International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 11, Issue 1, 2025, PP 18-28
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: https://doi.org/10.20431/2349-4859.1101003
www.arcjournals.org

Comparative Analysis of Ransomware Detection Techniques: Strengths and Vulnerabilities

Salah Abu Baker*

Head of Network and Cyber Security Department, irbid electricity company (ideco),Irbid, Jordan.

***Corresponding Author**: ***Salah Abu Baker,** Head of Network and Cyber Security Department, irbid electricity company (ideco),Irbid, Jordan.*

Abstract: *Ransomware, a rapidly evolving digital menace, has increasingly posed significant challenges to individual users, enterprises, and even national infrastructure. The critical nature of its impact necessitates the development and refinement of specialized detection techniques. This paper delves into the intricacies of ransomware detection, evaluating a range of methodologies from traditional signature-based approaches to modern machine learning-driven strategies. The study sheds light on the strengths and weaknesses of each technique, highlighting the dynamic landscape in which ransomware operates. As these threats grow in sophistication, the research emphasizes the urgency to adopt multi-faceted, integrative detection approaches. Incorporating insights from real-world case studies, the paper provides actionable recommendations for stakeholders to bolster their defense mechanisms.*

1. INTRODUCTION

Recently, cyberspace researchers have been closely monitoring ransomware known as the cryptovirus. These malware programs are used by hackers to steal people's confidential information by taking advantage of flaws, such as those from earlier malware assaults. In addition, it would threaten the victim with the loss of important files, data, or sensitive information if they refuse to comply with their demands. E-gold, cryptocurrencies, or demands to purchase from retailers could be used as ransom or demand. The PC CYBORG (AIDS) Trojan was the first ransomware attack, and it appeared in 1989. Modern ransomware assaults began in 2005 with "Trojan. Gpcoder," which was distributed electronically via a floppy disk, which was then used to attack a machine (Chittooparambil et al.,2019)

According to a new poll of senior executives, 46% of small firms have experienced ransomware attacks in the past few months. Since 2018, business ransomware detections have climbed (Malwarebytes, 2019). Additionally, 73% of firms that have experienced a ransomware assault have paid the demanded ransom, with 43% paying between $10,000 and $50,000 and 13% paying more than $100,000 to the hackers. However, only 17% of those who paid retrieved all the company's data, even though organizations are increasingly turning to cloud computing to automate a variety of business processes (MarketsInsider, 2020).

Industry surveys estimate that 68% of firms currently employ cloud technology, and another 19% want to do so soon (Customer think, 2020) The number of assaults against cloud services more than doubled in 2019, according to the 2020 Trustwave Global Security Report, echoing the trend of businesses progressively moving operations to the cloud. Ransomware defense in the cloud and virtualized systems is essential as cloud computing adoption increases in businesses (Trustwave, 2020).)

In contrast to other viruses, ransomware typically uses two methods of operation. Screen locks are the first, deliberately locking the screen of an infected computer. Crypto ransomware, on the other hand, progressively encrypts the victim's files using cryptographic techniques. The victims will then be prompted to pay a ransom to unlock their computers or decrypt their contents. By having victims reinstall their operating systems, screen locks can be avoided (OSes). Crypto ransomware is dangerous to users because attackers use powerful encryption algorithms and long-enough keys, making it practically difficult for victims to retrieve their encrypted files without a key (Tang et al., 2020). This study explores innovative methodologies for ransomware analysis and identification architecture. In addition, it can identify ransomware assaults and confirm their veracity and accuracy through a verification process comprising malware testing.

This paper was structured in four sections.

1. At first is presented the introduction.
2. Secondly, it is presented the materials and methods.
3. In the section three is detailed and discussed the systematic review performed.
4. Finally, in the section four is discussed some relevant points and addressed future works.

2. RELATED WORK

A significant and developing research field is ransomware and numerous studies are carried out to help researchers and developers understand what is taking place in the field. Next some of the studies that discussed methods to defeat ransomware will be highlighted in the discussion.

Tariq et al. (2022) established ransomware evaluation and identified a ransomware detection architecture. Furthermore, it validates their accuracy and validity through a time-consuming validation process. On their various samples (with an average and standard deviation of 21 and 18 tests, respectively), they evaluated ten different malwares, including GP code and Filecoder (with an average and standard deviation of five and two malware variants, respectively). As a result, 194 distinct malware samples and 46 variants were used to evaluate the architecture for ransomware analysis and identification. The studies looked at many ransomware attacks, including "Encrypting Files," "Deleting Files," and "Stealing Files," for each of the viruses that were chosen. Researchers examined network traffic data encrypted with the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols in a Cuckoo Sandbox to seek malicious network peer activity. A total of sixty minutes were spent running each of the experiment's 194 tests, and the network traffic data were carefully reviewed for signs of malicious activity.

Urooj et al. (2022) inspected dynamic ransomware detection on various platforms23 datasets from the Windows platform, 2 from Android, 4 from the cloud and IoT (Internet of Things), and 2 from networks were also included in the study. It also employed hybrid, machine learning, and deep learning malware detection methods. Overall, ransomware activity is investigated via dynamic analysis, which executes malicious code in a controlled environment. This study demonstrates the dearth of pre-encryption detection studies. The study's primary focus was on the following outstanding issues in ransomware detection studies. Based on memory-assisted stochastic dynamic fixed-point arithmetic, they suggested a rapid technique of ransomware detection.

A four-layer Deep Belief Network (DBN) structure was used to consider real-time detection, time complexity, low-spec hardware implementation, evasion, and obfuscation-tolerant systems. This technique creates an effective cross-correlation for the stochastic computation in the FPGA by storing random bit-streams in memory.

Alrawashdeh et al. (2019) reported a quick method for ransomware detection using a memory assisted stochastic dynamic fixed-point arithmetic and a four-layer Deep Belief Network (DBN) structure. This technique develops an efficient cross-correlation for stochastic computing in the FPGA by storing random bit-streams in memory. Dynamic fixed-point arithmetic and stochastic computation are coupled to train the Deep Belief Network (DBN) memory method. According to the study, the precision rate is 91% and the detection speed is 0.006 ms. This approach makes it easier for the Internet of Things to identify malware (IoTs).

To detect ransomware and its families using deep learning techniques like Long Short-Term Memory (LSTM) and Convolution Neural Networks (CNN), Homayoun et al. (2021) presented the "Deep Ransomware Threat Hunting and Intelligence system (DRTHIS)" for classification using the SoftMax algorithm. The training dataset contains 219 benign samples, 220 Locky, 220 Cerber, and 220 TeslaCrypt ransomware samples. The test's F-measure is 99.6%, and its positive rate is 97.2%. Even previously untrained forms of the Crypto Wall, Torrent Locker, and Sage ransomware families have been used to test this concept. For Crypto Wall, Torrent Locker, and Sage, the detection rate of new ransomware is 99%, 75%, and 92%, respectively. The sensitive data contained in the nodes of the fog layer was the focus of this study.

An intelligent and automatic approach for ransomware detection, categorization, and mitigation in integrated clinical environments (ICE++) was proposed by Fernandez et al. in 2019. By combining mobile edge computing (MEC), software-defined networking (SDN), and network function virtualization (NFV), ICE++ reduces the risk of ransomware attacks in ICE and offers adaptable,

affordable, and self-regulating security system administration. The system's architecture is made up of four modules: the monitoring module collects network traffic from medical devices and creates feature vectors; the offline model generation module selects a classification algorithm to train a model from the feature vectors generated training dataset; and the analyzer module accepts qualified ML models and categorizes traffic as ransomware or not right away. The decision and reaction module also evaluates the prospect of a successful ransomware assault. One Class SVM (Support Vector Machines) is used in this system to detect anomalies, and Naive Bayes is used to determine the likelihood that the new models will belong to the class with the most similar traffic pattern. While Naive Bayes attained 99.99% classification precision, the suggested model performed well in the anomaly recognition task, attaining 92.32% accuracy and 99.97% precision.

Baek et al. (2021) suggested a two-step hybrid malware detection system to safeguard IoT nodes in a smart city setting against covert malware (2-MaD). There were two distinct parts to the 2-MaD program. The first uses static analysis to find dangerous software, while the second uses a dynamic scan to find malware. A performance indicator was the false negative rate's (FNR) accuracy. When 2-MaD's performance was assessed, the malware discovery precision exceeded that of static analysis detection at 94.46%. The suggested plan has a flaw in that it undervalues the significance of related application interface calls, instruction trace logs, and registry modifications.

In order to identify a collection of ransomware features, Damien et al. (2022) proposed a feature section design, which increased the used machine learning classifier's endurance (FeSA). The recall, false negatives, and accuracy of the functional technique were compared to those of other systems, including evolutionary search, harmony search, and so on. The suggested mechanism failed to show how the boot record of the victim node affected the exploitation. The gateway, a key location for efficient anomaly detection and response, did not undergo a thorough analysis of the ransomware identification and prevention paradigm.

The major objective of Zahoora et al (2022) was to provide new Some researchers suggested the Deep Contractive Autoencoder-based Attribute Learning (DCAE-ZSL) method because it successfully examined code insertion that may analyze the semantic representation of zero-day assaults in an unsupported manner. The effectiveness of the strategy was tested using 942 conventional software tests and 582 ransomware tests based on Microsoft Windows OS-compatible widgets, mobile gaming APKs, and office productivity apps. The number of false positive and false negative findings was significantly reduced as compared to shallow baseline prototypes using Scheme. Only working with executable files, DCAE-ZSL does not provide promising solutions for a variety of ransomware oddities.

An open data collection with ransomware storage consumption habits based on hypervisors was presented by Hirano et al. in 2022. The validity of the dataset was assessed using feature engineering and confusion matrices to produce five-dimensional data vectors. The primary drawback of the study is the uselessness of the dataset because it was created with an outdated operating system (Windows 7) in mind. The dataset includes example benchmarks segmentation configurations for ransomware choices that accommodate for different OS (Operating System) versions and encryption techniques.

ICS-ARC, a cutting-edge ransomware attack mechanism that can produce network packets customized to certain control logic, was introduced by Zhang et al. in 2022. In four steps, ICS-ARC carried out a cyberattack using ransomware. To test the systems' capacity to exploit ICS-ARC vulnerabilities, they developed an Arduino with Open PLC already installed on it and another tap water treatment system. The outcomes of the presented operational anomaly reveal how ICS-ARC both lowers the cost of the assault and dramatically increases fault tolerance. Some PLC software claims control logic can repeatedly receive, process, and send control signals.

3. SYSTEMATIC REVIEW

The life cycle of ransomware, which is a type of malicious software (malware) that encrypts and locks down the victim's data or machine until a monetary ransom is paid, includes several stages, starting with distribution, in which the ransomware enters the victim's device through an email attachment, a download, or a code dropper; the infection stage, in which the ransomware sets up shop to withstand reboots and disable backup or antivirus processes; and the communication stage. During the preparation stage, ransomware scans user files—typically PDF, Docx, and jpg files—before encrypting them. Once the targeted user files are encrypted, the ransomware starts its extortion campaign by displaying a "ransom note" that demands payment. The user will receive instructions for obtaining the decryption key after paying the ransom (Chen et al., 2019)

Fig1. *Ransomware lifecycle*

According to attacks, ransomware is divided into two types, locky Ransomware, and crypto ransomware.

3.1 Locky Ransomware

By locking the victim's computer and preventing them from logging in, this kind of attack can be remedied by rebooting or starting in safe mode. (Kok et, 2019) ensures that its victims' data is not altered, simply locking their devices and documents with restricted capabilities, such as enabling user interaction with ransomware and payment of the ransom, and that the user must pay a charge to regain access to the data. Additionally, it makes your computer's operating system, programs, and basic operations less efficient. According to Imaji (2019), this kind is the least dangerous and easiest to remove is ransomware (Kok et al., 2019).

3.2 Crypto Ransomware

By encrypting particular file types that are presumed to be valuable to the victim, such as papers, spreadsheets, photos, and databases, this sort of assault paralyzes victims who are thus helpless in the absence of the decryption key. It can make use of symmetrical, asymmetrical, or hybrid encryption. Based on the step(s) needed, the encryption process canbe divided into three categories: Class C files are encrypted, renamed, and relocated, making it more challenging to discover and recover the file than class A, class B, or class C files that are encrypted but not renamed or relocated (Tariq et al., 2022).

3.3 Methodolgy

In the rapidly evolving landscape of cybersecurity, the threat of ransomware has become a persistent and sophisticated challenge. Detecting and mitigating ransomware attacks require a comprehensive understanding of the strengths, weaknesses, opportunities, and threats associated with various detection techniques. This research employs the SWOT analysis methodology to systematically assess the landscape of general ransomware detection techniques, aiming to enhance our understanding and inform strategic decision-making in the field.

4. General Ransomware Detection Techniques

4.1 Signature-Based Approach

The signature approach focuses on finding distinctive characteristics in ransomware, such as a particular arrangement of bytes in the source code, the calling order of functions, and the content of the ransom demand message. To discover these patterns in sequences that have been stored in a database, anti-malware software searches executable files. Techniques for detecting malware that employs signatures have previously been significantly appreciated since they have a low false positive ratio. such that if a particular pattern is discovered, an alarm can be set off. However, they are unable to handle malware that contains obfuscated code, and they are unable to identify new strains before an analyst has analyzed them (Alshaikh et al,2020) (Chew&Kumar,2019). Signature-based ransomware detection computes the hash of a sample of ransomware code and compares it to known file signatures. A signature is a one-

of-a-kind hash calculated from the content of a given file. It is helpful for strain detection and enables quick static analysis of files in the environment. A common threat is ransomware. Security teams can retrieve the file hash value and compare it to known malware samples using openly accessible tools like the Windows PowerShell Get -FileHash command. This technology is used by traditional antivirus programs to capture data from executables and determine the likelihood that a specific executable file contains ransomware. Beaman and others (2012)

4.2 Behavior-Based Approach

Behavior-based Approach looks at and evaluates the characteristics of the malware's operations based on the analysis of ransomware activities such as file access, file system activity, and network activity. There are some techniques for modeling ransomware behavior by utilizing execution traces discovered by dynamic analysis; For example, monitoring file system activity, network traffic, and Application Programming Interface (API) calls (Alshaikh et al., 2020). The most popular method for modeling behavior uses a process's system-call history (Goodware or malware). The execution patterns of malware and goodware can be compared and contrasted using system call patterns. Machine learning methods that leverage system calls as features have scalability problems due to the large dimensionality. Compared to methods based on syntax, methods based on behavior are more resistant to evasion strategies (Abbasi et al.,2022).

The execution patterns of malware and goodware can be compared and contrasted using system call patterns. Machine learning methods that leverage system calls as features have scalability problems due to the large dimensionality. Compared to methods based on syntax, methods based on behavior are more resistant to evasion strategies. (Abbasi et al.,2022)

Academic scholars and qualified security experts have presented ransomware detecting techniques. Many of them are still in use today. Static or dynamic examination of the executable that might contain ransomware was beneficial for most methods.

Without running the executable, static analysis of an executable is carried out by looking at the code. A binary's static analysis includes memory relocation, packer identification, static linking, and identifying American Source Code Information Interchange (ASCII) strings. Static file analysis is a method of malware detection where the code of an executable file is inspected without running it after the execution of the suspected ransomware.

Static file analysis in the context of ransomware searches for known dangerous code sequences or suspicious phrases, such as frequently targeted file extensions and words used in PeStudio ransom messages. This free tool looks for suspicious artifacts in executable files by scanning strings, libraries, imports, and other embedded indications of compromise (IOCs) (Yamany et al.,2022) One of its advantages is that it is reliable, has a low rate of false positives, and effectively combats well-known ransomware.

Dynamic analysis is performed. During execution, the suspected file's actions and system calls are recorded, and a final report is generated based on this information (Kapoor et al., 2022)

By keeping an eye out for mass file operations like renaming, writing, or deleting within a specific time range on the file system, the ransomware assault can be recognized in real-time and promptly stopped. The File Integrity Monitor (FIM) program helps identify ransomware in this way. When files are modified, updated, or compromised, FIM scans and validates them by comparing their most current version to a recognized, trusted "baseline," and it notifies you of these events (Abbasi et al.,2022).

Free open-source FIM programs are available such as OSSEC and Samhain File Integrity. On the other hand, other solutions feature real-time processing capabilities, which allow you to immediately prevent suspected ransomware by automatically responding to threats. One of its features is detecting ransomware that firmware engines do not. Regarding the disadvantages, files will be encrypted until the given limit is reached including a delay between encoding operations or generating numerous encoding processes to be easily avoided (Pont et al.,2020).

Ransomware detection methods are now more successful against ransomware attacks. Modern detection techniques are hybrid and rely on AI-based methodologies to boost detection effectiveness. Because current detection techniques are not designed to catch all Ransomware strands at once, the most recent

Ransomware families continue to evade them despite advancements. Solutions for detection are often developed to detect a specific strand or type of ransomware because it is challenging to design generic solutions. Furthermore, detection methods were created to detect a single Ransomware variant. Overall, it is clear that the current level of detection approaches is reactive (Kapoor et al., 2022)

4.3 Machine Learning

In machine learning (ML), pattern learning data is utilized to construct a form. This model can anticipate the outcome when fed new data. The issue of ML is finding the proper algorithm to match the desired data type and output. Moreover, the benefit of ML is that it can accurately predict the conclusion. Concisely, the training data should be changed to provide a balanced distribution of expected results. Because machine learning involves learning a pattern in data, it is less vulnerable to obfuscation. In terms of drawbacks, finding the correct algorithm indirectly is tough. It may require some trial and error. Furthermore, if proper precautions are not used, bias and overfitting may develop (Kok et al.,2019).

Machine learning has the unique capability of detecting any modifications to the way files behave, effectively triggering an alert when a variance occurs, this significantly improves the cyber security team's effectiveness because there are fewer alerts, but only significant detection techniques with insight into all file-related process executions and network requests. Machine learning systems can establish baselines and detect deviations from those baselines by thoroughly examining legitimate code executions. Machine learning is the best type of defense against complex ransomware attacks because it alerts cybersecurity teams to any anomalies caused by the attack. This includes unusual file behavior, which is common in ransomware attacks (Yamany et al.,2022).

With the evolution of ransomware as it performs data mining along with file encryption, it is becoming increasingly clear that without machine learning algorithms, organizations will not be effective in stopping ransomware attacks. However, it has become difficult to perform effective security analysis without the aid of machine learning solutions as signature-based detection is excluded from the category of effective incident response as ransomware strains change and new variants are rapidly introduced. As a result, machine learning will be a valuable tool in the arsenal of many organizations attempting to safeguard themselves from the security vulnerabilities of sensitive data mining and file-encrypting malware. Machine learning reduces the number of false positives and provides the granular insight required to detect and prevent ransomware by learning habitual behavior and establishing baselines (Yamany et al.,2022).

Anomalies in file behavior, such as unusual network traffic, process execution, or other actions, will be detected by properly deployed machine learning solutions. Machine learning models detect ransomware by classifying computer programs based on their behavior as benign or ransomware. With enough training data, these models can detect high-level attacks with high accuracy because ransomware is detected before any files are encrypted. Machine learning models are the most common methods for detecting ransomware. These models are adaptive. Discover the most common ransomware behavior patterns. Due to suspicious behavior or specific core processor instruction patterns. Machine learning's ability to detect general ransomware behavior is also important. Ransomware is constantly evolving and has a simple Code Signature, but it is difficult to change its attack pattern. Many of these models, however, necessitate an attack is already underway to locate the suspect Activity, such as file access or contact with a malicious program specialization. (Beaman et al.,2021)

This system offers benefits. Machine learning can accurately anticipate the outcome given adequate training data. In terms of expected outcome distribution, training data needs to be evenly distributed. Because ML needs learning the pattern in the data, it is less likely to be obscured. Finding the best algorithm may need a few iterations of trial and error, which is not always easy. Insufficient caution may result in biases and overfitting (Koeneman & Cavanaugh,2022).

Because machine learning is the most effective and mathematically sound way of data processing and decision-making, one of its fundamental flaws is that it does not comprehend the consequences of the model it is constructing. The program receives millions of data points, but no one is aware of which ones are used. According to the machine learning model, indicators of malware that it discovers on its own may point to a threat. It could consist of one data point or a group of 20 data points. An overzealous attacker may discover and exploit how the model uses these parameters to identify the threat. Changing an insignificant piece of data as a result, no human can truly predict which data points, according to the

machine learning model, may indicate a threat. It could be a single data point or a set of 20 data points. An overzealous attacker might figure out how the model utilizes these parameters to identify the threat and take advantage of it. A single modest adjustment to a risky file could cause the model to mistakenly classify the virus as safe. To solve the problem, combine the processed file with the data set and compute the whole model, which could take days or weeks. Sadly, this does not address the root of the issue; even if the model is rebuilt, it will not be long before a hacker discovers another data point or set of data points that may be used to deceive the machine learning system. (Koeneman & Cavanaugh,2022).

4.4 Honeypot

An alarm is set off when a honey file is opened, a fake file inserted into a shared folder or other area to detect an attacker's presence. A honey file on a workstation can be a file with the name passwords.txt.

Canarytokens are a popular way to create honeyfiles quickly and easily. Canarytokens is a free Canary method for embedding a token (unique identifier) in a document such as Microsoft Word, Microsoft Excel, Adobe Acrobat, images, directory folders, and other formats. Canary sent an email notification to the address associated with the token when it was accessed. You can rename the Canary files to words like "statement," "policy," or "insurance," which ransomware actors look for when searching for files on the victim network. Producing decoy files for Ransomware attacks is part of the honeypot. Once these files are accessed, the Ransomware can be identified, traps or honeypot files can be established, and the process can be completed. Just wait until you are attacked (Yamany et al.,2022).

Honeypots may recognize the user based on the number of changed files, which can be used to direct actions. A honeypot's core concept is to acquire information about an assault and utilize it to fight against it. User training must be supplemented with email reminders that urge users to disconnect their network cables. As a result, utilizing honeypots to detect ransomware is advantageous. Benefits of Honeypots: Because of the qualities of this technique, it does not necessitate a lot of system maintenance or processing resources. It can also detect ransomware that static engines cannot (Gómez-Hernández et al., 2018).

But its disadvantages are Some false positives may occur as programs and users interact with the bait files. Until ransomware touches the decoy files, files will be encrypted. Bypass by ignoring hidden files/folders or by focusing on specific folders. However, there is no guarantee that the attraction files will not be attacked by ransomware. As a result, it is critical to understand the elements of the files that the ransomware will attack. (Gómez-Hernández et al.,2018)

4.5 Statistic

Statistics can be used to analyze ransomware and gain a better understanding of its key characteristics. However, using this technique as a detection mechanism is difficult. (Kok et al.,2019)

Simple statistical techniques are popular and intuitive tactics for detecting ransomware; statistical tests may be used to discover unpredictability, which can signal the presence of encryption and, by extension, a ransomware attack. It investigates the already prevalent usage of statistical techniques for ransomware detection, primarily focused on false positive rates. The aim of the study is to show that the current over-reliance on simple statistical tests within anti-ransomware programs can cause major problems with the consistency and reliability of ransomware detection in the field. Shannon entropy, chi-square, arithmetic mean, Monte Carlo estimation for Pi, and serial correlation coefficient were five of the major statistics used to determine randomness. In order to signal the presence of encryption, which is a frequent means of detecting ransomware, statistical analyses can identify unpredictability. (Pont et al.,2020).

With an emphasis on false positive rates, the researchers investigated the widespread application of statistical techniques now employed to identify ransomware. Their main objective was to show how anti-ransomware algorithms' existing over-reliance on simple statistical tests may jeopardize the consistency and accuracy of ransomware detection by frequently classifying samples wrongly (Yamany et al.,2022).

This mechanism has several advantages: since the encryption process generates random data, it makes sense to investigate the use of randomness tests to identify encryption. The ease with which these randomization checks can be implemented may also be advantageous. Finally, because anti-ransomware solutions rely too heavily on simple statistical tests, which frequently lead to incorrect classifications, there may be significant issues with the consistency and reliability of ransomware.

The consistency and reliability of ransomware detection may be seriously compromised because anti-ransomware solutions rely too heavily on simple statistical tests, which frequently lead to incorrect classifications. As a result, relying solely on these fundamental statistical methods to identify (Pont et al.,2020).

Table1. *Comparison Table of all above Ransomware Detection Technique*

S.NO	Technique	Effectiveness	Error Rate
1	**Signature-based Approach**	High for known ransomware variants. As soon as a new ransomware signature is added to the database, detection of that variant is typically fully accurate	Low false positives for known variants. However, it misses novel or modified ransomware, leading to false negatives.
2	**Behavior-based Approach**	High for detecting anomalous behaviors, including novel ransomware strains.	Potential for higher false positives since legitimate software can behave like malware. The accuracy can be improved with fine-tuning, but there is always a trade-off between sensitivity and specificity.
3	**Machine Learning**	Varies based on the quality and breadth of training data. With adequate training on diverse malware samples, it can be highly effective against both known and unknown ransomware strains.	Initially, there might be false positives and negatives. However, as the model is trained and refined, the error rate can decrease. There is also the challenge of adversarial attacks that aim to deceive the model.
4	**Honeypot**	High for capturing ransomware samples in a controlled environment, especially if attackers do not recognize it as a honeypot	Low false positives since it is about capturing and analyzing. However, by the time ransomware is detected, real systems might already be compromised.
5	**Statistics**	moderate to high, depending on the quality of the baseline data and the specific statistical methods employed.	Does not contribute directly to the error rate as it is not a primary detection method. Understanding ransomware features, however, can help refine other techniques and reduce their respective error rates.

SWOT analysis for Ransomware Detection Techniques

Table2. *SWOT analysis for Signature-based Approach* ***Technique***

Strengths	**Weaknesses**
• High effectiveness for known ransomware variants. • Low false positives for identified variants. • Quick detection once a new signature is added.	• Inability to detect novel or modified ransomware. • Dependency on regularly updated signature databases.
Opportunities	**Threats**
• Integration with other techniques to enhance overall detection capabilities. • Continuous improvement through rapid data base updates.	• Increasing prevalence of polymorphic and • Reliance on signature databases makes it susceptible to evasion tactics.

Table3. *SWOT analysis for Behavior-****based Approach Technique***

Strengths	**Weaknesses**
• High effectiveness in detecting anomalous behaviors. • Capability to identify novel ransomware strains.	• Potential for higher false positives due to legitimate software behaving similarly. • Requires fine-tuning, leading to a trade-off between sensitivity and specificity
Opportunities	**Threats**
• Continued refinement through machine learning to reduce false positives. • Integration with other approaches to improve overall detection accuracy.	• Complexity in fine-tuning. • Adversarial attacks aiming to manipulate behavior-based models. • Difficulty in distinguishing between malicious and legitimate behavior.

Table4. *SWOT analysis for Machine* ***Learning***

Strengths	Weaknesses
• High adaptability, effectiveness against both known and unknown strains. • Effectiveness against both known and unknown ransomware strains with diverse training data. • Capability to reduce error rates through continuous training and refinement.	• Initial-false-positives/negatives, vulnerability to adversarial attacks. • Initial false positives and negatives during the learning phase. • Vulnerability to adversarial attacks aiming to deceive the model.
Opportunities	**Threats**
• Continuous learning, exploration of ensemble models. • Ongoing improvement through continuous learning and model updates. • Integration with other techniques for a comprehensive approach.	• Resource-intensive,training requirements. • Challenges in keeping up with evolving ransomware tactics.

Table5. *SWOT analysis for Honeypot* ***Technique***

Strengths	Weaknesses
• High capture in a controlled environment, low false positives. • High effectiveness for capturing ransomware samples in a controlled environment. • Low false positives as it focuses on capturing and analyzing.	• Real-time,compromise, recognition by attackers. • Delayed detection, as real systems might already be compromised by the time ransomware is identified. • Recognizable as a honeypot by sophisticated attackers.
Opportunities	**Threats**
• Integration with real-time detection, enhanced deception techniques. • Integration with real-time monitoring for faster response. • Enhancement through deception techniques to avoid detection	• Awareness by attackers. • Evolving tactics by attackers to recognize and avoid honeypots. • Limited real-world applicability for immediate threat mitigation

Table6. SWOT analysis for Statistics **Technique**

Strengths	Weaknesses
• Contribution to understanding, moderate to high effectiveness. • Moderate to high effectiveness based on the quality of baseline data and statistical methods. • Indirect contribution to reducing error rates by refining other techniques.	• Not primary detection. • Not a primary detection method, so it doesn't directly impact error rates. • Dependency on accurate baseline data for meaningful analysis.
Opportunities	**Threats**
• Informing other techniques, enhanced baseline data. • Integration with other techniques for a comprehensive threat intelligence approach. • Continuous improvement through refined statistical methods	• Dependency on data quality. • Misinterpretation of statistical data leading to misguided decisions. • Limited effectiveness without collaboration with primary detection methods.

5. CONCLUSION

The landscape of cyber threats, particularly ransomware, has undergone significant evolution, presenting challenges that demand dynamic and adaptable countermeasures. Our comparative analysis of various ransomware detection techniques underscores this evolving dynamic and offers insights into the strengths and limitations inherent to each method.

The Signature-based Approach, while formidable against known threats, highlights a clear vulnerability against new or slightly modified strains. Behavior-based Approaches, despite their adaptability, face challenges differentiating between malicious and benign behaviors. Machine Learning, with its promise of adaptive learning, is only as potent as the quality and diversity of its training data. Honeypots serve as efficient traps but are inherently reactive, potentially allowing real systems to be compromised before detection. Statistical Methods offer unique advantages but can be misled by sophisticated ransomware.

The analysis of Ransomware Features, while auxiliary, has demonstrated potential in refining and enhancing primary detection methods.

Each ransomware detection technique presents a unique set of strengths, weaknesses, opportunities, and threats. A comprehensive security strategy may involve a combination of these techniques, leveraging their strengths and addressing their respective challenges to enhance overall resilience against ransomware threats. Ongoing research and innovation are essential to stay ahead of the evolving landscape of cybersecurity threats

REFERENCES

[1] Abbasi, M. S., Al-Sahaf, H., Mansoori, M., & Welch, I. (2022). Behavior-based ransomware classification: A particle swarm optimization wrapper-based approach for feature selection. *Applied Soft Computing*, *121*, 108744.

[2] Alrawashdeh, K., & Purdy, C. (2019). Ransomware detection using limited precision deep learning structure in fpga. In NAECON 2018-IEEE National Aerospace and Electronics Conference (pp. 152-157). IEEE.

[3] Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware prevention and mitigation techniques. Int J Comput Appl, 117, 31-39.

[4] Baek, S., Jeon, J., Jeong, B., & Jeong, Y. S. (2021). Two-stage hybrid malware detection using deep learning. Human-centric Computing and Information Sciences, 11(27), 10-22967.

[5] Chen, Q., Islam, S. R., Haswell, H., & Bridges, R. A. (2019). Automated ransomware behavior analysis: Pattern extraction and early detection. In International Conference on Science of Cyber Security (pp. 199-214). Springer, Cham.

[6] Chew, C. J., & Kumar, V. (2019). Behaviour based ransomware detection. In: Proceedings - 34th International Conference on Computers and Their Applications. 2019;58:127-116.

[7] Chittooparambil, H. J., Shanmugam, B., Azam, S., Kannoorpatti, K., Jonkman, M., & Samy, G. N. (2019). A Review of ransomware families and detection methods. In International Conference of Reliable Information and Communication Technology (pp. 588-597). Springer, Cham.

[8] customerthink, Cloud Computing Security Risks and how to Protect Cloud Customers from Ransomware (2020). https://customerthink.com/ cloud-computing-security-risks-and-how-to-protect-cloud-customers-from ransomware/.

[9] De Groot, J. (2019). A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. Retrieved from Digital Guardian: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worstransomware-attacks-all-time

[10] Fernandez Maimo, L., Huertas Celdran, A., Perales Gomez, A. L., Garcia Clemente, F. J., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors, 19(5), 1114.

[11] Gómez-Hernández, J. A., Álvarez-González, L., & García-Teodoro, P. (2018). R-Locker: Thwarting ransomware action through a honeyfile-based approach. Computers & Security, 73, 389-398.

[12] Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019). Review of security and privacy for the Internet of Medical Things (IoMT). In 2019 15th international conference on distributed computing in sensor systems (DCOSS) (pp. 457-464). IEEE.

[13] Hirano, M., Hodota, R., & Kobayashi, R. (2022). RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. Forensic Science International: Digital Investigation, 40, 301314.

[14] Imaji, A. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods.

[15] Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), 8.

[16] Koeneman, S. H., & Cavanaugh, J. E. (2022). An improved asymptotic test for the Jaccard similarity index for binary data. Statistics & probability letters, 184, 109375

[17] Kok, S.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M. Ransomware, threat and detection techniques: A review. Int. J. Comput. Sci. Netw. Secur. 2019, 19, 136.Santorini, Greece, 29–31 May 2019; pp. 457–464.

[18] MarketsInsider, Infrascale survey reveals close to half of smbs have been ransomware attack targets (2020). https://markets.businessinsider. com/news/stocks/infrascale-survey-reveals-close-to-half-of-smbs-have-been ransomware-attack-targets-1029112584/

[19] Pont, J.; Arief, B.; Hernandez-Castro, J. Why current statistical approaches to ransomware detection fail. In International Conference on Information Security; Springer: Cham, Switzerland, 2020; pp. 199–216

[20] Tang, F., Ma, B., Li, J., Zhang, F., Su, J., & Ma, J. (2020). RansomSpector: An introspection-based approach to detect crypto ransomware. Computers & Security, 97, 101997.

[21] Tariq, U., Ullah, I., Yousuf Uddin, M., & Kwon, S. J. (2022). An Effective Self-Configurable Ransomware Prevention Technique for IoMT. Sensors, 22(21), 8516.

[22] Trustwave, 2020 trustwave global security report (2020). https://www.trustwave. com/en-us/resources/library/documents/2020-trustwave-global-security-report/.

[23] 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.

[24] Yamany, B., Elsayed, M. S., Jurcut, A. D., Abdelbaki, N., & Azer, M. A. (2022). A New Scheme for Ransomware Classification and Clustering Using Static Features. Electronics, 11(20), 3307.

[25] Zahoora, U., Rajarajan, M., Pan, Z., & Khan, A. (2022). Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier. Applied Intelligence, 1-20.

[26] Zhang, Y., Li, M., Zhang, X., He, Y., & Li, Z. (2022). Defeat Magic with Magic: A Novel Ransomware Attack Method to Dynamically Generate Malicious Payloads Based on PLC Control Logic. Applied Sciences, 12(17), 8408.

Citation: *Salah Abu Baker (2025). "Comparative Analysis of Ransomware Detection Techniques: Strengths and Vulnerabilities". International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), vol 11, no. 1, 2025, pp. 18-28. DOI: https://doi.org/10.20431/2349-4859.1101002.*