STM JOURNALS

International Journal of
Information Security Engineering

Volume 1, Issue 2, 2023
July—December
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

A Security Investigation Survey of Ransomware Detection and Avoidance Strategies for IoT Networks

Muhammad Nadeem[1], Syeda Wajiha Zahra[2,*], Muhammad Noman Abbasi[2], Ali Arshad[3], Saman Riaz[3], Waqas Ahmed[2]

Abstract

The internet of things (IoT) refers to the interconnection of a large number of distinct physical objects, which in turn makes possible a variety of services and applications. Because the IoT sector is developing at such a rapid rate, ensuring its safety ought to be a high concern. At this time, ransomware attacks constitute the biggest danger to IoT posed by cyberattacks. Ransomware is software that blocks access to or usage of a victim's computer and then demands money from the user in order to restore the machine to its previous state. In spite of the frequency of malware attacks, ransomware is considered to be the most devastating. This is due to the fact that it has caused companies to be interrupted, which has led to considerable cash loss while also creating a severe financial pressure on the organisation. Criminals may demand and collect extortion from victims while disguising their identities and whereabouts with the use of bitcoin, which is the most well-known cryptocurrency. A framework for the detection, prevention, and prediction of ransomware attacks has been established, and it is being used to conduct an analysis of various methodologies and tactics for detecting, preventing, and mitigating ransomware assaults.

Keywords: Internet of things (IoT), ransomware, prevention, detection, prediction

INTRODUCTION

Users store their private information digitally to safeguard it from various threats as more and more internet companies accumulate immense quantities of personal data [1]. Physical components of internet of things (IoT) infrastructure become intelligent objects due to their planning and controlling capabilities [2]. These smart objects are increasingly important in all spheres of human existence, from the household to significant industrial and institutional settings [3]. The general structure of IoT is depicted in Figure 1.

The most challenging step is then to protect the user's data because most attackers target the user's system, decrypt crucial files using dangerous viruses, and then demand payment, a practice known as a ransomware attack [4]. Ransomware refers to malicious software that effectively restricts access to a computer system or data, coercing the victim into paying to regain access [5]. "Ransomware" is a phrase created from the words "malware" and "ransom." The abbreviation "malware" stands for "malicious software." Malware is designed to access victim computers or harm them [6]. Malware today is primarily produced

*Author for Correspondence
Syeda Wajiha Zahra
E-mail: syeda.wajia786@gmail.com

[1]Student, Department of Computer Science and Technology, University of Science and Technology Beijing, China
[2]Lecturer, Department of Computer Science, Alhamd Islamic University, Islamabad, Pakistan
[3]Assistant Professor, Department of Computer Science, National University of Technology, Islamabad, Pakistan

Received Date: September 18, 2023
Accepted Date: October 05, 2023
Published Date: October 30, 2023

Citation: Muhammad Nadeem, Syeda Wajiha Zahra, Muhammad Noman Abbasi, Ali Arshad, Saman Riaz, Waqas Ahmed. A Security Investigation Survey of Ransomware Detection and Avoidance Strategies for IoT Networks. International Journal of Information Security Engineering. 2023; 1(2): 14–23p.

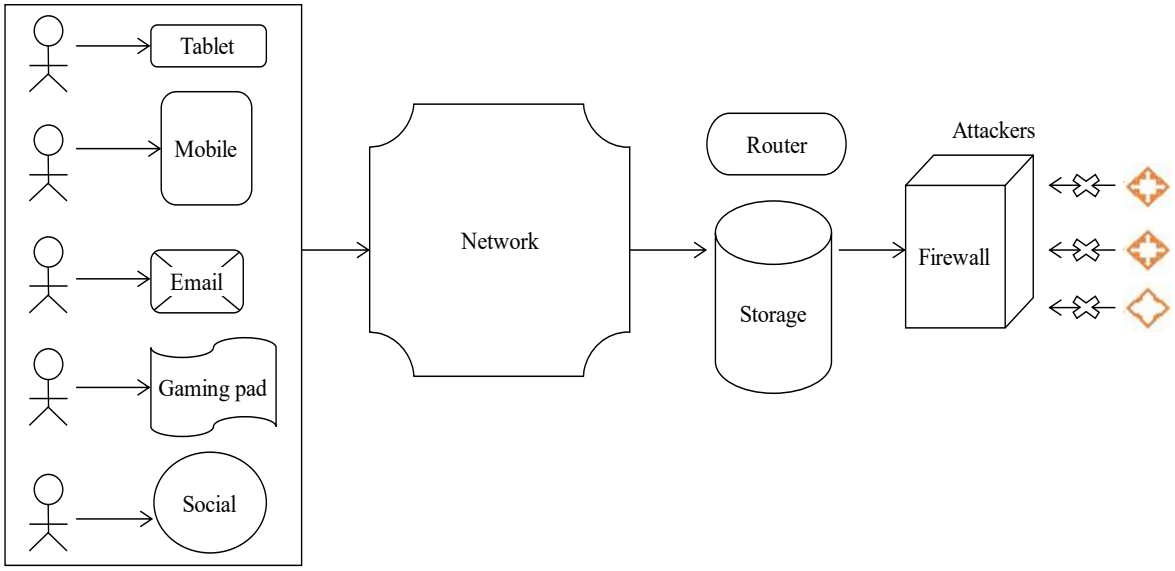

Figure 1. Structure of internet of things (IoT).

for financial gain [7]. According to the computer security company Symantec, as information technology advances, cybercriminals are becoming more skilled at hiding their malware programs and improving their ability to successfully evade the most up-to-date security solutions [8]. The attacker uses multi-phase ransomware to spread the infection. Because the attackers regularly incorporate new technologies in line with contemporary technology into their ransomware and employ them faster than others, the criminals are so effective with their ransomware [9].

PRECURSORIES

Association of Ransomware's Life Process and Situation Awareness System

Concerns regarding information security have increased with the growth of the internet, especially in light of the emergence of different types of malware [10]. Understanding the ransomware life cycle, how it relates to the situational awareness model, and its payment options is crucial to preventing or lessening this danger. The four steps of the Endsley situational awareness system [11] are shown in Figure 2:

1. *Perception:* This phase involves identifying and continuously monitoring certain assets and network indicators. Reports include both common incidents and atypical situations. During the perception stage, raw data about the protected system is collected unprocessed [12]. This data must be structured in separate formats to streamline its management and availability.
2. *Understanding:* The collected data is systematically correlated and integrated to streamline the analysis and prediction process. A preliminary analysis is conducted after removing excessive and duplicative data [13].

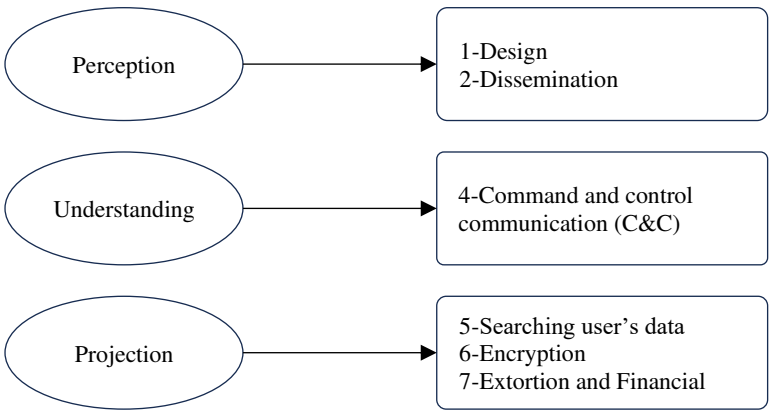

Figure 2. Stages of situational awareness system.

3. *Projection:* This stage employs analysis tools to forecast the system's behavior and monitor its development. This stage considers the effects of earlier countermeasures and their use on the environment [14]. Utilizing both proactive and reactive activities and replies, historical and present knowledge is combined.
4. *Payment:* The economic effect of ransomware depends on several factors, including the attack's origins, the nature of the ransom wanted, the degree to which the infection has propagated, and the amount of money in question. In the context of ransom payments, it is common for cybercriminals to demand a certain amount of one-bit currency, namely 1 BTC, or an equal value in US dollars [15].

Types of Ransomware Analysis

Ransomware analysis involves taking steps to understand its traits and behaviour. There are three primary forms of ransomware analysis approaches, similar to how malware is typically analyzed: static, dynamic, and hybrid.

Static Analysis

Before the crypto-binary functions are executed, this is used to detect them. Additionally, it uses heuristic analysis to search for loops, entropy, a large percentage of bitwise operations, and other things [16]. Data flow graphs are used in these techniques to help identify signatures and cryptographic constants for examination. Important information regarding the targets, persistence strategies, and command and control architecture of the virus may be revealed. Features like hashes, strings, opcodes, byte sequences, etc., are extracted and inspected to assess if a file is harmful. The virus may be examined using a variety of network analyzers and disassembler software without having to execute the binary code [17].

This approach aims to ascertain the nature of a given sample, namely if it constitutes ransomware, by extracting structural data without actual execution. In computer science research, decompiling sample binaries is used to extract pertinent details on the structure and content of those samples [18]. This methodology allows for the analysis of samples without their execution while still attaining crucial information. Static analysis is often regarded as a speedy and secure method due to the absence of sample execution. Nevertheless, the makers of malware exhibit resistance against static analysis endeavors and actively evade protection measures that rely on identifying structural components via static analysis. They do this by using concealment methods such as obfuscation, polymorphism, and encryption and utilizing anti-disassembler tools [19].

Dynamic Analysis

Dynamic analysis involves watching the operation of the cryptographic algorithms. To comprehend the disruption caused, one study technique is to look at the avalanche impact of input on output. Another method used in this research is counting the total number of consecutive memory accesses based on input and output parameters [20].

To assess the operational status of the sample and verify the existence of ransomware, it is essential to carry out the execution and subsequent inspection of the specimen. A dynamic analysis addresses any dangers related to the material under investigation by executing the samples inside a segregated or controlled environment, sometimes called a sandbox. To study the behaviour of the sample, researchers may use the unique characteristics of the sandbox environment and employ hooking tactics. Compared to static analysis, conducting dynamic analysis requires more time and money due to the need for an isolated environment and the actual deployment of ransomware.

Although concealment and anti-disassembler techniques worked well against static analysis, they are useless against dynamic analysis since they cannot mask the behaviour of the ransomware [21]. Dynamic analysis may be used to determine the encryption technique and ransom payment mechanism used by the ransomware. It may also be used to identify the methods used by ransomware to propagate, such as exploiting security holes or sending phishing emails [22].

Hybrid Analysis

Hybrid studies sometimes integrate static and dynamic analytic methodologies as researchers recognize each methodology's strengths and limitations. The proposed approach integrates static and dynamic analytic methodologies for malware analysis. The amalgamation of the information from both researches contributes to a more thorough understanding of the virus and its capabilities. Using the intricate hybrid analysis methodology, many forms of harmful software, such as ransomware, Trojans, and other types of malware, may be scrutinized [19].

Basic Branches of Information Security

To safeguard information security, the research community is developing novel tactics and methodologies to mitigate the risk of ransomware attacks. The tactics and procedures may be classified into three primary areas: prevention, detection, and prediction [23]. The fundamental principles behind these ideas are the diagnosis of device status and the prediction of potential attacks. The optimal strategies or countermeasures to address dubious situations are chosen based on the acquired information. To achieve this objective, contemporary research has advanced intelligent algorithms, including Bayesian networks (BNs), decision trees, and support vector machines (SVMs). The primary emphasis of each of these branches revolves around the specific activity outlined below:

1. *Prevention:* This subject pertains to the measures used to mitigate or reduce the probability of a ransomware attack. These operations may include the installation or use of a specific program, as well as the update of the operating system, among other possibilities. Implementing file backups is an additional measure to mitigate the risk of extortion [24]. The major objective of this phase is to address and rectify system vulnerabilities or security loopholes that have been exploited before.
2. *Detection:* The objective of this stage is to implement a range of tactics for detecting ransomware attacks, both before their occurrence, during their execution, and after their completion. The primary objective of detection is to discern potentially suspicious occurrences or conditions by an initial diagnostic assessment of the end devices. Implementing this measure may mitigate the impact on the system as it proactively deters and hinders the initiation of a possible attack. In addition, the detection process may include proactive and reactive measures.
3. *Prediction:* This stage aims to mitigate potential threats before their occurrence proactively. To do this, the system gathers data from terminal devices about various characteristics or connections. The data above is then analyzed and connected to detect probable instances of assault [25]. Intelligent methodologies are a fundamental principle in the field of prediction. Users can use preventive measures to obstruct or evade the impending assault, as indicated by the forecast. This section presents the latest research findings categorized according to preventive mechanisms and strategies for detection and prediction as shown in Figure 3.

Classification Based on Analysis

Several important factors may be used to categorize ransomware, malicious software that encrypts a victim's data or locks them out of their machine until a ransom is paid. First, it may be divided into groups depending on how it spreads [26]. These groups include ransomware spread by email via phishing emails, drive-by downloads from compromised websites, advertising via malicious adverts, and watering hole attacks that target certain websites that victims often visit. Second, the kind of

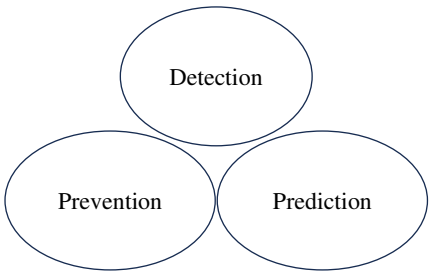

Figure 3. Information security branches.

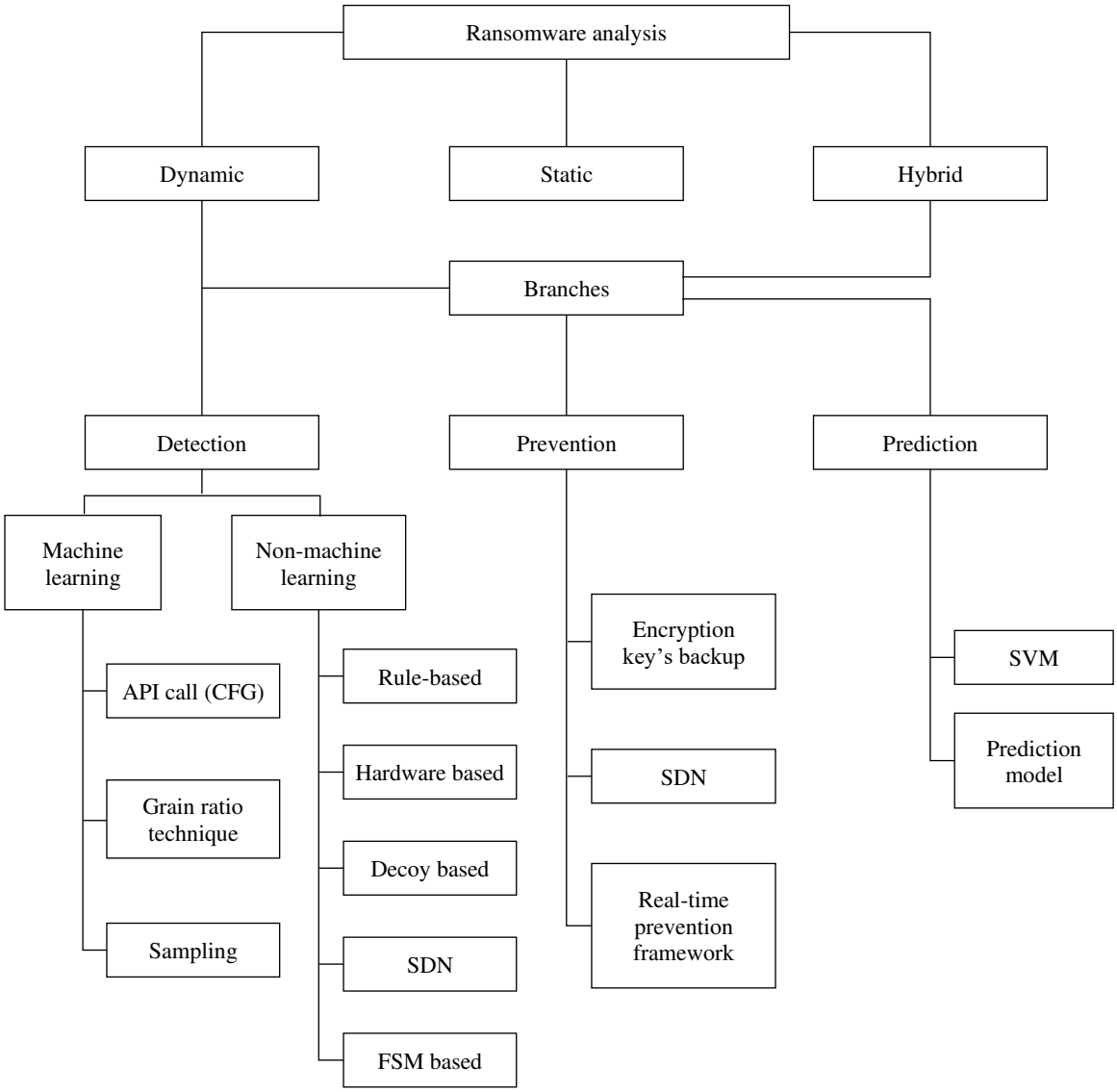

Figure 4. Classification of ransomware.

encryption used by the ransomware may be identified. Some variations use symmetric keys for encryption and decryption, but others use asymmetric keys and often keep the private key hostage. Third, a ransom payment technique that often demands cryptocurrencies like Bitcoin or other alternative digital currencies may be used to categorize.

Additionally, numerous groups may be ransomware targets, each with a distinct level of harm and ransom demands, such as consumers, businesses, or essential infrastructure. Last, ransomware may engage in various actions, such as file encryption, system lockout, tampering with the master boot record, or the display of menacing screen locks. With the help of this categorization methodology, cybersecurity experts can better comprehend the variety of ransomware threats and create efficient preventive and response plans as shown in Figure 4.

LITERATURE REVIEW

An in-depth analysis of ransomware is provided in this study, including information on its development, typical attack routes, encryption methods, and payment systems [27]. Along with numerous preventative and mitigation techniques, it also covers the effects of ransomware on people, organizations, and society.

The survey article by Sun and Grishman [28] investigates several ransomware attack detection and prevention methods. It discusses machine learning-based, behavior-based, and signature-based techniques while outlining the advantages and disadvantages of each. The difficulties in creating efficient ransomware defensive methods are also covered in the article.

The study by Tan et al. [29] focuses on the many assault methods that ransomware writers use to compromise computers. It thoroughly examines email phishing, drive-by downloads, infected attachments, and other ransomware operators' tactics [29]. Real-world case studies are also included in the paper.

The study by Krishnamoorty and Umarani [30] aims to provide an economic analysis of ransomware payments by looking at the goals of both attackers and victims. It examines the variables affecting ransom amounts, using cryptocurrencies in payments, and the moral quandaries victims confront [30]. The paper also touches on the consequences of policy.

The article by Sundar et al. [31] examines the unique problems ransomware attacks in healthcare companies present, focusing on the healthcare industry. It discusses patient safety threats, healthcare data breaches' effects, and regulatory compliance challenges [31]. Additionally, the report makes suggestions for enhancing hospital cybersecurity.

Wu et al. [32] offer insights into the changing ransomware scenario, including current patterns and potential future developments. The employment of sophisticated evasion strategies, the rise of double extortion, and the targeting of essential infrastructure are all covered [32]. The publication also describes possible defences.

Detection Approaches

Based on Machine Learning

Machine learning, including deep learning techniques, offers a significant advantage by using historical data to identify patterns indicative of ransomware existence. Furthermore, in light of the ongoing evolution of ransomware as a persistent threat, it is possible to train machine learning algorithms to identify novel and previously unknown manifestations of this menace.

To generate a set of API call flow graphs (CFG) for the feature vector space, the researchers [23] used dynamic analysis. They have used basic logistics to separate benign and malicious software, among other data mining methods. Machine learning algorithms were used to categorize and identify different ransomware families. The raw bytes were extracted via static analysis and created a feature space. With the use of the gain ratio approach, irrelevant features were eliminated. Some researchers put out a hybrid ransomware detection approach incorporating static and dynamic analysis [33]. Samples from all current ransomware families, including WannaCry, were included in the experiments. The findings showed that the suggested hybrid technique can identify ransomware more accurately as shown in Table 1.

Table 1. Pros and cons of machine learning detection techniques.

Techniques	Implementation	Detection	Pros	Cons
Dynamic analysis	API call flow graph (CFG)	Malicious software	Provide enough detail of interactions between ransomware and the target system.	Not fully encompass the behaviors of malware
Static analysis	Gain ratio technique	Ransomware families	Efficiency	False positives or false negatives
Hybrid analysis	Sampling	Ransomware families, including Wanna Cry	Higher accurate results	False negatives

Based on Non-machine Learning

The objective of current cybersecurity research has been to develop effective methodologies for detecting ransomware attacks. One method that has garnered favour is the use of decoy-based tactics. These tactics entail the construction of "honeypot" systems that replicate the attributes of critical network resources. The purpose of these systems is to attract and identify ransomware assaults. The investigation of using software-defined networking (SDN) to monitor network traffic and detect malicious activities has also been explored. Furthermore, several scholars have proposed using rule-based methodologies, which rely on predetermined rules or distinctive patterns to detect existing ransomware variants. In this part, we will examine these approaches' scientific contributions.

Authors Tandon and Nayyar [34] presented Crypto Drop, a mechanism for early detection that may provide alerts for ransomware operations. The system effectively employs behavioral cues to terminate potentially suspicious processes, resulting in few occurrences of false positives. Introduced UNVEIL, a system designed specifically for ransomware detection using dynamic analytic techniques. The identification process relies on analyzing manipulated files on the desktop and in the user's folders. The technology establishes an artificial user experience and identifies file changes due to ransomware. In addition, the system can monitor changes in behavior and modifications made to the system itself. The detection mechanism may identify evasive ransomware, namely zero-day variants, that have not yet been documented or reported. Introduced ShieldFS as a protective measure against ransomware attacks. The system proactively mitigates potential risks by continuously monitoring and analyzing file system behavior, establishing robust profiles for enhanced security measures. When a profile displays unusual behavior, its negative impacts on the file system are effectively reversed. The method was developed by analyzing a vast volume of input/output (I/O) file system requests conducted over one month. These requests were sourced from reliable programs and gathered from high-quality personal computers.

The efficacy of ShieldFS was evaluated via practical assessments, including several types of malware, namely ransomware. These assessments were conducted in real-world scenarios, and ShieldFS demonstrated its ability to detect and promptly restore compromised data effectively. Cabaj et al. [17] proposed a detection method for Windows systems using SDN. The methodology examines pertinent HTTP message sequences as the defining attributes while observing the network traffic between crypto-ransomware types, Crypto Wall and Locky. To address the issue of ransomware attacks, using Amoeba, a solid-state drive (SSD) solution that offers automatic backup functionality. The system has a hardware accelerator that can detect contaminated pages upon activation via a prompt backup control mechanism. The objective is to minimize the storage capacity needed for the primary data backup. The study used actual block-level FSM, finite-state machine; SDN, software-defined networking; SSD, solid-state device. Traces obtained via dynamic analysis, and the assessment was

Table 2. Pros and cons of non-machine learning detection techniques.

Technique	Implementation	Detection	Pros	Cons
Rule based (Crypto Drop)	Stop suspicious processes	Early detection system; notify ransomware activities	Behavior indicators	Data loss
Hardware based (Unveil)	Tampering files/generate artificial environment	Identify unknown evasive (zero-day) ransomware	Track system changes	Potential for false positives
Decoy based (ShieldFS)	Defense mechanism file system	Attacks monitoring and detection	Defend against attacks and efficiently recover files	Excessive use of resources
SDN	Detection method	Monitor network traffic	Enhanced flexibility and agility in the network	One failure point
FSM based	Amoeba, an SSD system	To combat ransomware threats, use automatic backup	Reduce space cost of backing up the original data	More resource utilisation

conducted using the Microsoft SSD Simulation tool. The program demonstrated superior performance compared to Flash Guard, a separate software application that supports device data backup as shown in Table 2.

Prevention

The primary focus was the safe storage of backup copies of encryption keys. This approach facilitates the restoration of compromised systems or data affected by ransomware, ensuring safeguarding against hostile intrusions. Several researchers [7] focused on the security risks ransomware poses in the internet of things (IoT) context. Furthermore, they also offered a detection model for ransomware attacks on IoT devices. The proposed approach uses a SDN gateway to meticulously monitor incoming traffic inside the IoT systems.

Table 3. Pros and cons of prevention techniques.

Technique	Implementation	Prevention	Pros	Cons
Dynamic	Encryption keys' backup	Defending against nefarious assaults	Easy recovery of files	Compromising the encryption keys' integrity and confidentiality
Static	SDN	Observe the incoming traffic and mitigate ransomware	Pro-activeness	Lack of updation
Hybrid	Real-time prevention framework (logs analysis)	Reduce early invasions	Detection of threats right away	Alarms that are not necessary and a workload increase for security staff

Furthermore, rules inside the SDN controller are employed to detect and address ransomware affecting IoT devices. Rehman et al. [35] developed a proactive strategy that operates in real-time, using cloud and anomalous behavior analysis for detection purposes. The second approach reduces the occurrence of intrusions by collecting data from various devices and logs and analyzing it using a cloud-based system as shown in Table 3.

Prediction

Malecki [36] proposed a methodology for proactively predicting ransomware attacks in industrial IoT systems. The context-aware approach employs support vector machines (SVMs) to proactively forecast such attacks in advance. George and Sagayarajan [37] use many characteristics derived from Bitcoin transactions. The researchers used descriptive statistical analysis and machine learning techniques to construct a predictive model to identify and classify ransomware families. The primary objective of this model was to mitigate financial losses incurred as a consequence of ransomware assaults as shown in Table 4.

Table 4. Pros and cons of prediction techniques.

Analysis	Technique	Implementation	Prediction	Pros	Cons
Dynamic	SVM (support vector machine) Algorithm	Context awareness model	Ransomware attacks in industrial internet of things (IoT)	Proactive prevention	Sometimes incorrect result
Static	Prediction model by using machine learning models	Bitcoin transaction	Ransomware families	Avoidance of financial loss	Lost chances to recognize and stop ransomware assaults.

CONCLUSION

Both individual users and businesses face a major risk when ransomware is present on their computers. It has been shown that the proliferation of ransomware has an increasing influence on businesses and organisations, resulting in significant financial implications and damaging impacts on their image. This is the case as a result of the fact that ransomware is becoming more prevalent. Additionally, the emergence of new markets and business models, such as mobile communication, the

IoT, cloud-based services, and the supposed anonymity of digital money, have all contributed to the development of fresh ransomware types. In spite of the strenuous efforts of the academic community to develop fresh ways for mitigating and avoiding ransomware attacks, there is a perceptible trend occurring towards the use of cognitive approaches for gaining information about endpoints and network aspects. Finding developing features that are acceptable inside the system is essential to both locating potential dangers and preventing them from occurring.

REFERENCES

1. Khan NA, Ansari MT. Ransomware: a digital extortion. Int J Adv Innov Res. 2019; 6 (4): 47–52.
2. Ali M, Jung LT, Sodhro AH, Laghari AA, Belhaouari SB, Gillani Z. A confidentiality-based data classification-as-a-service (C2aaS) for cloud security. Alexandria Eng J. 2023; 64: 749–760.
3. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud security threats and solutions: a survey. Wireless Pers Commun. 2023; 128 (1): 387–413.
4. Mohammad AH. Ransomware evolution, growth and recommendation for detection. Mod Appl Sci. 2020; 14 (3): 68–74.
5. Mallikarjunaradhya V, Pothukuchi AS, Kota LV. An overview of the strategic advantages of AI-powered threat intelligence in the cloud. J Sci Technol. 2023; 4 (4): 1–12.
6. Nadeem M, Arshad A, Riaz S, Zahra S, Rashid M, Band SS, Mosavi A. Preventing cloud network from spamming attacks using cloudflare and KNN. Computers Mater Continua. 2023; 74 (2): 2641–2659.
7. Reshmi TR. Information security breaches due to ransomware attacks – a systematic literature review. Int J Inform Manage Data Insights. 2021; 1: 100013.
8. Kapoor A, Gupta A, Gupta R, Tanwar S, Sharma G, Davidson IE. Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability. 2021; 14 (1): 8.
9. Razaulla S, Fachkha C, Markarian C, Gawanmeh A, Mansoor W, Fung B, Assi C. The age of ransomware: a survey on the evolution, taxonomy, and research directions. IEEE Access. 2023; 11: 10698–40723.
10. Oz H, Arış A, Levi A, Uluagac S. A survey on ransomware: evolution, taxonomy, and defense solutions. ACM Comput Surveys. 2022; 54 (11): Article 238.
11. Chen Z-G, Kang H-S, Yin S-N, Kim S-R. Automatic ransomware detection and analysis based on dynamic API calls flow graph: In: RACS'17: Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Krakow, Poland, September 20–23, 2017. pp. 196–201.
12. Aljubory N, Khammas BM. Hybrid evolutionary approach in feature vector for ransomware detection. In: 2121 International Conference on Intelligent Technology, Systemand Service for Internet of Everything (ITSS-IoE), Sana'a, Yemen, November 1–2, 2021. pp. 1–6.
13. Arshad A, Nadeem M, Riaz S, Zahra SW, Dutta AK, Alzaid Z, Alabdan R, Almutairi B, Almotairi S. Hill Matrix and Radix-64 bit algorithm to preserve data confidentiality. Computers Mater Continua. 2023; 75 (2): 3065–3089.
14. Fang C, Nazari N, Omidi B, Wang H, Puri A, Arora M, Rafatirad S, Homayoun H, Khasawneh KN. HeteroScore: evaluating and mitigating cloud security threats brought by heterogeneity. In: Network and Distributed System Security (NDSS) Symposium, San Diego, CA, USA, February 27–March 3, 2023. pp. 1–15.
15. Saddheer M, Ahmad W, Nadeem M, Zahra SW, Arshad A, Riaz S. A decrease in the encryption latency utilizing transport layer protocols for software defined networks. J Netw Security. 2023; 11 (1): 24–38.
16. Kousalya A, Baik NK. Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique. Int J Intell Netw. 2023; 4: 62–67.
17. Cabaj K, Gregorczyk M, Mazurczyk W. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. Computers Electr Eng. 2018; 66: 353–368.
18. Sheik SA, Muniyandi AP. Secure authentication schemes in cloud computing with glimpse of artificial neural networks: a review. Cyber Security Appl. 2023; 1: 100002.
19. Zahra SW, Nadeem M, Ramzan A, Ahmad W, Arshad A, Riaz S, Saddheer M. Enhancing the cloud data security using keeper key and kernel tag. J Adv Shell Program. 2023; 10 (1): 35–46.

20. Wani A, Revathi S. Ransomware protection in IoT using software defined networking. Int J Electr Computer Eng. 2020; 10 (3): 3166–3175.
21. Ayesha JAK, Ahmad W, Nadeem M, Zahra SW, Arshad A, Riaz S, Shahid U. Baggage detection and recognition using local tri-directional pattern. Int J Mobile Comput Technol. 2023; 1 (1): 8–17.
22. Mathane V, Lakshmi PV. Predictive analysis of ransomware attacks using context-aware AI in IoT systems. Int J Adv Computer Sci Appl. 2021; 12 (4): 240–244.
23. Nadeem M, Arshad A, Riaz S, Zahra S, Dutta A, Moteri M, Alaybani S. An efficient technique to prevent data misuse with matrix cipher encryption algorithms. Computers Mater Continua. 2022; 74: 4059–4079.
24. Nadeem M, Arshad A, Riaz S, Zahra S, Band SS, Mosavi A. Two layer symmetric cryptography algorithm for protecting data from attacks. Computers Mater Continua. 2022; 74: 2625–2640. doi: 10.32604/cmc.2023.030899.
25. Nadeem M, Arshad A, Riaz S, Zahra S, Dutta Ashit, Alruban A, Almutairi B, Alaybani S. Two-layer security algorithms to prevent attacks on data in cyberspace. Appl Sci. 2022; 12: 9736. doi: 10.3390/app12199736.
26. Hossain ME. Enhancing the security of Caesar Cipher algorithm by designing a hybrid cryptography system. Int J Computer Appl. 2021; 183 (21): 55–57.
27. Akanksha D, Samreen R, Niharika GS, Shruthi A, Kiran MJ, Venkatramulu S. A hybrid cryptosystem based on modified vigenere cipher and polybius cipher. EPRA Int J Res Dev. 2022; 7 (6): 113–119.
28. Sun H, Grishman R. Lexicalized dependency paths based supervised learning for relation extraction. Computer Syst Sci Eng. 2022; 43 (3): 861–870.
29. Tan CMS, Arada GP, Abad AC, Magsino ER. A hybrid encryption and decryption algorithm using Caesar and Vigenere Cipher. J Phys Conf Ser. 2021; 1997 (1): 012021.
30. Krishnamoorthy N, Umarani S. Implementation and management of cloud security for Industry 4.0-data using hybrid elliptical curve cryptography. J High Technol Manage Res. 2023; 34 (2): 100474.
31. Sundar K, Sasikumar S, Jayakumar C, Nagarajan D, Karthick S. Quantum cryptography based cloud security model (QC-CSM) for ensuring cloud data security in storage and accessing. Multimedia Tools Appl. 2023; 82: 4281742832.
32. Wu Y, Kang Z, Dai T, Cheng D. Managing cloud security in the presence of strategic hacker and joint responsibility. J Oper Res Soc. 2023. In press. doi: 10.1080/01605682.2023.2249506.
33. Alqahtani A, Sheldon FT. A survey of crypto ransomware attack detection methodologies: an evolving outlook. Sensors. 2022; 22 (5): 1837.
34. Tandon A, Nayyar A. A comprehensive survey on ransomware attack: a growing havoc cyberthreat. In: Balas V, Sharma N, Chakrabarti A, editors. Data Management, Analytics and Innovation. Advances in Intelligent Systems and Computing, Volume 839. Singapore: Springer; 2019. pp. 403–420.
35. Rehman F, Muhammad Z, Asif S, Rahman H. The next generation of cloud security through hypervisor-based virtual machine introspection. In: 2023 3rd International Conference on Artificial Intelligence (ICAI), Islamabad, Pakistan. February 22–23, 2023. pp. 116–121.
36. Malecki F. Best practices for preventing and recovering from a ransomware attack. Computer Fraud Security. 2019; 3: 8–10.
37. George AS, Sagayarajan S. Securing cloud application infrastructure: understanding the penetration testing challenges of IaaS, PaaS, and SaaS environments. Partners Univ Int Res J. 2023; 2 (1): 24–34.

