resource utilization, and provide a comprehensive and adaptive defence against the dynamic landscape of cyber threats.

ADVANTAGES OF THE PROPOSED SYSTEM

Advanced Machine Learning for Threat Detection:
By integrating advanced machine learning algorithms, the system can autonomously learn and adapt to new and evolving ransomware threats. This enables the detection of previously unseen variants and improves overall accuracy in identifying malicious patterns.

Behavioral Analysis for Anomaly Detection:
The inclusion of behavioral analysis enhances the system's ability to identify ransomware activities by monitoring and analyzing deviations from normal system behavior. This proactive approach helps in detecting threats based on their actions rather than relying solely on known signatures.

Real-time Detection and Response:
The proposed system operates in real-time, ensuring timely detection and response to ransomware threats. Rapid identification of malicious activities allows for swift containment and mitigation measures, reducing the potential impact of an attack.

Threat Intelligence Sharing for Collaborative Defense:
The system facilitates effective threat intelligence sharing among organizations, fostering a collaborative defense approach. By leveraging shared information on indicators of compromise (IoCs) and emerging threats, the system enhances the collective ability to detect and respond to ransomware attacks.

Encrypted Traffic Inspection:
Addressing the challenge of encrypted communication channels, the system incorporates mechanisms for inspecting encrypted traffic. This enables the detection of malicious activities within encrypted connections, preventing attackers from leveraging these channels to conceal their operations.

Adaptive Defense Against Polymorphic Ransomware:
The proposed system is designed to effectively combat polymorphic ransomware by dynamically adapting its detection mechanisms. The use of machine learning and behavioral analysis allows the system to recognize and respond to variations in ransomware code and behavior, increasing resilience against adaptive threats.

User Awareness and Training Integration:
The inclusion of user awareness and training modules enhances the overall security posture. Educating users about social engineering and phishing threats reduces the likelihood of successful ransomware attacks initiated through human manipulation.

IV.SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

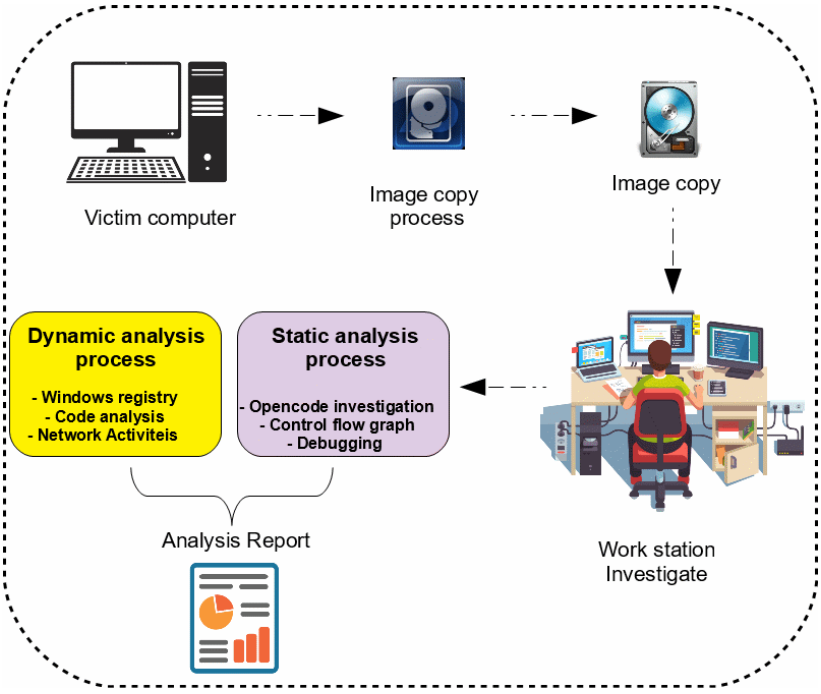


Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

Machine Learning-Based Threat Detection Module:
This module incorporates advanced machine learning algorithms to analyze patterns and characteristics of ransomware. It continuously learns from historical data and adapts to new threats, enabling the system to detect and classify potential ransomware activities based on their unique signatures and behaviors.

Behavioral Analysis Module:
The behavioral analysis module focuses on monitoring system activities in real-time. It establishes a baseline for normal behavior and identifies anomalies that may indicate ransomware activity. By assessing deviations from established patterns, this module enhances the system's ability to detect sophisticated, polymorphic, or previously unknown ransomware variants.

Threat Intelligence Sharing Module:
This module facilitates the sharing of threat intelligence among organizations. It integrates with external threat intelligence feeds and enables the exchange of indicators of compromise (IoCs) and insights into emerging threats. Collaborative defense is strengthened as participating organizations collectively contribute to and benefit from a shared knowledge base.

Encrypted Traffic Inspection Module:
Addressing the challenge of encrypted communication channels, this module includes mechanisms for inspecting and analyzing encrypted traffic. By decrypting and inspecting the content of encrypted connections, the system can identify potential ransomware activities within secure channels, enhancing overall visibility and security.

ISSN: 2348-1358

Impact Factor: 6.901

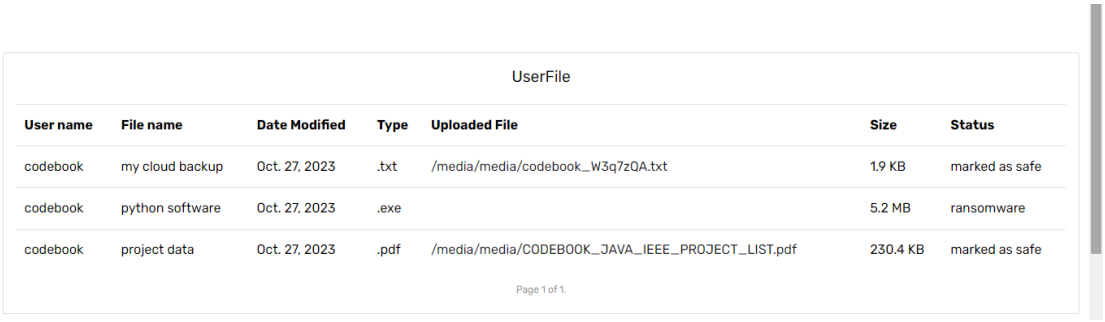
NAAS Rating: 3.77

User Awareness and Training Module:

The user awareness and training module focuses on educating users about potential threats, particularly those related to social engineering and phishing attacks. Interactive training sessions, simulated phishing exercises, and awareness campaigns aim to empower users to recognize and avoid behaviors that could lead to ransomware infections. This module complements technical defenses by strengthening the human element of cybersecurity.

VI . RESULTS AND DISCUSSION

Based on the attacker's IP address and the results of suspicious network traffic investigations, it seemed that the attacker could be located. However, for these kinds of attacks, attackers typically don't use a stable IP. It is possible to utilize specialized applications to render the attacker undetectable. Virtual private networks are the most widely used of these customized applications (VPN). By verifying identity, a virtual private network (VPN) enables users to access resources or servers remotely. VPNs are known to encrypt and encapsulate data, including IP addresses. Verifying questionable traffic is necessary if the attacker's IP address is identified.


UserFile

User name	File name	Date Modified	Type	Uploaded File	Size	Status
codebook	my cloud backup	Oct. 27, 2023	.txt	/media/media/codebook_W3q7zQA.txt	1.9 KB	marked as safe
codebook	python software	Oct. 27, 2023	.exe		5.2 MB	ransomware
codebook	project data	Oct. 27, 2023	.pdf	/media/media/CODEBOOK_JAVA_IEEE_PROJECT_LIST.pdf	230.4 KB	marked as safe

Page 1 of 1.

Fig 2. Uploaded Files

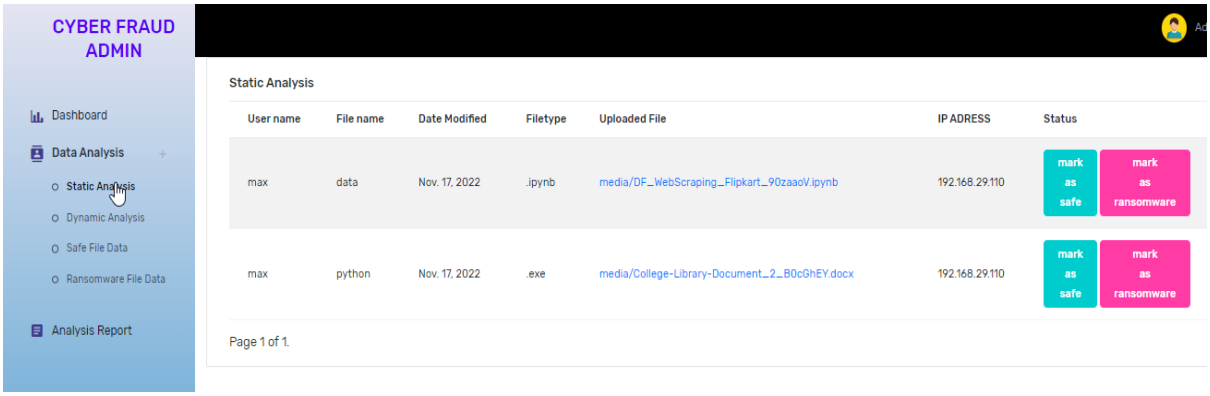


Fig 3. Verifying The Cyber Fraud Data

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

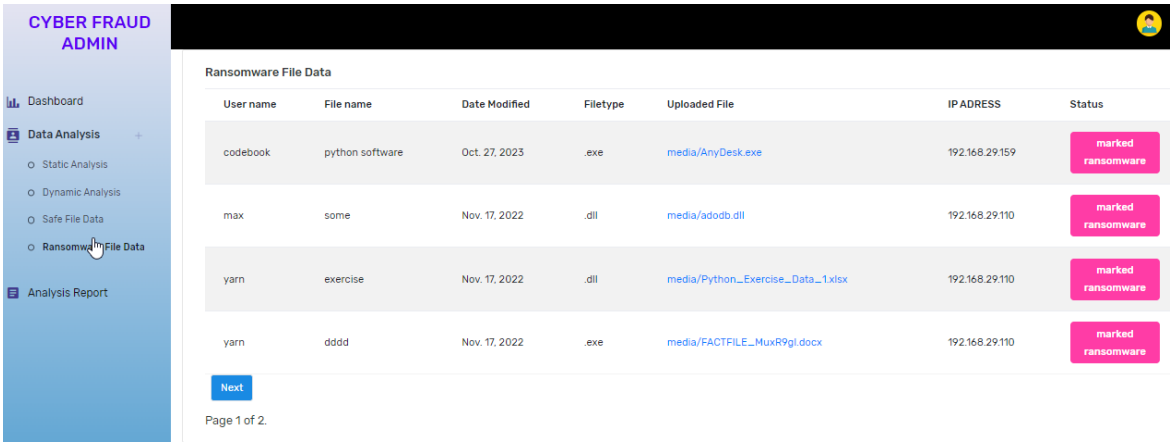


Fig 4. If any Changes happened then It Is Marked as Ransomware

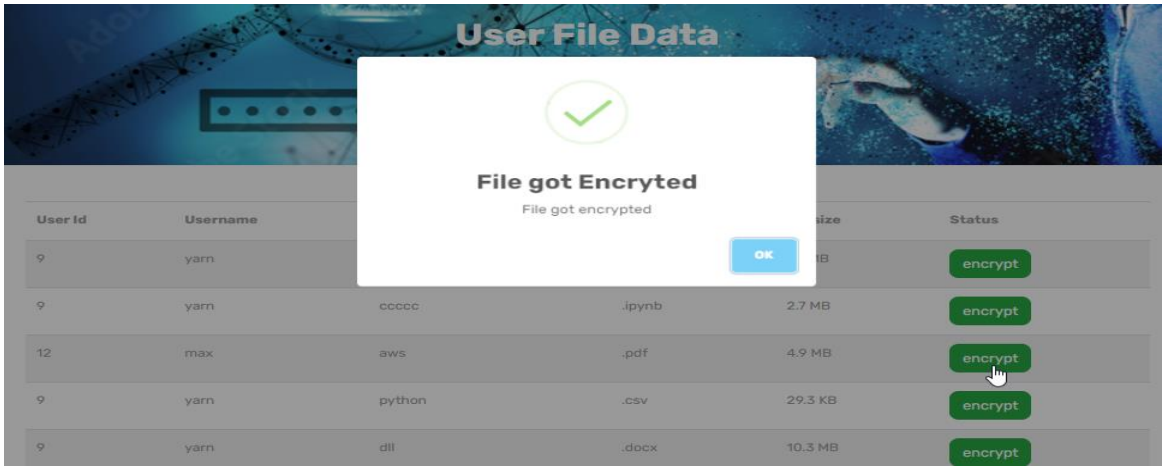


Fig 5. To Overcome Every File Was encrypted

VI I.CONCLUSION

Attacks using crypto-ransomware have increased significantly, particularly in light of the growing use of virtual currencies. The inability to trace virtual currency lawfully is the cause of this predicament. Attackers use crypto-ransomware to encrypt the victim's files and tell them they will need to purchase an encryption key in order to get access to their files once more. It is regarded as technically difficult to crack the encryption via outside interference due to the sort of encryption utilized in ransomware. After erasing the encrypted data from the victim's computer, the attacker claims to have them stored in a location they control. To make sure the victim accepts the story, attackers have recently sent a message promising to unencrypt a file of their choosing that is no larger than 100 MB. The victim is successfully granted access to the file once they consent. But the attacker's goal is accomplished and communication ends when the victim pays the requested ransom.

The detection of this malware, comprehending its operation, and locating the offender are all included in the analysis of ransomware. Reverse engineering techniques are employed in crypto-ransomware analysis to ascertain the malware's structure and its interaction with the system.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

REFERENCES :

[1] M. Egele, T.Scholte, E. Kirda, & C. Kruegel, 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), 1-42.

[2] D. Kim, D. Shin, D. Shin, & Y. H. Kim, 2019. Attack detection application with attack tree for mobile system using log analysis. Mobile Networks and Applications, 24(1), 184-192.

[3] F. L. Lévesque, S. Chiasson, A. Somayaji, & J. M. Fernandez, 2018. Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security (TOPS), 21(4), 1-30.

[4] İ. Kara, M. Aydos, 2019. The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).

[5] I. Kara, M. Aydos, 2018, December. Static and dynamic analysis of third generation cerber ransomware. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.

[6] B. A. S. Al-rimy, M. A. Maarof, S. Z. M. Shaid, 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[7] S. Baek, Y. Jung, A. Mohaisen, S. Lee, D. Nyang, 2018, July. SSD-insider: Internal defense of solid-state drive against ransomware with perfect data recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 875-884). IEEE.

[8] M. A. S. Monge, J. M. Vidal, L. J. G. Villalba, 2018, August. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).

[9] K. İlker, M. Aydos. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.

[10] S. Mohurle, M. Patil, 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).

[11] F. Karbalaie, A. Sami, and M. Ahmadi. 2012.Semantic malware detection by deploying graph mining. International Journal of Computer Science Issues,9(1):373-379.

[12] D. Sgandurra, L. Munoz-Gonz_alez, R. Mohsen, and E. C. Lupu. 2016. Automated dynamic analysis of ransomware: Bene_ts, limitations and use for detection. arXiv preprint arXiv:1609.03020.

[13] D. Kim and S. Kim. 2015. Design of quanti-cation model for ransom ware prevent. World Journal of Engineering and Technology, 3(03):203