Grenze International Journal of Engineering and Technology, June Issue

A Systematic Comparison of Ransomware Protection through Comprehensive Analysis for Effective Detection

Spandana Shashikumar[1] and S B Rudraswamy[2]
[1]Dell Technologies, Bengaluru, India
Email: Spandana.shashikumar@gmail.com
[2]Dept. of ECE, SJCE, JSSSTU, Mysuru, India
Email: rudra.swamy@sjce.ac.in

***Abstract*— Data is the critical asset in today's world that must be protected. Organizations of all sizes are now at risk due to their reliance on the internet, cloud computing, big data, IoT devices, and remote working. The necessity to safeguard our data and applications from an increasing multitude of impending dangers is paramount, regardless of whether we are operating an on-premises data center or utilizing a public cloud facility. Among various cyberattacks, Ransomware is considered one of the most critical and damaging forms of cyberattacks. Ransomware attacks have become one of the most popular and damaging cyber threats, which requires advanced early detection methods. This study is a complete review of the types of ransomware attacks, their evolution, and the manner of attack alongside the ransomware attack chain, namely, illustrating stages from infiltration to encryption. Early detection, therefore, is critically relied upon to minimize damage and minimize data breaches, and the study highlights there are various detection methods that fall into signature-based, behavior-based and heuristic-based detection. Current methods have been successful in detecting some known and unknown attacks; however, according to the review, there is still room for development in real-time, adaptive attacks detection with scalability in the environment.**

***Keywords*— Ransomware Attacks, Detection, Anomaly, Machine learning.**

I. INTRODUCTION

Attacks using ransomware have become a worldwide cybersecurity risk that affects everyone, including governments, businesses, and individuals [1]. It is malicious software that encrypts victims' data, locking them onto the system and rendering it unsolvable until a ransom is paid, much like Bitcoin. It is crucial to comprehend the factors that must be taken into account when selecting an encryption solution because ransomware has developed from basic hack and infect to complex variations like WannaCry, CryptoLocker, and REvil [2], using sophisticated attack mechanisms to attack vulnerabilities in systems and networks. Billions of dollars are lost annually as a result of these attacks, and critical infrastructure operations compromised. As the threat of ransomware increases, attention to this problem becomes more critical as these systems, which lack sufficient cybersecurity safeguards, are gaining a lot of digital power.

Grenze ID: 01.GIJET.12.2.36_25

The emphasis on early detection as a key to lessening the devastating impacts of these attacks has resulted from the rapid ineffectiveness of traditional defenses against thriving yet inventive cybercriminals.
By identifying kinds, techniques, and advancement along the attack chain, this work aims to comprehend ransomware attacks in their entirety. Examine current detection methods, highlights the need to concentrate on early detection in order to minimize harm, and identifies their shortcomings as a primary goal. However, the study intends to assess the efficacy of cutting-edge techniques, such as behavior-based models and artificial intelligence (AI), in real-time detection. In order to further strengthen strong cybersecurity architectures, the study also seeks to pinpoint the weaknesses in current ransomware defenses and suggest future lines of inquiry and improvement.
The article provides a comprehensive analysis of the many ransomware types, their traits, and their development history. It examines the entire ransomware attack chain, from the first compromise to the execution of the ransom demand. The books examine detection techniques such signature-based, behavior-based, and heuristic approaches, and the features they employ are examined in terms of their benefits and drawbacks as well as their possible applications in various situations.
The study also examines how new technologies like artificial intelligence (AI) and machine learning might be added to the growing field of ransomware detection. It also explores the issues with scalable and real-time detection techniques, offering potential directions for future study. The goal is to give scholars, cybersecurity experts, and legislators a thorough analysis as a foundation for proactive and flexible tactics against ransomware attacks [3].

II. Overview of Ransomware Attacks

A. Historical Evolution of Ransomware

Ransomware has fully matured into a standalone cyber threat, starting with its origins as the AIDS Trojan back in the late 1980s all the way to ransomware we see today. Ransomware attacks evolved to be more complex, but they also increasingly became financially motivated. During the mid-2000s 2000s, crypto-ransomware appeared in which users files were encrypted (Crypto Locker 2013) making them non-readable unless paid for by providing decryption keys[5]. This gave rise to the 2017 WannaCry attack that made headlines for hitting organizations from a global scale by exploiting system vulnerabilities. Double extortion efforts, which involve the theft and encryption of data, are now on the rise. This is due to the fact that cyber criminals continue to send out a completely new version of Ransomware everyday, making themselves a never-ending menace in the cyber world [1]. Figure 1 shows the diagrammatical view of ransomware threats' evolution.

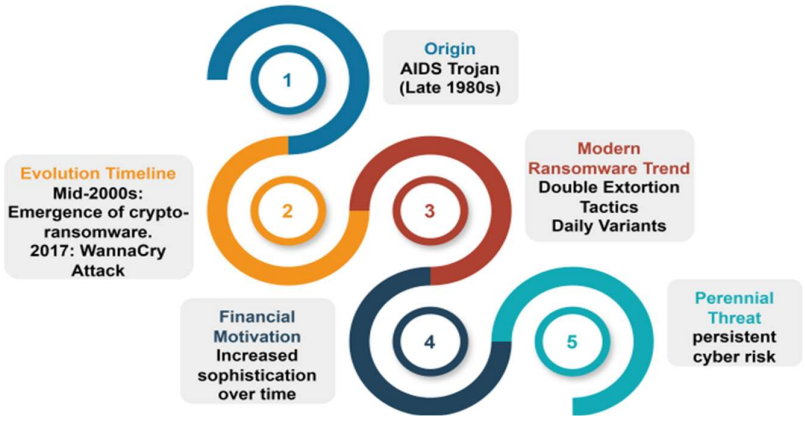

Fig. 1. Evolution of Ransomware

B. Ransomware Characteristics

Ransomware is an example of malware that restricts access to the computer system or its contents until the payment of a ransom fee, which is typically made using cryptocurrencies [4]. Files or the entire user's access to the system becomes encrypted by ransomware. Key features of ransomware involve the ability of the program to spread through emails that may be used for phishing purposes, malicious file downloads, or taking advantage of security holes in the system. Ransomware, when initiated, can involve the delivery of a ransom message demanding payment within a specific time frame, otherwise losing data forever.

C. Types of Ransomware Attacks

There are different methods of ransomware; see Table 1 below that outlines the categorization of attacks by Ransomware. This table shows the different ways of exploitation used by ransomware attackers for each vulnerability with unique ways of execution[6]. There are different effects resulting from each method of ransomware on organizations and individuals.

TABLE I. ATTACK CATEGORIZATION OF RANSOMWARE

Type	Description	Examples
Ransomware-as-a-Service (RaaS)	Enables attackers to "rent" ransomware tools from developers, often for a share of the ransom.	DarkSide, REvil
Crypto Ransomware	Encrypts critical files, rendering them inaccessible until a ransom is paid for the decryption key.	WannaCry, CryptoLocker
Fileless Ransomware	Operates in memory rather than writing files to disk, making detection by traditional antivirus tools challenging.	Sodinokibi
Locker Ransomware	Locks victims out of their devices or systems without encrypting files, displaying a ransom demand screen.	Police Ransomware
Mobile Ransomware	Targets mobile devices, locking access or encrypting files on smartphones or tablets.	Svpeng, Koler
Double Extortion Ransomware	Encrypts files and threatens to leak sensitive data if the ransom is not paid.	Conti, Maze
IoT Ransomware	Exploits Internet of Things (IoT) devices, targeting smart devices to disrupt operations or demand payment.	Mirai Variants

III. RANSOMWARE ATTACK CHAIN

The sequential order of an attack by ransomware from the first theft to the final extortion stage, is known as the ransomware attack chain [7]. It is designed to give a structured understanding of the attack, such as when they breach the system, place their malware, encrypt the data, and demand ransom. Because the attack proceeds through this chain, mapping this chain is critical to identifying vulnerabilities and developing targeted defense mechanisms that can be used to break the attack at different stages. Understanding these stages helps in implementing effective prevention and mitigation strategies

A. Stages of A Ransomware Attack

Fig. 2 demonstrates the attacking phases of ransomware strategies.

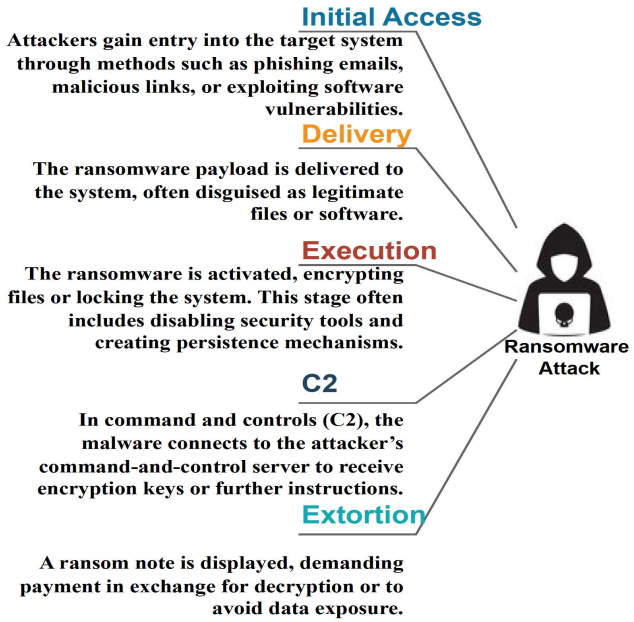

Fig. 2. Ransomware Attacking Phases

B. Common Entry Points and Vulnerabilities

Ransomware attacks have common entry points and vulnerabilities and exploit these weak spots in the system defenses. Ransomware remains a highly prevalent distribution vector and is easy to trigger through phishing emails using deceptive messages that include malicious attachments or links that initiate ransomware downloads. Additionally, there are other big vulnerabilities where attackers will exploit outdated operating systems or applications. Weak or improperly configured RDP settings commonly facilitate attacks which give attackers unwanted access to systems remotely.

Another common way attackers get in is by using stolen or weak passwords, which gives them direct access to important systems and sensitive information. In some cases, they target third-party vendors or suppliers to break into a system. These supply chain attacks make things even harder to detect and prevent, as the weakness comes from outside the main organization [8]. This incident demonstrates how serious ransomware can become in the absence of appropriate security measures and routine monitoring. The likelihood of these attacks is increasing in the absence of robust defense and early detection.

C. Attack Vectors and Propagation Mechanisms

The various kinds of attack vectors and propagation methods available to deploy the ransomware include those that have the capability of going deeper inside the target computer and spreading throughout the system. This includes ransomware attacks that will start with emails and hyperlinks in order to entice users to execute the malware embedded within the email attachment or malware installed on the link provided. The ransomware infection can also be achieved using drive-by downloads where simply visiting certain malicious websites will lead to ransomware installation without users' knowledge. In some cases, exploit kits can also be deployed in order to discover and utilize software vulnerabilities in order to successfully deploy malware infections. Once the ransomware is delivered, fileless techniques will be used in order to execute the ransomware infection on the memory of the computer in order to evade antimalware programs. Upon successful deployment of the ransomware, lateral movement follows in order to spread the infection across networks, leading to greater damage. USB devices can also be used by ransomware perpetrators in order to achieve ransomware infections [9].

IV. Importance of Early Detection

A ransomware attack becomes easier to counter if detected at an early stage. Early detection is key to dealing with ransomware attacks. There are researchers who believe that early detection of a ransomware attack can help in avoiding the encryption of the data as far as possible before suffering substantial data losses. Early detection also makes it easier to isolate the affected computer and nullify the attack. It also helps organizations to continue their business without much hindrance. This can also save organizations from any potential embarrassment that may arise from losing sensitive data. Since the new ransomware attacks have become extremely sophisticated, advanced methods of detection are required [10].

A. Consequences of Delayed Detection

Consequently, there are major problems resulting from late detection of ransomware. It is very hard to unlock encrypted files or systems affected by ransomware without decrypting keys; some ransomware infections may even require very expensive ransoms [11]. When ransomware goes unnoticed for a while, large amounts of data loss will be experienced, as well as huge costs involved and disruptions within businesses. Ransomware can cause significant destruction, such that infrastructure and lives of people may be affected, especially when hospitals and utilities are attacked. It also gives the attackers leverage to employ double extortion techniques whereby they hold sensitive data ransom and threaten to expose it when their demands are not met [12].

B. Role of Early Detection in Damage Mitigation

Early detection and quick response techniques reduce the impact of ransomware attacks. This aids security teams in identifying the attacker's true location, containing compromised systems, and preventing them from communicating with the attacker's command and control servers. Early detection reduces the likelihood that you will have to pay the ransom before the encryption procedure is completed and preserves the integrity of important data.

In addition, early intervention can also contain the attack and stop lateral movement, thereby stopping infection inside the network. Organizations can neutralize threats quickly and at a minimum cost, from both a financial and operational perspective, by proactive monitoring and real-time alerts [13].

V. Literature Review on Detection Methods for Ransomware Attacks

A. Signature-based Detection Methods

The study in [14] used a few file signatures and machine learning models, such as file headers, entropy, and extensions, to classify ransomware-encrypted files from non-encrypted and standard compressed files. Detection based on file extensions was achieved at an accuracy of 97% to 100%. Although effective against strains of ransomware that modify file extensions, their effectiveness is constrained against ransomware strains that do not modify file extensions, and their broader potential for robustness calls for a more comprehensive analysis of ransomware behaviors and file types.

In order to improve ransomware detection, Sangher et al. [15] suggested a hybrid machine learning and deep learning methodology. For the balanced data handling, the study implements a Random Classifier with SMOTE optimization, and to improve the detection accuracy, the study implements Convolutional Neural Networks (CNN) with Adam optimizer for the imbalanced data. The model is trained using 96,724 malware and 41,323 benign files to achieve 99.3% accuracy using Random Classifier with SMOTE and CNN with Adam, with a reduction in false positives and false negatives. While the study is limited in scale to dynamic real-world ransomware samples, relying on a pre-annotated dataset and limited ability to detect obfuscated malware variants, the approach is robust in prediction speed (5.14 ms) and accuracy. The shortcomings in these highlight the need for further adaptation of hybrid detection approaches incorporating runtime information.

Registry Analysis-Based Approach (Zirari et al. [16]) is designed for enhancing the process of detecting the occurrence of ransomware attacks using system registry analysis. By means of the technique-based approach, a brand-name attack with false positives of 14.4% and 62% accuracy will be converted into a ransomware attack having 96.4% accuracy with only 4.5 false positives out of 100. However, it lacks the ability to cope with all ransomware types, which are largely dependent on registry access capability. This may also not cover all ransomware types that rely on file-less or developed evasion techniques. This work shows the need for integration with additional detection methods for full protection against zero-day threats.

AlMajali et al. [17] introduced a ransomware detection methodology based on Similarity Preserving Hashing (SPH). Adaptive partitioning of files using hashing at the partition level is used to improve detection granularity while holding off delays associated with previous methods. For this, the BLAKE3 hashing function was used: a faster, more resource-efficient technique for use in detecting very fast file encryption caused by ransomware. In a simulated attack scenario where 50 files of size ~100 MB are injected into the system for protection, the proposed system can detect attack instances with a time of 0.75 seconds and successfully protects 92% of files in this attack scenario. However, there are two identified limitations: while this approach is robust to varying file volatility, it is susceptible to increased false positives based on the set threshold; as well as difficulties adapting to various operating systems and potential computational overhead for environments with a high file volatility. The two strengths of this study are adaptive parameters for security customization and modular implementation; however, further real-world validation and optimization will be needed for increased effectiveness.

In a study by Bhattacharjee and Dakhane [18] on the first ransomware attack prevention through SHA-256 hash signature analysis and automated backup system, they suggested that a strategy involving a hash signature database that can be used to recognize and isolate ransomware based on 38,157 ransomware sample signatures is utilized together with real-time and encrypted data backups using the automated backup system to prevent damages caused by ransomware attacks. Using the SHA-256 hash method, it is capable of detecting attacks from ransomware with 99.1% accuracy. However, this method does not provide the capability to detect zero-day attacks and even obfuscated ransomware because of its requirement for the presence of ransomware signatures. Future studies are expected to consider hybrid activities along with behavioral approaches to increase ransomware resilience.

B. Behavior-based Detection Methods

An efficient light-weight framework called RanDetector was proposed for detecting ransomware application through static analysis and supervised machine learning algorithm like XGBoost and Random Forest [19]. The approach takes into account factors such as permissions, intents, and libraries of encryption and attains an efficiency rate of 97.62 per cent with very little false positives and negatives for a dataset of 450 Android applications. In light of this form of attack, the detection mechanism through static analysis proves efficient in recognizing ransomware because it can detect various forms of data loss risks but, due to its reliance on static analysis, is unable to recognize ransomware through dynamic obfuscation.

The authors suggested an approach that includes behavior-based ransomware detection using process monitoring and machine learning (Decision Tree, Random Forest, and Neural Network) by Arabo et al. [20]. They monitor

which processes are used as resources (RAM, CPU, and disk I/O), and as API calls, then classify them into either benign or ransomware processes. High detection capabilities of their method are provided for zero-day ransomware with a precision rate between 97-98%. Still, the main drawback is that the method may be affected due to inaccurate labeling of the behaviors' patterns and may take time to process data in real-time mode during large volumes of data processing.

As discussed in [21], the RanPAS research introduces an approach of detecting ransomware behavior based on process and API sequences. To obtain the features of the approach, N-Gram and BAG of Words (BOW) feature extraction approaches are utilized, where the approach for classification of ransomware is based on the XGBoost model. The model of RanPAS is quite effective in terms of differentiating between ransomware and benign programs with an accuracy of 98.77% and 97.83%, respectively, measured with the help of the F1 san core metric. However, some limitations are associated with the method, such as heavy computation required due to feature extraction process and inadaptability to new API behavior.

Based on power consumption and CPU temperature monitoring, entropy analysis of stored data, and a honeypot environment to observe and analyze Ransomware, Madanayaka et al. [22] provided a behavior-based ransomware detection tool. It goes proactive and detects unusual encryption activities and emerging ransomware strains. Experimental evaluations show that the tool can greatly differentiate ransomware from ethics in terms of high accuracy. Nevertheless, it is susceptible to both potential overhead and scalability overhead due to its real-time measurement, and the honeypot requires complete samples. Future work could also include improving performance while being adaptive to zero-day ransomware.

The study in [23] introduced a model for Android ransomware detection using a behavior-based model by combining static analysis with machine learning algorithms such as Decision Tree, Extra Tree Classifier, Random Forest, and Light Gradient Boosting Machine. The model analyzed a dataset of 7,200 samples (3,572 ransomware and 3,628 benign apps) from Kaggle and achieved a detection accuracy of 98.05%. Effective at distinguishing ransomware, the approach is a static analysis-based approach, which may prove difficult to identify dynamic or obfuscated ransomware behaviors. Hybrid models incorporating dynamic features will be explored in future research that offers greater adaptability.

C. Heuristic and Anomaly-based Approaches

In [24], a heuristic approach to ransomware detection and prevention was proposed by which a system protection driver intercepts file I/O operations. The model monitors changes in file metadata against a predefined lookup table, stops malicious activity and restores the former data seamlessly using a caching mechanism. It is efficient in its protection and at the same time, minimizes real-time overhead by intervening only during file open/close events. Despite this, it is limited to predefined metadata patterns and may not be as effective in large-scale systems or in a wide range of file structures.

In [25], AntiBotics, a system that uses application authentication-based file access control to prevent ransomware, was proposed. AntiBotics implements a rule that forces periodic user identification and authorization to read files, preventing modern ransomware from encrypting protected data. When evaluated experimentally, complete protection (100% success) at the expense of low challenge rates for users is demonstrated against tested ransomware. Nevertheless, these come with limitations such as periodic interruptions that might discommode use, as well as reliance on user compliance, which might not scale nicely with user variability or advanced attack strategies.

The ransomware defence system introduced by Gomez-Hernandez et al. [26] uses honey files (FIFO-based trap files) to detect and attack ransomware. With minimal resource consumption, virtually eliminated system disruption, and a 100% detection rate, the honey files block ransomware activity on access and trigger automated countermeasures. However, this approach also has some drawbacks. It requires careful placement of honey files, and advanced ransomware may still find ways to avoid these traps by accessing files in random patterns. Issues like handling large-scale systems and dealing with such evasion techniques need to be improved in future work.

D. Machine Learning and AI-Driven Techniques

Similar to [27], ransomware classification employs a Random Forest Classifier via static analysis of raw bytes features in combination with frequent patterns mining and gain ratio technique for selecting an optimal number of features. This system has been able to demonstrate remarkable results by attaining an extremely high accuracy rate of 97.74 with a very low rate of false positives (0.043) with only 1,000 optimal features. The system does not involve disassembly process while maintaining high efficiency in terms of detection time and cost, which is almost zero. However, it should be noted that dynamic and obfuscation methods employed in new ransomware pose a serious challenge for static analysis.

Another research [28] suggested an innovative approach to ransomware detection based on Markov Models and Random Forest classifiers. First of all, Markov Models are used in order to examine the patterns of API sequences for detecting ransomware by means of the minimal number of false positives. In case a ransomware is not detected at this stage, the other samples are investigated using the Random Forest classifier taking into account the following dynamic features: registry changes, file activity, and string patterns. This approach resulted in 97.28% accuracy with false positive and false negative rates equal to 4.83% and 1.47%, correspondingly. Despite the fact that such results are quite high, this algorithm can be considered as too complex since it needs a huge amount of features along with sandboxing.

In [29], the authors developed the UA-DES technique which is based on the deep learning approach of Uncertainty Aware Dynamic Early Stopping using Deep Belief Networks (DBNs). The accuracy of ransomware detection was raised from 94% to 98%, while the false positive rate decreased from 0.18 to 0.10. This technique allows for a better generalization of the machine learning model and helps avoid the overfitting problem. However, there are certain disadvantages associated with such an approach to detecting ransomware threats. Firstly, the technique involves extensive computational power and a significant reliance on precisely crafted training sets. As a consequence, the method cannot be widely used due to the above drawbacks.

For example, [30] compares two rule-based methods for data mining ransomware activity in Bitcoin transactions: Decision Table and PART (Partial Decision Tree). The authors use ten-fold cross-validation to evaluate model performance using a dataset of 60804 Bitcoin addresses associated with 29 ransomware families. The PART algorithm outperforms the Decision Table, achieving an accuracy of 96.01%, a recall of 96%, and a precision of 95.9%, with a lower error rate of 3.99%. However, it's longer modeling time (26:49 minutes) compared to the Decision Table (1:43 minutes) may pose challenges for time-sensitive applications. Later work should go into hybrid models to scale and speed future work. Table 2 illustrates the summarized version of the review which provides a precise review on each of the studies.

TABLE II. SUMMARIZED VERSION OF THE REVIEW OF RECENT STUDIES

References	Method	Work Focused	Outcome	Remarks
[14]	Feature-Based Detection	Used features like Chi Squared and file entropy to identify ransomware-encrypted files.	Identified significant role of file extensions in detection.	Dependency on certain features (e.g., extensions) limits versatility against stealthier ransomware behaviors.
[15]	Hybrid Signature-Based Detection	Combines machine learning and deep learning to classify benign and ransomware.	Demonstrated high accuracy (99.3%) and robust predictive capability against pre-labeled datasets.	Lacks real-time adaptability and may not generalize to unseen, highly sophisticated ransomware variants employing advanced evasion techniques.
[16]	Registry Analysis-Based Approach	Monitoring system registry changes to identify ransomware-specific activities.	Achieved 96.4% detection accuracy.	Effective for behavior-based detection but limited in handling fileless ransomware or advanced evasion tactics.
[17]	Similarity-Preserving Hashing (SPH)	Adaptive ransomware detection using file partitioning and selective hashing.	Achieved 92% file protection with a detection time of 0.75 seconds for 50 files of size ~100 MB each.	Adaptive parameters for security customization; efficient detection but may encounter increased false positives depending on threshold configuration.
[18]	SHA-256 Hashing	Detect ransomware by comparing file hashes against a pre-established signature database.	Achieved 99.1% accuracy in detecting known ransomware samples from a repository of 38,157 entries.	Efficient for known threats but limited in detecting zero-day ransomware and heavily obfuscated malware.
[19]	RanDetector	Behavior-based ransomware detection using static analysis and supervised ML models.	Achieved 97.62% accuracy with low false positives/negatives.	Effective but limited in handling dynamic obfuscation or novel ransomware variants.
[20]	Behavior-Based Analysis	Detects anomalies in system usage patterns to classify ransomware.	Identified key usage patterns distinguishing ransomware from benign applications.	Potential delays in real-time detection during high system resource utilization.

[21]	RanPAS (Process- and API-Sequence Analysis)	Behavior-based ransomware detection using process and API sequences.	Achieved 98.77% F1 score for detection and 97.83% for multi-classification.	Effective but computationally intensive, with potential difficulties handling unseen API sequences.
[22]	Behavior-Based Detection Tool	Monitoring power usage, CPU temperature, data entropy changes, and honeypot environments.	Achieved high accuracy in detecting ransomware.	Proactive approach effectively detects unknown ransomware but may face scalability issues in real-time monitoring.
[23]	Static Analysis + Machine Learning	Detection of Android ransomware using static behaviors and ML classifiers.	Achieved 98.05% detection accuracy.	Effective for known ransomware but may face challenges with dynamically obfuscated or unknown variants.
[24]	Heuristic Approach via System Driver	Detects and prevents ransomware by intercepting file I/O operations and monitoring metadata changes.	Efficiently identifies and quarantines malicious activity.	Low overhead, however, limited adaptability in case of unpredictable behaviors or files.
[25]	AntiBotics (Authentication-Based File Access Control)	Protects files by enforcing periodic authentication/authorization for access.	Achieved 100% prevention of ransomware encryption.	Efficient against ransomware attacks currently existing, however, can be susceptible to usability issues because of users' involvement.
[26]	Honeyfile-Based Detection	Deploys trap files to block ransomware and trigger countermeasures.	Achieved 100% detection accuracy.	Efficient against ransomware, however, prone to advanced ransomware techniques such as accessing random files.
[27]	Random Forest Classifier	Ransomware detection using byte-level static analysis and feature selection via Gain Ratio.	Achieved 97.74% accuracy with a 0.043 FPR.	Faster and more efficient but has difficulty in dealing with dynamically obfuscated ransomware.
[28]	Markov Model + Random Forest	Two-stage detection: API sequence analysis (stage 1) and ML-based classification (stage 2).	Achieved 97.28% accuracy, 4.83% FPR, 1.47% FNR.	Efficient in managing false negatives, but computationally expensive because of dynamically extracted features..
[29]	UA-DES with DBNs	Optimizes DBN training using uncertainty-aware early stopping and calibration techniques.	Improved accuracy from 94% to 98%; reduced FPR from 0.18 to 0.10.	Efficient in minimizing overfitting, but computationally expensive. Well-curated datasets needed.
[30]	PART (Partial Decision Tree)	Classification of Bitcoin ransomware transactions using decision trees.	Achieved 96.01% accuracy, 3.99% error rate.	More accurate than Decision Table, but takes more computational time.

VI. Challenges in Ransomware Detection

A. Limitations of Existing Detection Methods

Nonetheless, conventional ransomware detection techniques, such as the use of signatures for detecting malicious software, may not be enough when dealing with evolving ransomware. Since these types of detection approaches rely on previously defined signatures to detect malicious software, they will fall short in cases where there are zero-day attacks or where the ransomware uses obfuscation to avoid detection. This might prove to be counterproductive as ransomware mimicking legitimate programs may lead to more false positives[31].

B. Challenges in Real-Time Detection

The rapidity in which files can be encrypted using ransomware is another problem when trying to detect ransomware in real-time.

Real-time detection requires huge amount of data analysis within limited period of time such as API calls, file operations, and even network traffic noise.

It becomes even more difficult to apply efficient solution for detecting ransomware under real-time constraints because of computational constraints within the endpoint devices themselves [32].

C. Adversarial Tactics and Evasion Techniques

The ransomware developers are getting more creative and complex with every passing day by using ever-evolving techniques to bypass detection systems. Static and dynamic analysis methods used to detect ransomware threats are complicated due to the presence of techniques like code obfuscation, encryption of the payload, use of polymorphism, and so forth. In addition, ransomware may delay the execution of its code and use environment-aware triggers to defeat the purpose of sandboxing to evade detection techniques, as such techniques demand highly sophisticated mechanisms for prevention [33].

Therefore, future research will have to focus on designing hybrid, efficient and adaptive detection systems to detect the known as well as unknown ransomware attacks, while at the same time preventing any possible evasion techniques employed by the adversary [34].

VII. Future Research Scope and Opportunities

A. Emerging Technologies in Ransomware Detection

Given that ransomware attacks continue to evolve, emerging technologies are playing a crucial role in improving detection capabilities. Machine learning, blockchain, and real-time threat intelligence are paving the way for more advanced approaches to address this problem. Machine learning can effectively detect anomalies and behavior that could be linked to ransomware attacks, including activities related to accessing files or encrypting them. Blockchain technology can also play a part in detecting any possible supply chain vulnerabilities [35]. Moreover, improvements in real-time advanced anomaly systems mean that attacks are detected before they can inflict damage on the organization.

B. Integration of AI and Adaptive Learning

AI and adaptive learning are leading the way in changing the way ransomware detection will be performed in the future, as they will make the system smarter and better at dealing with emerging threats. The ransomware signature lies in large quantities of data that can be processed with AI-based algorithms to perform analysis of how an attack may take place. The benefit of using adaptive learning processes is that they allow constant evolution according to new attack strategies and exploits of any kind. This process leads to improved accuracy in detection, fewer false positives, and greater success in defeating polymorphic ransomware with its constantly changing code [36].

C. Development of Proactive Detection Frameworks

Remaining one step ahead of the attackers entails proactive detection frameworks. Proactive frameworks in terms of development of frameworks do not wait for the threat to arise and react to it. They are designed to detect and neutralize a threat before the occurrence [37]. Such detection frameworks entail the use of technologies for predictive analytics, threat intelligence, and continuous monitoring in order to detect any vulnerability in the case under consideration. This will help organizations predict anything related to abnormal activity on their network or abnormal file behavior. In addition, they also adopt endpoint detection and response (EDR) tools, which also increase the effectiveness of defending from large-scale attacks.

D. Collaborative and Global Approaches to Ransomware Prevention

The government, various institutions, and cybersecurity professionals must collaborate cohesively to address the global issue of ransomware. Information regarding the threat can be shared across all industries and geographies to help understand any developing trends and common vectors of ransomware attacks, et cetera [38]. Coordinated enforcement measures against ransomware criminal syndicates, joint ventures by both private and public bodies to create disruption within the ransomware operations, and such global initiatives as those must become common practice. In addition to this, the creation of international policies and laws that would govern cybersecurity measures and cybercrime activities makes a lot more sense in such situations because it lowers the burden of compliance for decentralized oversight of cybersecurity [39]. [40].

References

[1] O'Kane, P., Sezer, S. and Carlin, D., 2018. Evolution of ransomware. Iet Networks, 7(5), pp.321-327.

[2] Deochakke, A. and Tyagi, A.K., 2022, May. Analysis of Ransomware Security on Cloud Storage Systems. In International Conference on Advancements in Interdisciplinary Research, Cham: Springer Nature Switzerland, pp. 47-59.

[3] Yaqoob, I., Ahmed, E., ur Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M., 2017. The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, pp.444-458.
[4] Oz, H., Aris, A., Levi, A. and Uluagac, A.S., 2022. A survey on ransomware: Evolution, taxonomy, and defense solutions. ACM Computing Surveys (CSUR), 54(11s), pp.1-37.
[5] Gómez Hernández, J.A., García Teodoro, P., Magán Carrión, R. and Rodríguez Gómez, R., 2023. Crypto-ransomware: A revision of the state of the art, advances and challenges. Electronics, 12(21), pp.4494.
[6] Kok, S., Abdullah, A., Jhanjhi, N. and Supramaniam, M., 2019. Ransomware, threat and detection techniques: A review. Int. J. Comput. Sci. Netw. Secur, 19(2), pp.136.
[7] Reshmi, T.R., 2021. Information security breaches due to ransomware attacks-a systematic literature review. International Journal of Information Management Data Insights, 1(2), pp.100013.
[8] Beaman, C., Barkworth, A., Akande, T.D., Hakak, S. and Khan, M.K., 2021. Ransomware: Recent advances, analysis, challenges and future research directions. Computers & security, 111, pp.102490.
[9] Kumar, E.P. and Priyanka, S., 2023. A comprehensive survey on hardware-assisted malware analysis and primitive techniques. Computer Networks, 235, pp.109967.
[10] Al-Rimy, B.A.S., Maarof, M.A. and Shaid, S.Z.M., 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, pp.144-166.
[11] Albshaier, L., Almarri, S. and Rahman, M.H., 2024. Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review. Information, 15(8), pp.484.
[12] McIntosh, T., Kayes, A.S.M., Chen, Y.P.P., Ng, A. and Watters, P., 2021. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. ACM Computing Surveys (CSUR), 54(9), pp.1-36.
[13] Gazzan, M. and Sheldon, F.T., 2023. Opportunities for early detection and prediction of ransomware attacks against industrial control systems. Future Internet, 15(4), pp.144.
[14] Duignan, M., Schukat, M. and Barrett, E., 2023, June. Detecting Ransomware Encryption with File Signatures and Machine Learning Models. In 2023 34th Irish Signals and Systems Conference (ISSC), IEEE, pp. 1-5.
[15] Sangher, K.S., Singh, A. and Pandey, H.M., 2024. Signature based ransomware detection based on optimizations approaches using RandomClassifier and CNN algorithms. International Journal of System Assurance Engineering and Management, 15(5), pp.1687-1703.
[16] Zirari, K., Idrissi, H.K., El-Yahyaoui, A., Bensaid, H. and En-Nouaary, A., 2023, August. Enhancing Ransomware Detection: A Registry Analysis-Based Approach. In 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, pp. 65-70.
[17] AlMajali, A., Elmosalamy, A., Safwat, O. and Abouelela, H., 2024. Adaptive Ransomware Detection Using Similarity-Preserving Hashing. Applied Sciences, 14(20), pp.9548.
[18] Bhattacharjee, S., and Dakhane, D. (2024) "A Signature-based Ransomware Detection and Automated Data Backup to Safeguard the System from Ransomware Attack ", International Journal of Intelligent Systems and Applications in Engineering, 12(18s), pp. 714–721.
[19] Alzahrani, A., Alshahrani, H., Alshehri, A. and Fu, H., 2019, December. An intelligent behavior-based ransomware detection system for android platform. In 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), IEEE, pp. 28-35.
[20] Arabo, A., Dijoux, R., Poulain, T. and Chevalier, G., 2020. Detecting ransomware using process behavior analysis. Procedia Computer Science, 168, pp.289-296.
[21] Wang, B., Liu, H., Han, X. and Xuan, D., 2021, October. RanPAS: A Behavior-based System for Ransomware Detection. In 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC), IEEE, pp. 309-314.
[22] Madanayaka, B.W., Dias, N.A., Samaranayake, A.K.D.D.V., Karawita, K.V.D.A.U., Abewardhana, K.Y. and Siriwardana, D., 2023, December. A proactive approach for behavior based ransomware detection. In 2023 5th International Conference on Advancements in Computing (ICAC), IEEE, pp. 346-351.
[23] Kirubavathi, G. and Anne, W.R., 2024. Behavioral based detection of android ransomware using machine learning techniques. International Journal of System Assurance Engineering and Management, 15(9), pp. 4404-4425.
[24] Alexandrov, B., Gotsev, L., Petkova, M.V. and Petkova, V.V., 2023, July. Heuristic approach to ransomware detection and prevention at software or hardware level. In 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), IEEE, pp. 1-6
[25] Ami, O., Elovici, Y. and Hendler, D., 2018, April. Ransomware prevention using application authentication-based file access control. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1610-1619.
[26] Gómez-Hernández, J.A. and García-Teodoro, P., 2024. Lightweight Crypto-Ransomware Detection in Android Based on Reactive Honeyfile Monitoring. Sensors, 24(9), pp.2679.
[27] Khammas, B.M., 2020. Ransomware detection using random forest technique. ICT Express, 6(4), pp.325-331.
[28] Hwang, J., Kim, J., Lee, S. and Kim, K., 2020. Two-stage ransomware detection using dynamic analysis and machine learning techniques. Wireless Personal Communications, 112(4), pp.2597-2609.
[29] Gazzan, M. and Sheldon, F.T., 2024. Novel Ransomware Detection Exploiting Uncertainty and Calibration Quality Measures Using Deep Learning. Information, 15(5), pp.262.
[30] Talabani, H.S. and Abdulhadi, H.M.T., 2022. Bitcoin ransomware detection employing rule-based algorithms. Science Journal of University of Zakho, 10(1), pp.5-10.

[31] Ispahany, J., Islam, M.R., Islam, M.Z. and Khan, M.A., 2024. Ransomware detection using machine learning: A review, research limitations and future directions. IEEE Access, 12, pp. 68785–68813.
[32] Popoola, S.I., Iyekekpolo, U.B., Ojewande, S.O., Sweetwilliams, F.O., John, S.N. and Atayero, A.A., 2017, October. Ransomware: Current trend, challenges, and research directions. In Proceedings of the World Congress on Engineering and Computer Science, 1, pp. 169-174.
[33] Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G. and Davidson, I.E., 2021. Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), pp.8.
[34] Olaimat, M.N., Maarof, M.A. and Al-rimy, B.A.S., 2021, January. Ransomware anti-analysis and evasion techniques: A survey and research directions. In 2021 3rd international cyber resilience conference (CRC), pp. 1-6.
[35] Urooj, U., Al-rimy, B.A.S., Zainal, A., Ghaleb, F.A. and Rassam, M.A., 2021. Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. Applied Sciences, 12(1), pp.172.
[36] Fernando, D.W., Komninos, N. and Chen, T., 2020. A study on the evolution of ransomware detection using machine learning and deep learning techniques. IoT, 1(2), pp.551-604.
[37] Maigida, A.M., Abdulhamid, S.I.M., Olalere, M., Alhassan, J.K., Chiroma, H. and Dada, E.G., 2019. Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. Journal of Reliable Intelligent Environments, 5, pp.67-89.
[38] Raghunath, K.K., Kumar, V.V., Venkatesan, M., Singh, K.K., Mahesh, T.R. and Singh, A., 2022. XGBoost regression classifier (XRC) model for cyber attack detection and classification using inception V4. Journal of Web Engineering, 21(4), pp.1295-1322.
[39] Adeyeri, A. and Abroshan, H., 2024. Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. Information, 15(11), pp.682.
[40] Raghunath, K.K. and Rengarajan, N., 2013. Investigation of faults, errors and failures in wireless sensor network: A systematical survey. International Journal of Advanced Computer Research, 3(3), pp.151.