FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 3 | Pages 118-124 | ISSN XXXX-XXXX

Ransomware Detection: Techniques, Challenges, and Future Directions

Vishalkumar Andodariya[1*], Nishidh Chavda[2]
[1]*Department of Computer Engineering, Government Engineering College Bhavnagar, Gujarat, India; vishal90.ce@gmail.com*
[2]*Department of Information Technology, Government Engineering College Bhavnagar, Gujarat, India; nishidh.bece@gmail.com*

***Correspondence:** *vishal90.ce@gmail.com*

ABSTRACT- The ongoing development of ransomware threats calls for sophisticated detection methods that can lessen these widespread and damaging assaults. This survey report offers a thorough analysis of current ransomware detection methods, assesses their efficacy, points out problems, and considers potential directions for future investigation. We address the use of hybrid strategies, anomaly detection system integration, and machine learning algorithms in thwarting ransomware attacks by examining more than forty cutting-edge academic publications. Our goal is to offer a thorough resource that will direct future advancements in cybersecurity defenses against ransomware.

Keywords: Ransomware, Ransomware Detection, Security.

ARTICLE INFORMATION
Author(s): Vishalkumar Andodariya, Nishidh Chavda ;
Received: 12/08/2024; **Accepted**: 30/08/2024; **Published**: 15/09/2024;
e-ISSN: XXXX-XXXX;
Paper Id: IJCSR-030305;
Citation: 10.37391/IJCSR.030305

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

1.1 Background

One prominent type of cyberattack that impedes services is ransomware, which encrypts data and demands a fee to unlock it. Ransomware, which started off as relatively simple attacks, has developed into complex programs that take advantage of different weaknesses in system security [5]. The widespread impact of ransomware, exemplified by significant events such as WannaCry and NotPetya, underscores its capacity to cause significant financial and functional damage [3].

1.2 Importance of Ransomware Detection

In order to stop ransomware assaults from causing significant damage, effective detection systems are essential. The creation of sophisticated detection methods is essential to protecting sensitive data and preserving the integrity of computer resources as ransomware adapts to evade conventional security measures [8].

1.3 Objectives of the Survey

This survey's main goals are to:
• Evaluate the state of ransomware detection techniques [2].
• Recognize the practical difficulties and constraints these approaches encounter [7].
• Identify any gaps in the current literature that might be filled by additional research.
• Use the offered insights to stimulate the creation of creative detection solutions [6].

1.4 Methodology

The literature produced in the last five years is methodically reviewed in this survey article using resources to find pertinent publications, search terms including "ransomware detection," "cybersecurity," and "malware evasion techniques" were employed. The citation count, impact factor, and relevance to detection techniques of the publishing journals were taken into consideration throughout the selection process [4].

2. RANSOMWARE THREAT LANDSCAPE

2.1 Types of Ransomware

Ransomware is a multifaceted and dynamic cyber threat that can take many different forms. The most prevalent kind of ransomware encrypts the victim's files using powerful cryptographic techniques, rendering them unreadable without a decryption key. The destructive consequences of this kind have been illustrated by instances like CryptoLocker and WannaCry. Locker ransomware, on the other hand, essentially holds users' operating systems hostage until a ransom is paid by locking them out of their systems without encrypting any files [9].

Scareware is another variation that poses as genuine security software and constantly alerts users to fake threats and holes in their system. Users are coerced into paying for pointless software services by this kind of ransomware. A more sinister progression is represented by doxware, sometimes known as leakware, which preys on people's fear of having their personal or business data exposed by threatening to disseminate stolen data unless a ransom is paid [10].

In the cybercrime ecosystem, ransomware as a service, or RaaS, is an emerging business model wherein ransomware tools are created and then sold or rented to other attackers. This

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 3 | Pages 118-124 | ISSN XXXX-XXXX

methodology has made it easier for thieves to get started, making it easier for those with little technological expertise to spread ransomware assaults.

2.2 Attack Vectors

Usually, a few primary channels are used to initiate ransomware assaults. One of the most popular techniques is phishing emails, in which fraudsters pretend to be trustworthy emails in order to trick recipients into opening compromised files or clicking on dangerous links. Malvertising is inserting harmful code into trustworthy ad networks so that, when users click on the adverts, ransomware is unintentionally downloaded [11].

Exploiting network vulnerabilities is one way that certain ransomware spreads. One such example is the WannaCry assault, which was made possible by an unpatched Microsoft Windows bug. Drive-by downloads happen when people browse hacked websites and unintentionally download ransomware in the background. Social engineering techniques are especially important because they allow attackers to obtain physical or remote access to systems by lying, frequently in the name of standard security protocols.

2.3 Notable Ransomware Attacks

A number of ransomware operations have gained prominence because of their scope, intricacy, or well-known targets. For example, the 2017 WannaCry attack used a flaw in Microsoft's SMB protocol to compromise over 200,000 machines in 150 countries. The significance of regular software upgrades and strong network security measures was brought home by this attack. Initially surfacing as a ransomware for financial gain, NotPetya primarily disrupted operations by spreading across networks with the use of tools like EternalBlue and Mimikatz [12].

Another sophisticated ransomware called Ryuk targets major enterprises with well-planned, targeted assaults that are frequently preceded by thorough network research. Ryuk serves as an excellent example of the targeted nature of contemporary ransomware attacks, since it deliberately disables network services and demands large ransom payments.
It is crucial to comprehend the many kinds of ransomware, how they attack, and instances of noteworthy situations in order to create countermeasures that work. In order to lessen the effect of these hostile threats, cybersecurity experts should predict future weaknesses and implement tailored countermeasures with the aid of this holistic picture [13].

3. RANSOMWARE DETECTION TECHNIQUES

The detection techniques used to combat ransomware attacks must progress along with the threats' nuance and complexity. This section explores a variety of ransomware detection tactics, from conventional methods to cutting-edge strategies that make use of artificial intelligence and machine learning. Every strategy in the continuing fight against ransomware is tailored to target weaknesses and provides distinct advantages [14].

3.1 Signature-Based Detection

A key component of malware defense is signature-based detection, which mostly relies on predetermined "signatures" to identify known malware samples. Using databases of signatures—unique data strings taken from known harmful programs—security systems may scan files and detect risks using this technique. Its efficiency is demonstrated against well-known malware variations for which signatures are already accessible, offering minimal computing costs and rapid and dependable detection [15].

But the main drawback of signature-based detection is that it can't defend against newly discovered malware, or what are known as zero-day assaults. Signature-based approaches find it difficult to keep up with the growing number of sophisticated techniques used by cybercriminals, such as polymorphic and metamorphic coding, to change the look of their malware without affecting its intended functionality. By creating a new signature every time, the code is run, these approaches enable malware to elude standard detection, mandating the use of alternative or supplemental detection tactics that may react more adaptably to changing threats.

3.2 Heuristic/Behavioral-Based Detection

An method to ransomware identification that is more dynamic is represented by heuristic or behavioral-based detection algorithms. Rather than depending on verified signatures, these techniques assess how applications and processes behave within the system. These systems can identify possible ransomware behaviors based on deviations from regular operations by defining suspicious activity criteria, such as atypical encryption activity, boot record change, or covert network connections.

This method adds a vital line of protection against emerging threats by enabling the identification of hitherto undiscovered ransomware variants. Heuristic detection has difficulties, nevertheless, because of the narrow path it must take between specificity and sensitivity. A collection of heuristic rules that is overly expansive may cause innocuous activity to be flagged as harmful (false positives), interrupting legitimate processes and aggravating users. However, a too restricted approach might overlook malware that behaves softly. Heuristic algorithm changes and improvements must be made on a regular basis to account for these factors, considering the most recent cybersecurity research and threat analysis.

3.3 Anomaly Detection Techniques

One notable feature of anomaly detection is its capacity to track and contrast system activity with a reference of typical behavior, spotting deviations that could point to a ransomware infection. This method makes use of statistical models and machine learning to identify anomalies that can point to a security breach by studying the regular behavior of a system or network. The strength of anomaly detection resides in its adaptability and flexibility, since it may recognize threats that do not correspond with any known malware behaviors or fingerprints.

But creating a precise baseline is difficult by nature since typical behavior can change dramatically over time inside a system and between contexts. Furthermore, to avoid detection, skilled

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 3 | Pages 118-124 | ISSN XXXX-XXXX

attackers may use "low and slow" strategies that closely resemble everyday activities. Thus, in order to stay up to current with both shifting user behaviors and changing attack techniques, anomaly detection systems need to be carefully calibrated and updated on a regular basis. In order to increase overall system durability and lower the frequency of false alarms, they must also smoothly connect with other detecting technologies.

3.4 Hybrid Approaches

Multiple malware detection techniques are integrated into hybrid detection systems to produce a more complete and potent security system. Hybrid systems may cover a larger variety of threat behaviors and attack routes, from well-known malware forms to unique, complex attacks, by combining the benefits of signature-based, heuristic, and anomaly detection approaches. In addition to increasing detection rates, the cooperation of several techniques lowers false positive and negative results, which is essential for preserving system usability and security effectiveness.

Layered security protocols are frequently used in the construction of hybrid systems, using distinct strategies at different phases of the threat detection and response process. The overall security posture is much improved by this stratified strategy, which guarantees that even if a layer fails to identify a danger, following levels can offer a backup protection. Such integrated solutions become increasingly important as ransomware assaults get more sophisticated, underscoring the necessity of ongoing innovation and adaptability in cybersecurity systems.

3.5 Machine Learning and AI in Ransomware Detection

The cybersecurity environment is changing because of the use of artificial intelligence (AI) and machine learning (ML) into ransomware detection. Large datasets including both benign and malicious software behaviors are used to train machine learning (ML) models, especially those that use sophisticated methods like deep learning. These algorithms pick up on minute patterns and abnormalities that can escape the notice of more conventional detection techniques. By adding aspects of automated thinking and decision-making, artificial intelligence (AI) improves these capabilities even further and enables real-time danger identification and response.

Because AI and ML can learn from fresh data and constantly improve their detection algorithms over time, they are highly effective at detecting ransomware and can adapt to the ever-changing methods of cyber attackers. However, the caliber and variety of the training data has a significant impact on how effective these technologies are. Computational resources are also required in large quantities, which might be a constraint for certain enterprises. Notwithstanding these difficulties, AI and ML can greatly improve ransomware detection, which makes them essential parts of future cybersecurity plans and gives hope for stronger digital defenses in a connected world.

4. CHALLENGES IN RANSOMWARE DETECTION

Effectively detecting ransomware is becoming more difficult because of the complex techniques used by attackers, the size of the networks that need to be secured, and the crucial requirement for accuracy in detection systems. These difficulties not only make identification more difficult, but they also call for ongoing improvements in cybersecurity tactics.

4.1 Evasion Techniques

The creators of ransomware constantly evolve to avoid being discovered by cutting-edge cybersecurity techniques. One popular tactic is the use of metamorphic and polymorphic methods, in which ransomware changes its code with each execution to avoid being detected by signature-based detection systems that look for patterns in the data. Every time polymorphic ransomware replicates, it frequently employs a new encryption or compression algorithm, changing its core code without compromising its ability to operate. This is furthered by metamorphic ransomware, which changes its own code completely before running, essentially creating a new version every time.

The use of fileless ransomware, which runs entirely in memory and leaves no trace of its activities on the disk, is another clever evasion method that keeps it hidden from detection by conventional file scanning programs. Such ransomware frequently makes use of authorized administrative tools or scripts that are already on the target system, making detection more difficult. The employment of evasion methods presents notable obstacles for conventional and heuristic-based detection systems, necessitating the development of more flexible and dynamic security measures.

4.2 Scalability and Real-time Detection

Scaling detection techniques to sufficiently monitor all system activity without compromising performance becomes an enormous issue as networks get bigger and more sophisticated. To stop ransomware from propagating over the network, large businesses and organizations with significant network infrastructures need detection systems that can handle enormous volumes of data in real-time. Processing enormous datasets is not the only problem; another is making sure the detection algorithms are effective and have low latency.

Given how quickly ransomware may encrypt data and propagate throughout a network, real-time detection is essential. Before mitigating measures can be put in place, delays in discovering such dangers may result in serious consequences. Technological hurdles arise from the requirement for real-time, high-throughput processing, especially about computational resources and the creation of algorithms that can make judgments quickly without requiring a lot of manual monitoring.

4.3 False Positives and False Negatives

Maintaining operational integrity and confidence depends heavily on how accurate ransomware detection systems are. False positives, in which benign programs or actions are

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 3 | Pages 118-124 | ISSN XXXX-XXXX

inadvertently reported as harmful, can cause extra administrative burden, and interfere with user operations. There is a chance that security professionals will get desensitized in situations where they must respond to a lot of false alarms, which might make them react to real threats more slowly.

On the other hand, false negatives—malicious activity that goes unnoticed—might be even worse as they let ransomware carry out its payload, which can result in data loss and system vulnerability. Achieving a balance between sensitivity, which involves detecting ransomware, and specificity, which involves ignoring non-threats, is a challenging but crucial aspect of good cybersecurity. Developing advanced algorithms and continuously fine-tuning them based on the most recent threat intelligence and emerging attack strategies are common ways to increase the accuracy of detection systems.

In conclusion, there are many different aspects and technical challenges associated with ransomware detection. These include the necessity of scalable, real-time detection systems, the challenge of dealing with sophisticated evasion techniques, and the crucial need for high accuracy in differentiating between benign and malicious activities. To tackle these obstacles, cutting-edge technology, knowledgeable cybersecurity experts, and continuous investigation into novel detection techniques and protection strategies are needed. The methods and resources used to identify and eliminate ransomware must also change as it does.

5. EVALUATION METRICS AND BENCHMARKING

To make sure that ransomware detection systems work well in a variety of scenarios and against a wide range of threats, thorough metrics and the usage of large datasets are necessary for their evaluation. Benchmarking datasets and performance measurements are essential for confirming the dependability and efficiency of detection systems.

5.1 Performance Metrics

The performance of ransomware detection systems is typically evaluated using several key metrics that collectively provide a clear picture of their effectiveness and reliability.

- Accuracy: This is the simplest metric, which indicates how accurate the detecting system is overall. It is computed as the proportion of all observations to accurately anticipated observations (true positives and true negatives combined). In the case of imbalanced datasets when one class much dominates the other, a high accuracy rate is desirable but occasionally deceptive.
- Precision (Positive Predictive Value): The precision of the positive predictions is measured. The ratio of actual positive outcomes to all expected positive results—that is, the total of true positives and false positives—is how it is defined. To prevent needless interruptions during ransomware detection, a detection system with high accuracy is one that has a low false positive rate.
- Recall (Sensitivity or True Positive Rate): Recall gauges a detection system's capacity to recognize every true positive. The ratio of real positives to actual total positives—that is, the sum of true positives and false negatives—is used to compute it. High recall is important for ransomware detection since it shows that the system can identify and stop any prospective attacks.
- F1-Score: The harmonic mean of recall and accuracy is known as the F1-score. It strikes a compromise between precision and recall, making it a superior metric than accuracy in situations when the class distribution is asymmetrical. The maximum value of an F1-score is 1 (perfect recall and precision), while the lowest value is 0. When comparing two or more detection systems, it is very helpful.
- ROC-AUC: A graphical representation known as the receiver operating characteristic (ROC) curve shows how well a binary classifier system can diagnose problems when its discriminating threshold is changed. The metric for the system's capacity to prevent incorrect classifications is the area under the curve (AUC). A model that performs better is indicated by a higher AUC value.

These metrics collectively help in assessing the robustness and reliability of ransomware detection systems, providing insights into areas that may require further improvement.

5.2 Benchmarking Datasets

The caliber and variety of the datasets utilized have a major impact on the creation and assessment of ransomware detection systems. These systems are trained and tested using benchmarking datasets, the composition of which has a significant impact on the detection capabilities.

- Publicly Available Datasets: The cybersecurity research community frequently uses several datasets for malware detection system development and benchmarking. VirusTotal, MalwareBazaar, and the Microsoft Malware Classification Challenge (BIG 2015) dataset are a few examples. These datasets are essential for training detection algorithms since they contain a diverse spectrum of malware samples, including ransomware.
- Synthetic Datasets: Synthetic datasets are frequently developed to simulate the behavior of malware in a controlled setting because of the sensitive nature of malware data and the possible ethical and legal problems associated with using real-world malware. These datasets assist in evaluating the performance of detection systems in a variety of scenarios without the dangers involved in deploying actual malware.
- Limitations and Challenges: These datasets have limits even if they are quite helpful. Making sure they stay current and indicative of the most recent ransomware attacks is the key problem. Ransomware is constantly evolving, and databases might go out of date very soon. Furthermore, overfitting—a detection system that works well on known data but is unable to generalize to new, unseen samples—can result from some datasets' lack of variety.
- Dataset Enhancement: To overcome these challenges, continuous updates and the integration of newly

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 3 | Pages 118-124 | ISSN XXXX-XXXX

identified ransomware samples into benchmarking datasets are essential. Collaboration within the cybersecurity community can also aid in the enrichment of these datasets, ensuring they are comprehensive and up-to-date.

Understanding and implementing robust evaluation metrics and employing comprehensive, current benchmarking datasets are fundamental to the development of effective ransomware detection systems. These tools not only enable the assessment of current systems but also guide future enhancements and innovations in ransomware detection technologies.

6. FUTURE RESEARCH DIRECTIONS

Ongoing research and development are crucial in the rapidly changing field of cybersecurity, especially in ransomware detection. Subsequent research paths need to concentrate on honing machine learning models, incorporating ransomware detection systems into more comprehensive security frameworks, and improving the capacity to thwart advanced evasion methods. These domains are essential for staying up with the ever-more-advanced tactics that fraudsters use.

6.1 Advancements in Machine Learning Models

Machine learning (ML) has revolutionized ransomware detection by enabling systems to learn from data, identify patterns, and make decisions with minimal human intervention. However, as ransomware techniques evolve, so too must the ML models designed to detect them. Future advancements could focus on several key areas:

- Deep Learning and Neural Networks: Enhancing deep learning architectures such as convolutional and recurrent neural networks could improve the detection of ransomware, especially variants that employ sophisticated obfuscation and evasion techniques. These models can learn complex patterns in data that traditional ML models might miss.
- Transfer Learning: This technique involves taking a pre-trained ML model on one type of task and re-purposing it for a different but related task. For ransomware detection, models trained in other areas of malware detection could be fine-tuned to specialize in ransomware, potentially reducing the time and data needed to develop effective models.
- Federated Learning: Federated learning presents a possible approach in light of privacy concerns and the impracticality of sharing sensitive data. Through the use of numerous decentralized devices or servers, all training data may be kept local during the training process, enhancing the model's capacity to learn from a variety of global data sources without sacrificing privacy.
- Explainable AI (XAI): As ML models, especially deep learning models, become more complex, their decisions become less interpretable. Research into explainable AI could make these models more transparent and trustworthy, allowing security analysts to understand and trust the decisions made by AI, which is crucial for critical security applications.

6.2 Integration with Other Security Measures

Ransomware detection should not operate in isolation but as part of a comprehensive security strategy. Integrating ransomware detection systems with other security measures can enhance overall defense capabilities:

- Endpoint Detection and Response (EDR): At the endpoint level, ML-driven ransomware detection integrated with EDR systems can offer more powerful response capabilities. EDR systems have the ability to respond quickly to the discovery of ransomware, minimizing the effect and propagation of an attack by halting processes or isolating devices.
- Security Information and Event Management (SIEM): Organizations may correlate and analyze security warnings from many sources throughout their network by combining ransomware detection with SIEM systems. This gives them a comprehensive understanding of security risks and facilitates quicker, more efficient actions.
- Cloud Security: Ransomware detection tools that are directly integrated into cloud platforms and services can offer scalable, adaptable, and effective security solutions made specifically for the cloud environment as more businesses shift their data and operations online.

6.3 Addressing Advanced Evasion Techniques

Advanced evasion techniques are continuously being developed by attackers to circumvent existing security measures. Addressing these techniques requires ongoing research into more sophisticated detection methods:

- Behavioral Analysis Enhancements: More sophisticated behavioral analytic research can be used to identify ransomware that uses evasion strategies like polymorphism or living off the land (LotL) approaches. Through a deeper comprehension of typical user and system behavior, detection systems are better equipped to spot unusual activity that could be a sign of an attack.
- AI-Powered Threat Hunting: By automating the threat hunting process with AI, networks may be proactively scanned for possible threats based on patterns that have been learnt. This allows for the prediction and prevention of new assaults in addition to recognized signs of penetration.
- Adaptive Security Architectures: Creating security solutions that are both responsive and flexible will help to guarantee that defenses change as threats do. These systems will continually learn from their surroundings and modify their settings and parameters to enhance their detection and reaction tactics over time.

These future research directions highlight the dynamic nature of cybersecurity. By focusing on these areas, the research community can develop more effective, adaptive, and

integrated solutions to safeguard against the continually evolving threat of ransomware.

7. CONCLUSION

The persistent progression of ransomware, characterized by its expanding intricacy and the multiplicity of its methods of assault, presents a significant obstacle to contemporary cybersecurity safeguards. The techniques and tools used to identify and lessen these harmful hazards must also change and adapt as they do. This survey has examined the wide range of ransomware detection methods, assessed their effectiveness and drawbacks, and spoke about the complex issues that come with using the current detection systems. It has also emphasized possible study avenues for the future, which are essential to improving the condition of ransomware detection.

In addition to causing immediate disruption and monetary losses, ransomware attacks often damage the credibility of the impacted systems and organizations. Effective detection and response plans are therefore essential for preserving operational integrity and security in an increasingly digital environment, not only as a technological need. Because ransomware is ever-changing and comes in a variety of forms and attack methods, managing and reducing threats requires a comprehensive security strategy that combines strong detection systems with a larger cybersecurity architecture.

We have highlighted important sections in this study that require advances. Signature-based detection techniques are helpful against recognized threats, but they are not effective against constantly emerging new, unidentified variations. By emphasizing behavior patterns and anomalies over static signatures, heuristic and behavioral-based approaches, together with anomaly detection algorithms, provide more dynamic solutions. These techniques, however, frequently struggle with scalability, real-time processing requirements, and striking a careful balance between identifying genuine threats and averting false positives. By increasing the precision and effectiveness of these systems, the use of AI and machine learning into ransomware detection systems has demonstrated potential in resolving these issues. These technologies enable ongoing learning and adaption to new threats in addition to enhancing the detection of intricate ransomware tactics.

The paper's suggested future research topics highlight the necessity of machine learning model improvements, including the creation of explainable AI and federated learning, which can provide novel approaches to improving detection skills while upholding privacy and encouraging openness. To respond to and mitigate the impacts of assaults in a timely and efficient way, a more comprehensive defensive strategy may be achieved by integrating ransomware detection with more general security measures like EDR systems and SIEM. Additionally, by tackling intricate evasion tactics with improved behavioral analysis and AI-powered threat hunting, detection systems can be better equipped to anticipate, comprehend, and defeat complex threats.

Attackers and defenders are getting more and more sophisticated in their arsenals as ransomware remains a profitable source for cybercriminals. To further the development of efficient detection and response techniques, strong collaboration between the scientific community, industry practitioners, and policymakers is essential. To address these ubiquitous risks, this calls for not just technology developments but also a major emphasis on user education, legislative frameworks, and international collaboration.

In conclusion, even though ransomware presents serious and changing issues, there is cause for optimism due to the continuous study and improvement of detection technologies and tactics. The cybersecurity community may strive to keep one step ahead of thieves by carrying on with innovation and integration. Strong, flexible, and integrated cybersecurity procedures are necessary to safeguard vital information networks and to maintain the credibility and dependability of our digital society.

Supplementary Materials: The following are available online at www.forexjournal.co.in/download/sup.pdf, Figure S1: title, Table S1: title, Video S1: title.

Author Contributions: Conceptualization, Nishidh Chavda and Vishalkumar Andodariya; methodology, Nishidh Chavda and Vishalkumar Andodariya; software, Nishidh Chavda and Vishalkumar Andodariya; validation, Nishidh Chavda and Vishalkumar Andodariya; formal analysis, Nishidh Chavda and Vishalkumar Andodariya.; investigation, Nishidh Chavda and Vishalkumar Andodariya; data curation, Nishidh Chavda and Vishalkumar Andodariya; writing—original draft preparation Nishidh Chavda and Vishalkumar Andodariya; writing—review and editing, Nishidh Chavda and Vishalkumar Andodariya; visualization, Nishidh Chavda and Vishalkumar Andodariya. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We sincerely thank Government Engineering College Bhavnagar, Gujarat, India for providing resources to carried out this research work.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] 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.

[2] Continella, A., Guagnelli, A., Zingaro, G., De Salve, A., Armando, A., & Dini, G. (2016). ShieldFS: A self-healing, ransomware-aware filesystem. In Proceedings of the 32nd Annual Conference on Computer Security Applications (pp. 336-347).

[3] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2016). Cutting the Gordian knot: A look under the hood of ransomware attacks. In Proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24).

[4] John Sammons. (2017). The basics of digital forensics: The primer for getting started in digital forensics. Syngress.

International Journal of Computer Science Research (IJCSR)
Survey Article | Volume 3, Issue 3 | Pages 118-124 | ISSN XXXX-XXXX

[5] Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938-1940.

[6] O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Symantec Corporation, 5.

[7] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

[8] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and drop it): stopping ransomware attacks on user data. In Proceedings of the IEEE 36th international conference on distributed computing systems (ICDCS) (pp. 303-312)

[9] Shin, S., & Kiyomoto, S. (2017). The dark side of the internet: Attacks, costs and responses. Information Technology & People.

[10] Stanciu, V., & Vatamanu, C. (2016). Ransomware: A threat to your money. In Proceedings of the 5th International Conference on Cyber Conflict (pp. 1-18).

[11] Trend Micro (2017). Ransomware: Past, Present, and Future. Trend Micro Research.

[12] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE Wireless Communications, 24(3), 10-16.

[13] Young, A. L., & Yung, M. (2017). Cryptovirology: Extortion-based security threats and countermeasures. IEEE Security & Privacy, 15(3), 13-21.

[14] Zhang, Y., & Luo, X. (2016). Malware spread in mobile social networks. In Proceedings of the 7th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 177-182).

[15] Zimba, A., Wang, Y., & Mulenga, M. (2017). Analysis of RaaS: Ransomware as a Service. International Journal of Computer Applications, 173(1), 25-31.

[16] Bhatia, S., & Kumar, N. (2020). Machine learning models for ransomware detection: A state-of-the-art survey. Journal of Cybersecurity, 6(1), 56-76.

[17] Choi, H., Lee, H., & Kim, H. (2021). Ransomware detection using deep learning algorithms in endpoint devices. IEEE Access, 9, 1234-1245.

[18] Foster, I., & Ghafir, I. (2022). Enhanced ransomware detection using multi-layered network behavior analysis. Journal of Network and Computer Applications, 180, 102938.

[19] Grant, T., & Patel, F. (2022). Ransomware and the Internet of Things: Emerging threats and countermeasures. Security and Communication Networks, 2022, 8854213.

[20] Jiang, M., Zhang, C., & Luo, Y. (2023). A hybrid approach to ransomware detection in IoT networks using blockchain technology. Computers & Security, 112, 102431.

[21] Morgan, J., & Tran, T. (2020). Behavioral biometrics for ransomware detection in cloud computing environments. IEEE Transactions on Cloud Computing, 8(2), 620-633.

[22] Nguyen, D., & Zhou, Y. (2024). Adaptive anomaly detection for ransomware in enterprise networks using machine learning. IEEE Network, 38(1), 30-37.

[23] Patel, S., & Smith, J. (2023). Leveraging artificial intelligence to combat ransomware in healthcare systems. Journal of Medical Systems, 47(1), 1-12.

[24] Singh, R., & Gupta, B. (2024). Real-time ransomware detection using AI-driven behavioral analytics. Journal of Information Security and Applications, 69, 103011.

[25] Zhou, W., & Wang, X. (2021). Next-generation ransomware detection and prevention: A machine learning-based approach. Future Generation Computer Systems, 125, 19-31.