International Journal of Safety and Security Engineering
Vol. 14, No. 6, December, 2024, pp. 1963-1973
Journal homepage: http://iieta.org/journals/ijsse

Machine Learning Approaches to Ransomware Detection: A Comprehensive Review

Shayma Jawad*, Hanaa Mohsin Ahmed

Department of Computer Sciences, University of Technology, Baghdad 10066, Iraq

Corresponding Author Email: cs.21.04@grad.uotechnology.edu.iq

https://doi.org/10.18280/ijsse.140630

Received: 17 August 2024
Revised: 10 December 2024
Accepted: 18 December 2024
Available online: 31 December 2024

Keywords:
ransomware, prevention, detection, classification, machine learning, cybersecurity

ABSTRACT

Ransomware is a widespread and dangerous cyberattack that encrypts data on systems and demands payment for decryption. This research provides a comprehensive review of ransomware detection methods, emphasizing machine learning-driven approaches. It explores dynamic analysis techniques, assesses detection frameworks, and highlights tools like SentinelOne and SandBlast Anti-Ransomware. Studies conducted between 2018 and 2023 were examined to compile the latest findings. The review underscores the effectiveness of predictive methods, with one approach achieving 99.9% accuracy using a pre-encryption detection algorithm. This work provides a valuable resource for understanding ransomware threats and offers actionable insights for enhancing detection and mitigation strategies.

1. INTRODUCTION

Ransomware is a type of malware that encrypts files on a device, rendering both the files and the systems dependent on them inoperable. In recent years, ransomware incidents have surged nationwide, significantly impacting critical infrastructure organizations as well as state, local, tribal, and territorial (SLTT) governments [1, 2].

The ongoing pandemic and increased reliance on remote work have led to numerous attacks globally, exposing vulnerabilities in both public and private IT infrastructures. As highlighted in a recent study by Marais et al. [1], attackers often exploit these vulnerabilities by targeting information systems using ransomware, employing tactics such as exploiting security weaknesses or social engineering [3].

Victims typically face limited options, primarily communicating with the attacker and deciding whether to pay the ransom [4]. Organizations often feel compelled to pay due to the desire to recover valuable data or the fear of losing potential customers. Furthermore, less informed users who wish to regain access to their data are more likely to comply with ransom demands. This situation leads to increasing costs for individuals and organizations as the attacks continue to escalate. The frequency of these attacks is on the rise, driven by the development of new ransomware variants, user-friendly kits (RaaS), and obfuscation techniques, despite ongoing research efforts aimed at countering these threats [5, 6].

The study looks at different types of ransomwares, operating scenarios, and data sets used, providing valuable insights to researchers. It is worth noting that one method using Learning Algorithm (LA) and Pre-Encoder Detection Algorithm (PEDA) achieved exceptional results with a 100% recall rate and 99.9% accuracy through 10-fold cross-validation [4-6]. This approach's ability to identify ransomware before encryption underscores its robustness in cybersecurity, making it highly effective in practical applications [7].

This study aims to develop a robust machine learning framework for detecting ransomware, evaluate the strengths and weaknesses of dynamic analysis techniques, and provide actionable insights into effective ransomware mitigation strategies to enhance cybersecurity resilience [8]. Ultimately, this work aims to fill current gaps in the literature and provide a comprehensive summary to assist future researchers. The insights gained from this study will benefit researchers and developers working to identify effective solutions across various domains [9, 10].

The contribution of this research is as follows: First, it compiles recent ransomware detection studies that focus on dynamic analysis, enhancing the understanding of ransomware behavior and its characteristics. Second, it provides valuable insights for researchers and developers, aiding them in combating ransomware more effectively by drawing from controlled experiments and machine learning models. Finally, this study offers a valuable resource for future research by detailing the latest trends in ransomware and compiling effective detection strategies, helping to guide ongoing efforts in improving ransomware detection and mitigation techniques.

The rest of the paper is structured as follows: Section 2 covers the methodology employed in the study. Section 3 discusses various aspects of ransomware, including its types, typical scenarios, and the impact of ransomware attacks on software and hardware. Section 4 focuses on ransomware analysis, detailing the approaches used to understand and assess ransomware threats. Section 5 explores remediation strategies and ransomware decryption techniques. Section 6 describes the datasets utilized in developing the ransomware detection system. Section 7 reviews existing studies that

address ransomware analysis, detection, protection, and preventive measures. Finally, Section 8 summarizes the findings of the research and discusses potential directions for future studies.

2. RANSOMWARE: AN OVERVIEW

Ransomware is a type of malware that restricts user access to data until a ransom is paid. It has evolved into a profitable cybercrime model, often facilitated through Ransomware-as-a-Service (RaaS), where cybercriminals provide ransomware tools in exchange for a fee or profit-sharing. This collaborative ecosystem allows criminals to specialize in various aspects of the attack process, increasing the sophistication and reach of ransomware operations [7, 11].

2.1 Types of ransomwares

Locker Ransomwares: This type locks users out of their devices, preventing access to systems or services by blocking the execution of software [1, 12].

Crypto Locker Ransomwares: It encrypts sensitive files and data, making them inaccessible without a decryption key. This ransomware operates covertly, scanning and encrypting files [1, 12].

Scareware: Designed to intimidate victims into paying a ransom, scareware may impersonate authorities or threaten exposure of alleged crimes. Variants like Leakware coerce victims through social pressure and intimidation [7].

2.2 Ransomware attack lifecycle

Ransomware attacks generally progress through five stages [12]:

1. Deployment: The malware executes via phishing or exploiting vulnerabilities.
2. Installation: Using a dropper mechanism, the ransomware installs its program.
3. Command and Control (C2) and Key Exchange: Communication with a remote server provides encryption keys and instructions.
4. Encryption: Specific files are encrypted, rendering them inaccessible without the decryption key.
5. Extortion: The victim receives a ransom demand, often with threats of data loss or increased ransom if payment is delayed.

2.3 Ransomware impact on software and hardware

Ransomware can target both software and hardware:

Software Attacks: These attacks encrypt or lock files, denying access until a ransom is paid. Initial infection often occurs through phishing emails, malicious links, or vulnerabilities in network-facing devices. Tools like Shodan expose weaknesses in internet-connected devices, highlighting the importance of comprehensive security measures [13, 14]. Software ransomware comprises components such as a trigger (e.g., a malicious file download), a cryptographic payload, and a user interface, making it a complex threat.

Hardware Attacks: Although speculative, hardware-based ransomware could target components like hard drives or motherboards, potentially disabling entire systems. However, there are no documented cases of hardware-specific ransomware, and such attacks remain largely theoretical [15, 16].

2.4 Ransomware protection tools

Several tools offer protection against ransomware:

1. Threat Locker: Prevents unauthorized software execution, mitigating damage until removal.
2. ManageEngine Vulnerability Manager Plus: Provides vulnerability scanning, patch management, and system hardening.
3. SpinOne: Features ransomware defense, risk analysis, and secure data backup.
4. Acronis Cyber Protect Home Office: Combines endpoint security with backup and recovery.
5. Malwarebytes Anti-Ransomware: Detects ransomware through behavior analysis.
6. Bitdefender Antivirus Plus: A comprehensive antivirus solution with robust ransomware protection.

3. METHODOLOGY

3.1 Search strategy

A comprehensive review of the literature was conducted by searching databases such as IEEE Xplore, Springer, ACM Digital Library, SpringerLink, Scopus, and Elsevier. The primary emphasis was placed on recent research articles, although a selection of earlier papers was also incorporated. To narrow down the search, specific keyword combinations were utilized, including the key terms "machine learning," "Ransomware Attacks Prevention," "classification," and "Ransomware Attacks." This search strategy yielded relevant research papers.

3.2 Inclusion and exclusion criteria

Research evaluating the performance of machine learning models in the analysis of ransomware attacks was considered. The focus was on studies published between 2018 and 2023, and only studies written in English were included. Selection criteria included studies that addressed (Analysis of Ransomware Detection) using dynamic analysis, with a focus on mitigation tools for ransomware attacks.

Exclusion criteria included papers reporting results solely on those exploring traditional approaches, conference papers not indexed in Scopus, abstracts, preprints, grey literature, book chapters, non-English studies, case reports, and studies unrelated to the specified topic. The following keyword combinations were used: (“e-learning” AND “ransomware attack prevention”), (“taxonomy” AND “ransomware”). Different variations (AND, OR, NOT) were used to combine terms and narrow the search. The search and results management were better modified to improve the quality of retrieved studies.

3.3 Study selection

Initially, a selection of papers was chosen based on the relevance of their titles to our subject. Subsequently, the titles and abstracts of the identified articles were individually evaluated for relevance by all authors. The determination of inclusion or exclusion was made based on the specified

criteria. Adhering to this methodology, comprehensive reviews of the pertinent studies were conducted in full text. Any disagreements regarding the study's relevance were resolved through consensus after both screening and a thorough full-text review.

4. RANSOMWARE ANALYSIS

Malware analysis encompasses the systematic investigation and examination of malicious software to understand its functionality, origins, and operational behavior [17]. This process is crucial for developing effective strategies to detect and combat malware, whether through static or dynamic analysis techniques.

In response to ransomware threats, the scientific community is actively developing advanced techniques for detection, prevention, and prediction. These efforts involve assessing system vulnerabilities, predicting potential attacks, and implementing robust defense mechanisms using intelligent technologies such as Machine Learning (ML), which includes Bayesian networks (BN), decision trees (DT), and support vector machines (SVM), among others. Each approach focuses on specific aspects to ensure information security and mitigate ransomware risks.

4.1 Ransomware detection and prediction

Ransomware detection and prediction have become crucial areas of research in cybersecurity due to the increasing prevalence and sophistication of ransomware attacks. While the terms "detection" and "prediction" are often used interchangeably, some studies refer to the detection phase as "early prediction." The main objective of prediction is to prevent ransomware attacks before they occur by collecting data from endpoint devices about their behavior and network connections. This data is then analyzed and correlated to identify potential threats. Predictive methods, especially those involving intelligent algorithms, help users take preemptive measures against anticipated threats, thereby minimizing or even preventing attacks altogether.

Machine learning (ML) methods have become increasingly important in ransomware prediction due to their ability to analyze complex attack patterns and behaviors. The strength of ML lies in its ability to detect patterns within large datasets, provided that the data is sufficient and representative. However, the challenge lies in selecting the optimal ML approach that aligns with the specific characteristics of the data and the desired outcome. Recent research has shown that deep learning (DL) techniques, particularly those used in intrusion detection, offer superior performance in detecting ransomware attacks.

Numerous studies have introduced a wide range of machine learning (ML) algorithms to enhance ransomware detection, with each approach focusing on improving detection accuracy and addressing the unique challenges posed by evolving ransomware tactics. These studies leverage diverse techniques, from traditional classification methods to advanced deep learning models, to optimize performance across different environments and datasets.

One study [18] applied Z-score standardization along with various machine learning classifiers and neural network architectures to detect ransomware. The results revealed that Random Forest (RF), Logistic Regression (LR), and Neural Networks (NN) achieved an impressive mean Area Under the Curve (AUC) score of 0.99, significantly outperforming Naive Bayes, which had a much lower AUC of 0.73. A paired t-test confirmed that these results were statistically significant (p-value < 0.05), and the Z-score method demonstrated its robustness with a confidence interval for AUC between 0.96 and 1.00.

Researchers employed Binary Code Analysis to process ransomware binaries and analyze the activity sequences they generate [19]. The use of decision tree classifiers led to an accuracy of 97.1%, while Random Forest classifiers achieved an exceptional 99.9% accuracy in a Windows environment, underscoring the effectiveness of machine learning in detecting ransomware threats.

Another important study [20] incorporated Recursive Feature Elimination with Cross-Validation (RFECV) to optimize model performance, utilizing a variety of machine learning algorithms such as LR, Stochastic Gradient Descent (SGD), K-Nearest Neighbors (KNN), Naive Bayes (NB), RF, and Support Vector Machine (SVM). The dataset was sourced from the "GetRansomware" web crawler, dataset includes 1,200 samples (700 malicious and 500 benign), with features such as entropy, byte frequency, and process behavior logs. The researchers achieved a high accuracy of 99.15%, which highlighted the importance of feature selection in enhancing the performance of machine learning models for ransomware detection.

A study [21] used Correlation-based Feature Selection (CFS) on a dataset containing 582 ransomware samples and 942 goodware samples. The results showed that the XGBoost algorithm achieved precision and recall values of 0.96 and 0.99, respectively, demonstrating its high reliability in distinguishing between ransomware and legitimate software.

Researchers explored the application of advanced deep learning models, including Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks, to detect ransomware [8]. The study achieved an accuracy of 97%, with an Area Under the Curve (AUC) greater than 98% and an average F1-score of under 1.88%, showing the effectiveness of sophisticated neural network architectures in ransomware detection.

Another study [9] employed a neural network model to assess the impact of crypto-ransomware traffic on network security. This model successfully identified 100% of previously unseen crypto-ransomware binaries, leading to a recorded data loss of 99 MB. The study highlighted the model's ability to perform real-time threat detection, which is crucial for safeguarding networks against emerging ransomware threats.

Further research [10] evaluated a range of machine learning techniques, including Support Vector Machine (SVM), Random Forest, and Naive Bayes, to detect ransomware. The results showed that both SVM and Random Forest achieved an accuracy of 99.5%, while Naive Bayes had a solid accuracy of 96%, demonstrating the reliability of these methods in malware detection.

Finally, a study [22] investigated the role of entropy, a measure of uniformity, in improving ransomware detection. The study examined several machine learning models, such as logistic regression, linear SVM, decision trees, random forests, gradient boosting trees, and Multi-Layer Perceptron (MLP), with detection rates ranging from 91% to 99%. The study emphasized the importance of entropy in enhancing the performance of detection models. Table 1 summarizes the key findings from these studies.

Table 1. A summary of ransomware detection

Ref.	Technique		Dataset	PC/Mobile	Result
	Feature Selection / Extraction	Detection			
[23]	Z-score standardization technique	ML classifiers and NN-based architecture detect ransomware using traditional methods.	70% are ransomware. 30% are legitimate observations	-	RF, LR, NN achieved highest mean AUC (0.99) scores, while NB had lowest (0.73)
[18]	Binary code analysis (BCA)	Using ML approaches, real-world ransomware binaries and activity sequences are processed and analyzed.	ransomware datasets	Windows	DT and RF classifiers achieve detection rates of 97.1% and 99.9%, respectively
[19]	"Recursive Feature Elimination with Cross-Validation (RFECV) / Application Programming Interface (API)"	ML algorithms to detect and classify (LR, SGD, KNN, NB, RF, SVM)	Web-Crawler i.e., 'GetRan somware'	Windows	Achieved accuracy of 99.15%
[20]	Correlation-based Feature Selection (CFS) technique is featuring selection	ML models are DT, RF, KNN, SVM, XGBoost and LR.	Dataset include: ✓ 582 ransomwar e samples. ✓ 942 ✓ goodware samples	Windows	**Name** **Prec.** **Recall** DT 0.92 0.97 RF 0.92 0.98 KNN 0.89 0.95 SVM 0.93 0.97 XGB 0.96 0.99 LR 0.97 0.98
[21]	Python programming was used for CSV file creation, grouping, frequency generation, and feature extraction	DNN, CNN, and (LSTM) recurrent neural network	447 normal samples and 561 malware samples totaling 1008	Windows 10 OS	ACC achieve 97% AUC achieve more than 98% F1-score with a far of under 1.88% on average
[8]	Crypto-ransomware programs read and write vast numbers of bytes	Neural network model (NN)	Crypto-ransomware traffic infected; staff office users accessing shared files uninfected	Windows	Identified 100% of 10 unutilized crypto-ransomware binaries with 99 MB data loss
[9]	Malware Analysis	"ML Techniques: ✓ SVM ✓ random forest ✓ Naive Bayes"	Ransomware dataset	Windows 10	SVM and random forest accuracy of 99.5%, and the Naive Bayes method accuracy of 96%
[10]	Entropy is one of the approaches used to measure uniformity in the study	"ML models: ✓ logistic regression ✓ linear SVM ✓ DT ✓ random forest ✓ gradient boosting tree ✓ SVM ✓ MLP."	-	-	Different detection rates, from a minimum of 91% to a maximum of 99%, were attained

4.2 Ransomware prevention and mitigation

Ransomware prevention focuses on proactive measures aimed at reducing the risk of ransomware attacks by addressing vulnerabilities before they can be exploited. Common strategies include upgrading operating systems, employing specialized security software, and maintaining regular file backups. The primary objective during this stage is to identify and mitigate potential security flaws that could be targeted by ransomware attackers [24].

One of the key challenges in ransomware prevention is detecting the source of attacks, particularly those involving data extortion or kidnapping, which often makes it difficult to trace perpetrators. Effective prevention measures enable users to prevent ransomware infections or recover files, thus breaking the cycle of attacks. The following are key preventative measures to mitigate the risk of ransomware attacks:

1. Regular Data Backups: Regularly backing up data and storing it off-site is essential for quickly restoring files in the event of ransomware encryption. However, organizations often face challenges regarding the time and cost required for backup processes, with some backups consuming large storage capacities, potentially slowing down system performance. Maintaining reliable and efficient backup systems is crucial, even with the associated costs and time investments [25].
2. Caution with Email Attachments: Users should exercise caution when opening unsolicited email attachments, as these are common vectors for ransomware delivery.
3. Limit Administrator Access: To minimize the risk of ransomware infections, it is recommended to avoid prolonged sessions logged in as an administrator and limit internet browsing or document access while using administrator privileges.
4. Awareness of Social Engineering: Users should remain vigilant against malicious links on social media and messaging platforms, even if they appear to come from trusted contacts.

5. Firewall and Security Settings: It is essential to maintain Windows Firewall functionality and configure additional security measures, such as blocking malicious IP addresses, to enhance overall protection against ransomware attacks.
6. Use Antivirus and Anti-Malware Software: Installing reputable antivirus and anti-malware software, along with performing regular scans, is an effective method to detect and eliminate potential threats before they can cause harm.
7. Cybercriminal Insurance: As ransomware attacks continue to proliferate globally, many organizations have suffered significant financial losses due to these threats, leading to dire consequences such as bankruptcy, divestment by investors, or severe financial strain [25]. As a result, cybercriminal insurance has become increasingly important for organizations to mitigate the financial risks associated with ransomware attacks.

In today's threat landscape, leveraging specialized anti-ransomware software is vital for comprehensive protection. Effective anti-ransomware tools should be capable of detecting suspicious behaviors, providing proactive defense against attacks, and offering mechanisms for file remediation. Many anti-ransomware solutions are now equipped with forensic and behavioral analysis tools that can detect, block, and even decrypt encrypted files [24].

5. REMEDIATION AND RANSOMWARE DECRYPTION

Remediation involves removing persistence mechanisms, recovering deleted files, and reverting changes to the registry. Several commercially patented tools integrate detection, mitigation, and cleanup to counter ransomware. While detailed performance data are proprietary, company claims provide insights into their functionality [26].

SentinelOne employs dynamic process behavior analysis throughout the threat lifecycle, using Machine Learning (ML) and proprietary algorithms. It blocks malicious activities, halts associated processes, and utilizes the Windows Volume Shadow Copy Service (VSS) for encrypted data restoration. This approach ensures effective rollback of ransomware modifications (see Figure 1) [27].

Checkpoint's SandBlast Anti-Ransomware operates similarly but uses a VSS implementation instead of SentinelOne's proprietary algorithms [28]. Some poorly constructed ransomware, despite employing strong encryption like AES256 and RSA-2048, contain vulnerabilities. These flaws allow analysts to extract encryption keys or decrypt files directly. Initiatives like NoMoreRansom, a collaboration among Europol, Kaspersky Lab, and others, provide free decryption tools for victims [26, 29].

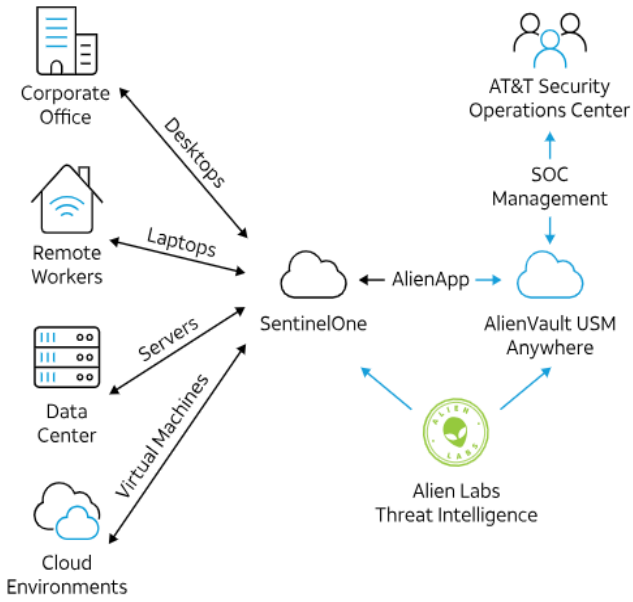

Figure 1. SentinelOne [27]

6. THE IMPORTANCE OF DATASETS

Datasets are vital for developing accurate ransomware detection systems. Examples include:

- Kaggle Ransomware Competition: Provided encrypted and decompiled ransomware samples for AI model development.
- Malware-Traffic-Analysis.net: Offers network traffic data to analyze ransomware behavior patterns.

Figure 2 illustrates how the quality of the dataset influences the creation of an adaptive detection model, emphasizing the importance of using trustworthy and dependable data.

High-quality datasets ensure reliable detection models, emphasizing their critical role in combating ransomware.

Figure 2. Importance of datasets in ransomware detection system development [5]

7. OVERVIEW OF EXISTING RANSOMWARE DETECTION, PREVENTION, AND MITIGATION STRATEGIES

The field of ransomware detection, prevention, and mitigation has seen significant research efforts over the years. However, due to the rapid evolution of ransomware tactics, many previous studies have become outdated or less relevant. This section provides a comprehensive overview of prior research, comparing different techniques and summarizing their outcomes (see Table 2).

Table 2. Summarize state of art

Ref.	Contributions	Tools/Methods	Results	Limitations/Future Direction
[1]	• The first model detects malicious files, and the second model determines if the file is ransomware or not. • This approach is flexible and can be independently trained, making it useful for optimization and production environments.	• ML and DL algorithms • Features that the Ember extractor that retrieve from PE files, three models are trained (XGBoost, DNN, lightgbm)	They found that XGBoost, lightgbm, and DNN had good performances with an average accuracy score of 0.9947.	Hacker methods constantly change, causing persistent cybercrime and virus attacks. Explore new ideas or suggest adjustments.
[30]	A new strategy based on static analysis and ML that successfully distinguishes between good ware and ransomware files while successfully detecting and classifying ransomware using n-gram features and gain ratio approach.	Use Linux object-code dump tool and portable executable processor for converting binaries to assembly-level instructions and dynamic link libraries.	98.33% detection accuracy was attained using the RF ML model.	Limitations of dynamic sandboxing for ransomware detection include ransomware recognition and command line parameter ignorance.
[31]	The contribution of this paper is proposing a solution to mitigate the Sodinokibi ransomware attack on cloud networks using Software-Defined Networking (SDN).	The proposed solution utilizes the SDN controller to monitor and control network traffic, detect and isolate infected hosts.	The mitigation system can reduce virus spread by 17.13% and suppress Sodinokibi traffic records by up to 73.97%.	Mitigation limitation: SDN Ryu controller commands and applications limited to TCPUDP and ICMP protocols.
[4]	Article presents dynamic analysis of WannaCry ransomware in a controlled virtual lab, focusing on infection, persistence, recovery, prevention, and dissemination mechanisms.	The method that used is dynamic analysis, which involves executing the malicious software (in this case, WannaCry ransomware) in a controlled environment and observing its behavior.	The results achieved in this paper are a better understanding of the behavior and characteristics of WannaCry ransomware through dynamic analysis.	The authors plan to explore this approach as a potential solution for defending against WannaCry and other similar types of ransomwares.
[32]	Hybrid approach investigates permissions, text, network features using memory usage and system performance.	Ensemble learners use various classifiers like C4.5, Random Forest, JRip, Logistic Regression, SVM, AdaBoost.	High-accuracy Android malware detection, resisting adversarial evasion; exception: ensemble with 0.9 precision and F-Measure.	Future work should focus on countering circumvention attacks, identifying subsets, and improving ML classifier resilience.
[33]	Study identifies 14 APIs for early ransomware detection and prevention, enhancing security.	• Pre-Encryption Detection Algorithm detects crypto-ransomware before encryption using signature comparison and Learning Algorithm based on pre-encryption API. • Applications such as Cuckoo Sandbox and mysql	LA achieved 100% recall using 80:20 training and 99.9% using 10-fold cross-verification test.	PEDA should be developed so that it can be used independently of other apps without requiring a special configuration.
[34]	the proposed method has able to discriminate between the two types of applications with high accuracy.	• Heldroid, R-packdroid, and a hybrid static-dynamic approach. • ML techniques, process monitoring, and logic rules for detecting Android ransomware.	The precision of the proposed method is 0.96, the recall is 0.97, and the F-measure is 0.96.	The technology will be tested on a larger dataset in the future, and it will be used to applications designed for the Apple mobile environment.
[35]	The construction and evaluation of a ML model dubbed NetConverse, which leverages network traffic conversation data to accurately identify	• ML classifiers: (BN, DT, K-Nearest Neighbours, Multi-Layer Perceptron, RF, and Logistic Model Tree).	The DT (J48) classifier, which had the highest detection rate accuracy of 97.1%, came in second with a detection rate	Future research can build on this work to expand the dataset and improve the detection method by extracting more attributes.

	Windows ransomware, is the contribution of this study.	• TShark for feature extraction. • use of Virus Total Intelligence platform to collect goodware samples.	accuracy of 96.8%, according to the data.	
[36]	Study presents data analytics methodology for automatically identifying ransomware and malicious Bitcoin addresses, improving precision and recall in ransomware detection.	A combination of TDA and novel blockchain graph related features.	TDA and blockchain graph features enhance Bitcoin address identification accuracy in ransomware.	Future research should integrate the strategy with other techniques and threat intelligence data to enhance forecast accuracy.
[37]	The paper identifies ransomware traits and suggests a technique for detection using patterns infected files follow when destroying registries.	Cuckoo Sandbox and ResNet-18 neural network architecture are highlighted, along with feature engineering procedures like PCA and N-gram analysis, and machine learning classifiers like SVM and Random Forest.	Static analysis in Random-forest yields accuracy of 98% with a false negative rate of 0.03.	N-Gram approach identifies sequences for comparing malicious and benign file behavior, enhancing prediction accuracy and reducing computational time using genetic algorithms.
[38]	Paper's contribution by creating a method to detect ransomware, independent of the individual virus strain, when it is encrypting data.	DL -based techniques like CryptoKnight, dynamic analysis systems like UNVEIL, and programs for spotting cryptographic functions like Cryp-toHunt and K-Hunt.	More than 95% of the encryption keys could be recovered.	The amount and complexity of the dataset under analysis, as well as other variables, may affect how effective this technique performs.
[39]	The paper's contribution is its analysis of the very destructive Hive ransomware, which first surfaced in June 2021 and seriously injured businesses.	• UNVEIL • Cryp-toHunt • K-Hunt • CryptoKnight	The master key was retrieved by the authors by resolving XOR equations from encrypted files, and they experimentally confirmed a 95% success rate in key recovery, which may be useful for Hive ransomware victims.	When the encryption algorithm has changed, this technique might not work for subsequent versions of Hive ransomware or other forms of ransomware.
[40]	The contribution of this study is to provide an efficient ransomware recovery system for XML documents called self-healing version-aware ransomware recovery (SH-VARR).	SH-VARR architecture for XML document recovery against ransomware assaults.	The outcomes demonstrated that the solution employing the default zip strategy may defend XML-based data from ransomware assaults.	The suggested SH-VARR framework's drawbacks are not specifically mentioned in the research. However, it is crucial to remember that, like any other system or strategy, there can be potential restrictions or disadvantages.
[41]	Customized recurrent neural networks utilize attention processes to identify local event patterns in ransomware sequences, demonstrating improved LSTM models' effectiveness on Windows-targeted sequences.	• Recurrent Neural Networks • Enhanced LSTM models	This study does not mention any specific limitations of the study or the proposed method.	**Model** / **Accuracy** LSTM 0.87 ARI-LSTM (L=5) 0.93 ARI-LSTM (L=8) 0.91
[42]	Malware detection by proposing two models based on statistics and machine learning using opcode n-grams.	• Implement models using Naive Bayes, random forest, logistic regression, KNN, and SVM. • Employed MalConv (a type of CNN learning) and byte n-gram for feature extraction in deep learning approaches.	The random forest-based model achieved the highest detection accuracy of 96.29%, outperforming other models in detection performance.	The models are currently limited to detecting character-based DGA botnet malware. The false alarm rate is relatively high. Future work will focus on improving detection accuracy and exploring other feature extraction methods such as TF-IDF, bag-of-words, and Word2vec (Detecting Malware Based).

A dual-model approach was proposed for detecting malicious files and identifying ransomware [1]. The models are independently trainable, which allows for optimization in different production environments. By leveraging both Machine Learning (ML) and Deep Learning (DL) algorithms and using features extracted from Portable Executable (PE) files, the study utilized XGBoost, DNN, and lightgbm models, achieving an impressive average accuracy of 99.47%. However, the continuous evolution of hacker tactics calls for ongoing exploration of new strategies to counter cybercrime effectively.

A 2019 study focused on dynamic analysis and examined

the behavior of WannaCry ransomware through controlled virtual lab experiments [4]. This approach proved to be vital for developing effective prevention and recovery strategies. Future research should validate dynamic analysis as a robust defense mechanism to mitigate emerging ransomware threats.

A novel strategy based on static analysis and ML techniques was presented to distinguish between benign and ransomware files [30]. The study achieved a high detection accuracy of 98.33% using Random Forest models. The study utilized Linux object-code dump tools and portable executable processors to convert binaries into assembly-level instructions. However, limitations in dynamic sandboxing techniques were noted, highlighting the need for improvements in ransomware recognition and handling of command-line parameters.

The researchers proposed a solution leveraging Software-Defined Networking (SDN) to mitigate Sodinokibi ransomware attacks on cloud networks [31]. By using an SDN controller to monitor and control network traffic, the system reduced the virus spread by 17.13% and suppressed Sodinokibi traffic by 73.97%. Future research should focus on expanding SDN capabilities beyond traditional protocols such as TCP/UDP and ICMP to enhance adaptability against evolving ransomware tactics.

A hybrid approach that integrated permissions, textual analysis, and network features was employed for android malware detection [32]. The study achieved high accuracy using ensemble learners and various classifiers such as C4.5, Random Forest, and SVM, demonstrating resilience against adversarial evasion tactics. Future research should enhance defense mechanisms against circumvention attacks and improve the robustness of ML classifiers to ensure continued efficacy in malware detection.

The researchers introduced a Pre-Encryption Detection Algorithm aimed at identifying critical APIs for early ransomware detection [33]. This approach achieved 100% recall under specific training conditions, emphasizing the importance of developing standalone applications that do not require specialized configurations, thus enhancing the practicality and usability of ransomware detection systems.

A hybrid static-dynamic approach was applied to discriminate Android ransomware, achieving precision and recall metrics of 0.96 [34]. Future work aims to expand these methodologies to larger datasets and apply them to iOS environments, thereby increasing the applicability of ransomware detection across mobile platforms.

The NetConverse model, introduced in 2018, utilized network traffic data to identify Windows ransomware [35]. The Decision Tree (J48) classifier emerged as the top performer, achieving an accuracy rate of 97.1%. Future enhancements could focus on enriching the model with additional attributes to improve its detection capabilities and adaptability to new ransomware variants.

A data analytics methodology combining Topological Data Analysis (TDA) and blockchain graph features was introduced to enhance Bitcoin address identification accuracy in ransomware cases [36]. Future research could integrate this methodology with broader threat intelligence datasets to improve predictive accuracy and strengthen defense against ransomware attacks.

Static analysis using machine learning classifiers was explored for WannaCry ransomware detection, achieving 98% accuracy using N-gram approaches and SVM models [37]. Future developments should optimize computational efficiency and broaden the predictive capabilities across different ransomware families and attack vectors.

The study focused on DL-based techniques such as CryptoKnight for recovering encryption keys, showing promising results in mitigating ransomware attacks [38]. Future research should address dataset complexities and improve algorithmic robustness to maintain effectiveness against evolving ransomware encryption techniques.

The analysis of Hive ransomware demonstrated a 95% success rate in recovering encryption keys [39]. As ransomware encryption techniques evolve, future research will need to adapt to these changes to ensure sustained efficacy in supporting victims affected by newer variants.

SH-VARR, a self-healing version-aware ransomware recovery system, was introduced for XML documents [40]. The study demonstrated effectiveness against ransomware attacks, but future work should address system-specific limitations and scalability issues to ensure the solution's robustness and reliability.

Customized recurrent neural networks were employed to improve LSTM models for identifying ransomware patterns with high accuracy on Windows-based sequences [41]. Future research should validate these findings across different operating systems and enhance model adaptability to diverse ransomware behaviors and attack scenarios.

The study reviewed various strategies for defending against ransomware, including backup solutions, network segmentation, and user education [42]. The quantitative analysis of ransomware incidents revealed that regular backups reduce incidents by 40%, network segmentation cuts the spread by 35%, and user education increases awareness by 30%. The study advocates for a multi-layered defense strategy, recommending the incorporation of advanced ML models and real-time threat detection systems to further reduce ransomware risks.

Two malware detection models based on statistical methods and ML on opcode n-grams were proposed [25]. The random forest model achieved the best results, with 96.29% accuracy and a 96.15 F1-score. Future work should explore other feature extraction methods like TF-IDF and Word2vec to enhance detection accuracy [43, 44].

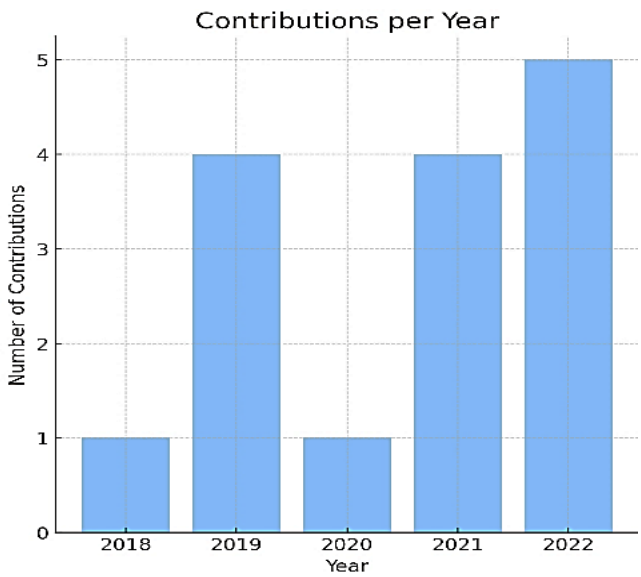

Figure 3. Publications per year

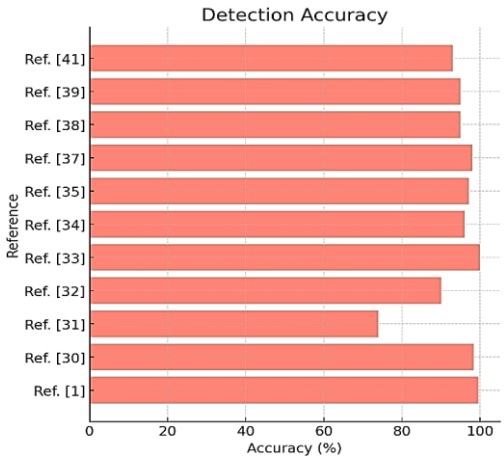

Figure 4. The achieved accuracy per study

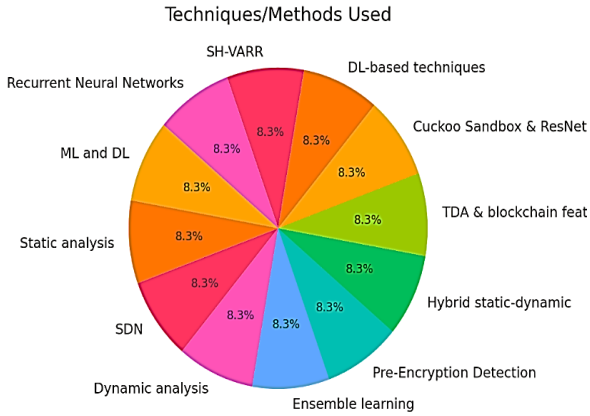

Figure 5. The methods used in the literature

Table 2 summarizes the accomplishments and limitations of the reviewed studies, while Figures 3-5 illustrate the publications per year and other relevant aspects of the studies discussed.

8. CONCLUSION

This study provides a comprehensive overview of ransomware attacks, detailing the types of ransomware, their methods of deployment, and their impact on victims. The attack vector influences the type of ransomware used, affecting the scale and scope of the assault. Our findings emphasize the importance of deploying security tools and backing up data as crucial steps to mitigate the severity of ransomware attacks. Regardless of the type, ransomware poses a significant threat to individuals and businesses. We presented state-of-the-art detection methods and assessed their potential for future ransomware detection by examining vulnerabilities that ransomware may exploit in future versions to evade detection and remediation. The study underscores the dynamic nature of ransomware and the need for continuous adaptation in detection methodologies.

For practitioners, the findings highlight the importance of staying updated with the evolving ransomware landscape and adopting multi-layered security approaches. The study's insights can inform the development of more robust and adaptive ransomware detection and prevention systems. Additionally, the analysis of real-world ransomware scenarios and detection techniques offers practical guidance for cybersecurity professionals to enhance their incident response strategies. Implementing offline or immutable backups can help prevent data from becoming inaccessible during an attack.

9. FUTURE WORK

Future work should focus on exploring and validating dynamic analysis as a robust defense mechanism against emerging ransomware threats. There is a need for continued investigation into machine learning and artificial intelligence models to improve ransomware detection accuracy and efficiency. Additionally, expanding the applicability of detection methodologies to various operating systems and environments, such as mobile platforms and cloud networks, can further strengthen the defense against ransomware attacks.

As the criminal underworld expands its automated extortion reach, we can anticipate advancements in ransomware tactics, including more stable attack vectors, refined demands, sophisticated second-wave attacks targeting vulnerable users, improved evasion techniques, and exploit kits using data mining for social engineering and malware detection. Understanding these trends will be crucial in developing future-proof defense strategies.

As depicted in Table 2, ransomware detection employs various techniques such as signature matching, hashing, entropy analysis, and others. Machine learning (ML) based systems are increasingly favored for their effectiveness and resilience in this domain. The efficacy of these ML models heavily relies on the quality and relevance of the features used during training. Therefore, meticulous feature engineering plays a crucial role in crafting a robust ransomware detection system.

REFERENCES

[1] Marais, B., Quertier, T., Morucci, S. (2022). AI-based malware and ransomware detection models. In Conference on Artificial Intelligence for Defense, Rennes, France. https://hal.science/hal-03881198v1.

[2] Ransomware Guide. Multi-State Information Sharing and Analysis Center (MS-ISAC).

[3] Rani, N., Dhavale, S.V., Singh, A., Mehra, A. (2022). A survey on machine learning-based ransomware detection. In Proceedings of the Seventh International Conference on Mathematics and Computing: ICMC 2021. Springer, Singapore, pp. 171-186. https://doi.org/10.1007/978-981-16-6890-6_13

[4] Akbanov, M., Vassilakis, V.G., Logothetis, M.D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology, 75(1): 113-124. https://doi.org/10.26636/jtit.2019.130218

[5] Urooj, U., Al-rimy, B.A.S., Zainal, A., Ghaleb, F.A., Rassam, M.A. (2022). Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. Applied Sciences, 12(1): 172. https://doi.org/10.3390/app12010172

[6] Popli, N.K., Girdhar, A. (2019). Behavioural analysis of recent ransomwares and prediction of future attacks by polymorphic and metamorphic ransomware. In Computational Intelligence: Theories, Applications and Future Directions-Volume II: ICCI-2017. Springer, Singapore, pp. 65-80. https://doi.org/10.1007/978-981-13-1135-2_6

[7] Kok, S.H., Abdullah, A., Jhanjhi, N.Z., Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers, 8(4): 79. https://doi.org/10.3390/computers8040079

[8] Basnet, M., Poudyal, S., Ali, M.H., Dasgupta, D. (2021). Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. In 2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America), Lima, Peru, pp. 1-5. https://doi.org/10.1109/ISGTLatinAmerica52371.2021.9543031

[9] Berrueta, E., Morato, D., Magaña, E., Izal, M. (2022). Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. Expert Systems with Applications, 209: 118299. https://doi.org/10.1016/j.eswa.2022.118299

[10] Egunjobi, S., Parkinson, S., Crampton, A. (2019). Classifying ransomware using machine learning algorithms. In Intelligent Data Engineering and Automated Learning–IDEAL 2019. Springer, Cham, pp. 45-52. https://doi.org/10.1007/978-3-030-33617-2_5

[11] Al-Rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74: 144-166. https://doi.org/10.1016/j.cose.2018.01.001

[12] Hernandez-Castro, J., Cartwright, A., Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. Royal Society Open Science, 7(3): 190023. https://doi.org/10.1098/rsos.190023

[13] Liska, A., Gallo, T. Ransomware 2023. https://www.oreilly.com/library/view/ransomware/9781491967874/ch04.html.

[14] Zimba, A., Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. European Journal for Security Research, 4(1): 3-31. https://doi.org/10.1007/s41125-019-00039-8

[15] Almeida, F., Imran, M., Raik, J., Pagliarini, S. (2022). Ransomware attack as hardware trojan: A feasibility and demonstration study. IEEE Access, 10: 44827-44839. https://doi.org/10.1109/ACCESS.2022.3168991

[16] Martin, H., Peris-Lopez, P., Entrena, L., Natale, G.D. (2017). Ransomware based on hardware trojans. Forget the typical ransomware you should start worrying about hardware. In USENIX Security '17. https://lightweightcryptography.com/wp-content/papercite-data/pdf/c41honorioperis2017.pdf.

[17] Kok, S., Abdullah, A., Jhanjhi, N., Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. IJCSNS International Journal of Computer Science and Network Security, 19(2): 136-146. http://paper.ijcsns.org/07_book/201902/20190217.pdf.

[18] Masum, M., Faruk, M.J.H., Shahriar, H., Qian, K., Lo, D., Adnan, M.I. (2022). Ransomware classification and detection with machine learning algorithms. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 0316-0322. https://doi.org/10.1109/CCWC54503.2022.9720869

[19] Vehabovic, A., Ghani, N., Bou-Harb, E., Crichigno, J., Yayimli, A. (2022). Ransomware detection and classification strategies. In 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sofia, Bulgaria, pp. 316-324. https://doi.org/10.1109/BlackSeaCom54372.2022.9858296

[20] Mowri, R.A., Siddula, M., Roy, K. (2022). Application of explainable machine learning in detecting and classifying ransomware families based on API call analysis. arXiv preprint arXiv:2210.11235. https://doi.org/10.48550/arXiv.2210.11235

[21] Rani, N., Dhavale, S.V. (2022). Leveraging machine learning for ransomware detection. arXiv preprint arXiv:2206.01919. https://doi.org/10.48550/arXiv.2206.01919

[22] Lee, K., Lee, S.Y., Yim, K. (2019). Machine learning based file entropy analysis for ransomware detection in backup systems. IEEE Access, 7: 110205-110215. https://doi.org/10.1109/ACCESS.2019.2931136

[23] Kadhem, S.J., Ahmed, H.M. (2024). Ransomware detection and prevention using machine learning and honeypots: A short review. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 24(2): 29-40. https://doi.org/10.33103/uot.ijccce.24.2.3

[24] Herrera Silva, J.A., Barona López, L.I., Valdivieso Caraguay, Á.L., Hernández-Álvarez, M. (2019). A survey on situational awareness of ransomware attacks—detection and prevention parameters. Remote Sensing, 11(10): 1168. https://doi.org/10.3390/rs11101168

[25] Atetedaye, J. (2024). Ransomware defense strategies: A comprehensive analysis.

[26] Tailor, J.P., Patel, A.D. (2017). A comprehensive survey: Ransomware attacks prevention, monitoring and damage control. International Journal of Scientific Research, 4(15): 116-121. https://www.researchgate.net/publication/321161261.

[27] Christensen, J.B., Beuschau, N. (2017). Ransomware detection and mitigation tool. Ph.D. dissertation. Department of Applied Mathematics and Computer Science, Technical University of Denmark, Lyngby, Denmark.

[28] Checkpoint. Ransomware: A new approach to identifying, blocking. https://www.sentinelone.com/.

[29] Kaspersky Lab. (2021). WannaCry mistakes that can help you restore files. https://thehackernews.com/2017/06/wannacry-ransomware-unlock-files.html.

[30] Khalil, N.A., Khammas, B.M. (2022). An effective and efficient features vectors for ransomware detection via machine learning technique. Iraqi Journal of Information and Communication Technology, 5(3): 23-33. https://doi.org/10.31987/ijict.5.3.205

[31] Umar, R., Riadi, I., Kusuma, R.S. (2021). Mitigating Sodinokibi ransomware attack on cloud network using Software-Defined Networking (SDN). International Journal of Safety and Security Engineering, 11(3): 239-246. https://doi.org/10.18280/ijsse.110304

[32] Ahmed, U., Lin, J.C.W., Srivastava, G. (2022). Mitigating adversarial evasion attacks of ransomware using ensemble learning. Computers and Electrical Engineering, 100: 107903. https://doi.org/10.1016/j.compeleceng.2022.107903
[33] Kok, S.H., Abdullah, A., Jhanjhi, N.Z. (2022). Early detection of crypto-ransomware using pre-encryption detection algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5): 1984-1999. https://doi.org/10.1016/j.jksuci.2020.06.012
[34] Mercaldo, F., Martinelli, F., Santone, A. (2020). Timed automata for mobile ransomware detection. Electronic Communications of the EASST, 79. https://doi.org/10.14279/tuj.eceasst.79.1120
[35] Alhawi, O.M., Baldwin, J., Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. Cyber Threat Intelligence, 93-106. https://doi.org/10.1007/978-3-319-73951-9_5
[36] Akcora, C.G., Li, Y., Gel, Y.R., Kantarcioglu, M. (2019). Bitcoinheist: Topological data analysis for ransomware detection on the bitcoin blockchain. arXiv preprint arXiv:1906.07852. https://doi.org/10.48550/arXiv.1906.07852
[37] Ashraf, A., Aziz, A., Zahoora, U., Rajarajan, M., Khan, A. (2019). Ransomware analysis using feature engineering and deep neural networks. arXiv preprint arXiv:1910.00286. https://doi.org/10.48550/arXiv.1910.00286
[38] Davies, S.R., Macfarlane, R., Buchanan, W.J. (2021). Differential area analysis for ransomware attack detection within mixed file datasets. Computers & Security, 108: 102377. https://doi.org/10.1016/j.cose.2021.102377
[39] Kim, G., Kim, S., Kang, S., Kim, J. (2022). A method for decrypting data infected with hive ransomware. Journal of Information Security and Applications, 71: 103387. https://doi.org/10.1016/j.jisa.2022.103387
[40] Al-Dwairi, M., Shatnawi, A.S., Al-Khaleel, O., Al-Duwairi, B. (2022). Ransomware-resilient self-healing XML documents. Future Internet, 14(4): 115. https://doi.org/10.3390/fi14040115
[41] Agrawal, R., Stokes, J.W., Selvaraj, K., Marinescu, M. (2019). Attention in recurrent neural networks for ransomware detection. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, pp. 3222-3226. https://doi.org/10.1109/ICASSP.2019.8682899
[42] Tiu, Y.L., Zolkipli, M.F. (2021). Study on prevention and solution of ransomware attack. Journal of IT in Asia, 9(1): 133-139. https://doi.org/10.33736/jita.3402.2021
[43] Mutleg, M.L., Mahmood, A.M., Al-Nayar, M.M.J. (2024). A comprehensive review of cyber-attacks targeting IoT systems and their security measures. International Journal of Safety and Security Engineering, 14(4): 1073-1086. https://doi.org/10.18280/ijsse.140406
[44] Rao, S.M., Jain, A. (2024). Advances in malware analysis and detection in cloud computing environments: A review. International Journal of Safety and Security Engineering, 14(1): 225-230. https://doi.org/10.18280/ijsse.140122