iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67850

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Harnessing Machine Learning for Early Ransomware Detection and Prevention

Sri Vaishnavi Koduri[1], Pampari Rohan Raj[2], L. Chandra Sekhar Reddy[3], M. Parameswar[4]
[1]*Artificial Intelligence and Data Science,* [2]*Cybersecurity, CMR College of Engineering and Technology, Hyderabad, India*
[3, 4]*Artificial Intelligence and Data Science, CMR College of Engineering and Technology, Hyderabad, India*

Abstract: ***Ransomware attacks pose significant and critical threats to organizations, individuals, etc. This generally leads to loss of data, financially and economically. This paper explains the applications and advantages of using Data Science Techniques in Cybersecurity in order to prevent ransom attacks that may cause complications in using or sharing of data. Firstly, the characteristics and behaviors of ransomware attacks need to be examined. This enables the model to understand the proactive measures. Machine Learning algorithms like Random Forest and XGBoost, Decision Trees, Isolation Forest, SVM are used to analyze and understand historical Ransom attacks. These algorithms help in analyzing hidden patterns, and indicate potential ransomware threats. The integration of Data Science techniques with Cybersecurity increases the effectiveness of the model's performance. This can be aided with a comprehensive dataset that highlights the key attributes required for providing accurate results. It also plays an important role in enhancing the role of Cybersecurity frameworks. Finally, the predictive models are integrated into the real time security systems, emphasizing the importance of continuous monitoring to mitigate ransomware attacks. This research paper underscores the potential of Data Science as a critical tool in battling ransomware attacks.***

Keywords: Ransomware, SVM, Isolation Forest, Ransomware prediction, Decision Trees, Random Forest, Cyber Security, Data Science.

I. INTRODUCTION

Malicious attacks such as malwares, ransomware attacks, phishing attacks, etc have become one of the most concerning issues in the branch of cybersecurity lately. Ransomware is a type of malicious software that encrypts victims data and demands for ransom in exchange for its release. It usually targets both organizations and individuals alike causing financial losses, data breaches, and other hazards[17]. Traditional ransomware detection techniques including event-based,statistical-based, and data-centric-based techniques are not adequate to combat. The growing popularity of ransomware attacks and their ability to evade through traditional security measures has urged the need for proper solutions to predict and prevent such attacks to secure the system data. Data science has become a vital tool in battling the growing threat of ransomware. By using AI, ML and data analytics, researchers and analysts can spot various patterns and trends in malicious activity which detect potential threats as they occur, and minimize the risk of ransom attacks. These advanced ML techniques allow for smart and fast responses, helping to stay ahead of cybercriminals and protect sensitive data before it's too late. These techniques enable strategic defense mechanisms that go beyond existing cybersecurity approaches, offering the potential to forecast attacks and hinder them before they can cause any harm. This paper explains the application of data science in ransomware prediction and prevention. It derives the importance of data-driven approaches in analyzing huge amounts of network traffic, user behavior, and system logs to identify and verify early signs of ransomware activities. This enables the user to put an end to the attack before it latches itself to the network system. It also digs deep into various Data Science methods, including Random Forests, Decision Trees and behavioral analysis, which can be applied to predict ransomware attacks with better accuracy and hence increases the performance of the model[1]. The main objective is to focus on the prevention and early detection of data loss, data breaches caused by malicious softwares, enhancing real-time detection,and mitigating ransomware risks and to improve cybersecurity efficiency. Multiple machine learning tools and techniques can help in overcoming this problem of handling huge datasets of malicious and suspectful activities and analyzing it .

II. RELATED WORKS

In recent years, multiple studies have explored the application of data science techniques for ransomware prediction and prevention. One such area of research involves the use of machine learning algorithms such as decision trees, support vector machines (SVM), and random forests to classify malicious and benign activities by analyzing network traffic and system logs. Bhuvaneswari1, Gopinath, K.S.Shyam, A.Manoj, B. Sudarshan built a model able to predict the types of ransomware attacks [9]. Then the pre-processing techniques are applied to deal with missing values.

The preprocessed data is then used to build a model by dividing the dataset into 7:3 ratios Where 70% of the data is used for training purposes where the model learns the pattern and the remaining 30% testing data is used to test. Mohammad Masum, Md Jobair Hossain Faruk, Hossain Shahriar, Muhaiminul Islam Adnan have applied traditional and basic ML classifiers to detect ransomware. Several studies have explored machine learning for ransomware detection. Shabtai et al. investigated behavioral analysis using file system activity. Al-Garadi et al. explored anomaly-based detection[10]. Research by Saxe & Anderson highlighted deep learning's potential for malware analysis.

Liu et al.'s work on Isolation Forest offers an effective unsupervised approach. Furthermore, ensemble methods like Random Forest, as described by Breiman, have shown promise in capturing complex ransomware patterns. These works provide a foundation for early ransomware detection and prevention using machine learning.

III. BENEFITS OF RANSOMWARE PREVENTION

Ransomware prevention offers many important benefits, mainly by preventing the disastrous consequences of a successful attack. Its greatest advantage is preventing important financial losses. Ransomware attacks are expensive, costing businesses money for ransom payments, recovery, legal and public relations fees and lost revenue due to business disruption. Through the prevention of some attacks, organizations avoid many of these costs and potentially save millions of dollars[2]. Ransomware prevention is important for safeguarding sensitive data and preventing immediate financial losses. Ransomware attacks encrypt and sometimes infiltrate all or some sensitive data and this exposes businesses to several data breaches, many regulatory penalties and the theft of some intellectual property.

Preventing these attacks protects important data and maintains customer and partner trust for organizations. This protection guarantees personal data is safe, compliant with privacy regulations and shielded from reputational harm caused by data breaches. Business continuity is also an analytically important benefit. Ransomware attacks cause major running disruptions and stop important services.

Preventing these attacks guarantees continued operation by maintaining business productivity, avoiding disruptions and minimizing downtime. This is especially important for organizations offering necessary services such as healthcare, emergency response and important infrastructure. Prevention enables these organizations to operate reliably and avoid being held hostage. Ransomware protection safeguards an organization's reputation. Ransomware attacks considerably damage company image, resulting in the loss of large customer trust and harming many business relationships. By investing in strong prevention measures, organizations show a serious commitment to cybersecurity and data protection, safeguarding their reputation and guaranteeing stakeholder satisfaction[11].

Thorough preventative measures ultimately guarantee the continued availability of all important IT resources. Ransomware attacks require important time and effort from IT staff to respond to and recover from. Preventing many attacks frees up organizational resources for more considerately deliberated initiatives, thus improving overall IT efficiency and cybersecurity.. Preventing ransomware proactively protects finances, data, operations, reputation and resources, thus building a more resilient and secure organization[12].

IV. STEPS INVOLVED IN PREVENTING RANSOMWARE ATTACKS

In this section, the paper discusses the various steps involved in analyzing and classification of the ransom attacks posed on the client system.

The overview on this issue involves a step by step procedure as follows:

1) *Threat Analysis:* Threat analysis involves spotting, understanding, and assessing possible weaknesses, dangers, and risks in a specific setting[18]. During this step of prevention, the aim is to collect information and observe patterns about possible attack methods, the people behind the threats, and the kinds of cyber dangers that might threaten the system. Some of the key activities include historical data on breaches, organization’s infrastructure, identifying weak entry points, and prioritizing threats based on likelihood and impact. This step lays the foundation for implementing effective anomaly detection systems. Ransomware attacks usually start when hackers get in through phishing emails, harmful downloads, RDP exploits, or software weaknesses. After they gain access, the ransomware locks up files and asks for payment to unlock them. Key indicators of ransomware activity include mass file encryption, unauthorized access attempts, unusual network traffic, and abnormal system process execution[23].

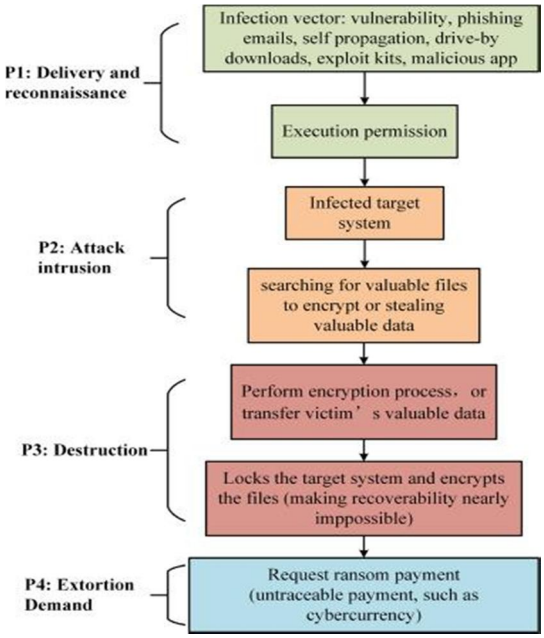


Fig. 1. Early detection of Ransomware attacks

2) *Data Collection & Preprocessing:* Building a strong ransomware prediction model requires high-quality data, including system logs, network traffic, threat intelligence and user activity. Detailed system logs offer important understandings into many process executions, large file modifications and registry alterations and this thorough network traffic data aids in the detection of communication with malicious servers. Data preprocessing involves cleaning to remove redundancies, feature extraction to identify key ransomware indicators, labeling to classify normal and malicious activities, as well as normalization of numerical values[19]. Accurate performance in real-world detection scenarios by many machine learning models depends on using properly preprocessed data. Effective anomaly detection along with behavioral analysis requires the collection of many relevant datasets. System logs, network traffic and user activity data are included in these datasets. Careful preprocessing, cleaning, normalization and transformation of all the data into a usable format is important for effective data analysis. This includes managing missing values and extraneous noise and transforming categorical features into numerical representations. High-quality data prioritization is necessary for preventing biased or inaccurate model development[3].
3) *Exploratory Data Analysis(EDA):* Data exploration helps understand its characteristics and structure. Exploratory data analysis helps pinpoint outliers, key trends and data distributions. These are important for building accurate threat detection models. EDA analyzes trends in system activity. This reveals patterns in ransomware behavior. Powerful visualizations, including detailed time-series plots, effectively reveal important anomalies such as sudden, sharp spikes in file encryption or network activity.
4) *Model Selection & Training:* Machine learning models for ransomware detection typically use either supervised or unsupervised learning. Random Forest, XGBoost, along with Support Vector Machines (SVM), in addition to other supervised models, highly successfully identify ransomware using precisely defined features. Deep learning techniques are important for analyzing sequential data. LSTMs and CNNs are examples of these techniques used to analyze system logs and network traffic. Unsupervised learning methods, such as Isolation Forests and Autoencoders, effectively detect zero-day ransomware attacks by identifying normal system behavior and pointing out deviations. Strong ransomware threat detection relies on using metrics such as accuracy, precision, recall, F1-score and AUC-ROC to assess model performance and selecting the optimal machine learning or statistical model for anomaly detection[20]. Clustering algorithms, neural networks and ensemble methods are examples of models that may be used, depending on the application. Further training employs the preprocessed data, allowing the model to distinguish between normal and abnormal behaviors. This research prioritizes all hyperparameter optimization and good generalization to all unseen data. Several cross-validation techniques assess the selected model's performance[16].

5) *Real time anomaly detection and behavioral analysis:* Real-time anomaly detection uses a trained model to watch live data for anything unusual. Advanced behavioral analysis detects many greatly unusual activities, including instances of forbidden access or meaningful data exfiltration, by precisely profiling all users, all devices, or all network activities. This phase analytically focuses on minimizing false positives, guaranteeing that threats are detected rapidly to prevent or substantially reduce harm.
6) *Deployment & Integration with Security Systems:* The advanced anomaly detection system works with the organization's existing security tools, including firewalls, intrusion detection systems and SIEM platforms. Effective ransomware prediction models need to work with current cybersecurity systems because system reliability, scalability and proven real-world performance are important. Splunk, IBM QRadar and the ELK Stack are prime examples of strong SIEM platforms that comprehensively analyze security logs to effectively detect and pinpoint anomalies. CrowdStrike and Palo Alto Networks and other endpoint security solutions, use machine learning for real-time ransomware prevention. Ransomware threats are proactively prevented through the smooth integration of security frameworks[24].
7) *Continuous Monitoring & Model Updating:* Constant monitoring protects the system from new threats. The system updates and retrains itself thoroughly in response to new data, changing attack patterns and user behavior shifts. This study conducts many, thorough audits and thorough performance evaluations to recognize areas of improvement. Automated pipelines make model retraining and deployment more efficient, guaranteeing the system remains accurate and current. Ransomware is constantly evolving and machine learning models need continuous updates to detect new versions. This involves retraining models using updated threat intelligence data, integrating new attack patterns and improving feature selection. High-quality threat intelligence feeds reveal important ransomware signature discoveries, thereby enabling important model adaptation. Highly effective ransomware detection systems consistently remain effective against increasingly advanced cyber threats because of diligent continuous monitoring and frequent updates[4].
8) *Cyber Security Measures & Proactive Measures:* This section explains how to strengthen the anomaly detection system using strong cybersecurity measures. Proactive strategies are necessary for strong security. These include penetration testing, vulnerability assessments and user education. Strong authentication protocols, strong encryption, along with stringent access controls, can greatly reduce the probability of successful attacks[13]. Staying informed about emerging threats and using a thorough dynamic defense approach proactively maintain a secure environment.

V. VARIOUS MACHINE LEARNING APPROACHES FOR RANSOM ATTACKS

Machine learning is transforming how enterprises combat the insidious threat of ransomware. Sophisticated algorithms utilizing supervised classification, unsupervised clustering, and deep architectural autoencoders now facilitate against malicious encryption. These novel neural networks can identify deviations from routine data behaviors to pinpoint stealthy assaults in real-time, limiting losses.

A. *Supervised Learning Approaches*

1) *Decision Tree:* Decision Trees provide a simple way to categorize data in supervised learning, grouping it by key features to uncover trends often associated with ransomware. Advanced Cybersecurity Decision Trees can effectively learn to differentiate certain benign activities from certain malicious activities through the detailed analysis of past ransomware attacks. This learning process examines several changes in documents, process behavior and network traffic patterns. Security experts are still researching methods for identifying evolving attacks. Their methods also incorporate unstructured data. Organizations analyze considerably more thorough contextual signals and this substantially improves their algorithms' ransomware detection and prevention[5].
2) *Random Forest and XGBoost:* Random Forest and XGBoost are powerful machine learning methods that increase accuracy and help defend against ransomware through model combination. Random Forest effectively avoids overfitting and identifies many attack indicators, such as considerably anomalous file behavior and strikingly unusual network patterns, by averaging results from multiple Decision Trees and diverse data subsets[22]. XGBoost, a considerably gradient-increasing framework, iteratively refines its predictions by concentrating on multiple misclassified instances; this is analytically important for identifying subtle ransomware indicators. These methods use system logs, many file access patterns and all network traffic to build a strong model for early ransomware detection. These models enable proactive monitoring, which allows for early identification of potential ransomware incidents, thus minimizing the effect and spread of attacks.

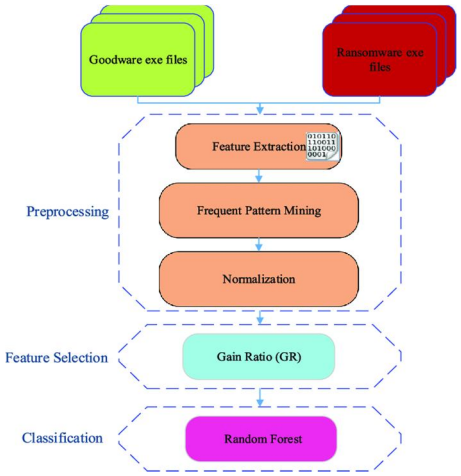


Fig. 2. Ransomware Detection using Random Forest

3) *Support Vector Machines:* Support Vector Machines (SVMs) are powerful machine learning tools adept at detecting ransomware attacks by efficiently separating normal system activity from malicious behavior within complex datasets. Using labeled datasets of normal system behavior and known attack patterns, trained SVMs prevent ransomware attacks through the precise classification of new observations. Because support vector machines effectively handle complex, nonlinear relationships with kernel functions, they are important for identifying evolving advanced ransomware techniques[14]. Support Vector Machines (SVMs) maximize the margin separating classes. This guarantees that even subtle deviations from normal behavior, such as irregular file access or unusual process activities, are flagged for subsequent, thorough investigation. SVMs possess high sensitivity. Therefore, many early detection systems requiring a rapid response use them. Support vector machines are thus an analytically important part of a multi-layered defense system and these machines offer exceptionally strong detection capabilities that powerfully prevent ransomware execution and propagation across a network.

B. Unsupervised Learning Approaches

1) *Isolation Forest & One class SVM (Anomaly Detection):* Isolation Forest and One-Class SVM are unsupervised anomaly detection algorithms that excel in identifying outliers in datasets, which is essential for spotting ransomware behavior that deviates from normal patterns. Isolation Forest works by randomly partitioning data and isolating anomalies faster than normal points, making it ideal for real-time monitoring of system logs, file activities, and network traffic[6]. Its ability to focus on irregularities without relying on labeled data means it can detect emerging ransomware techniques that may not have been seen before. Similarly, One-Class SVM is designed to learn the boundary of normal behavior from unlabelled data, flagging any data points that fall outside this boundary as potential threats. Both methods are effective in identifying subtle anomalies—such as sudden spikes in encryption activity or uncharacteristic network communications—that often precede ransomware outbreaks. By alerting security teams to these deviations, these unsupervised approaches facilitate rapid investigation and proactive mitigation of ransomware attacks.

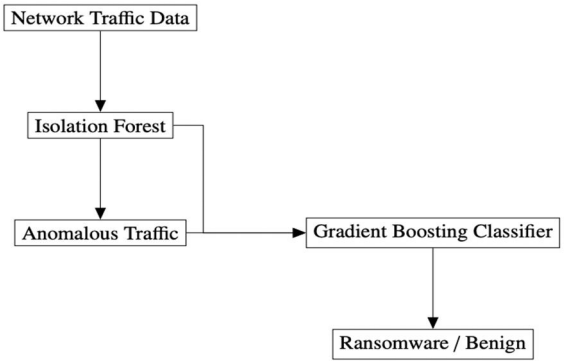


Fig. 3. Anomaly detection Architecture

2) *Autoencoders:* Autoencoders, a type of neural network for unsupervised learning, excel at ransomware detection by learning to compress and rebuild typical computer activity. By training on benign data, an autoencoder learns to recognize the usual structure and patterns found in network traffic, file access logs and system activities[21]. Meaningful ransomware attacks cause input to deviate substantially from the expected pattern. This deviation results in a greatly large reconstruction error clearly signaling a problem. Autoencoders offer real-time anomaly detection. This capability is important for continuously monitoring many cybersecurity systems. Highly effective autoencoders swiftly detect meaningful abnormal errors and this furnishes security teams with an important early warning system. Their deep learning approach helps them recognize complicated patterns, which is key for spotting advanced ransomware methods that can slip past regular detection systems. By quickly identifying unusual reconstruction errors, autoencoders act as an early alert system[7]. This allows security teams to take action, isolate the affected areas, and limit the spread of ransomware, ultimately lessening the damage caused.

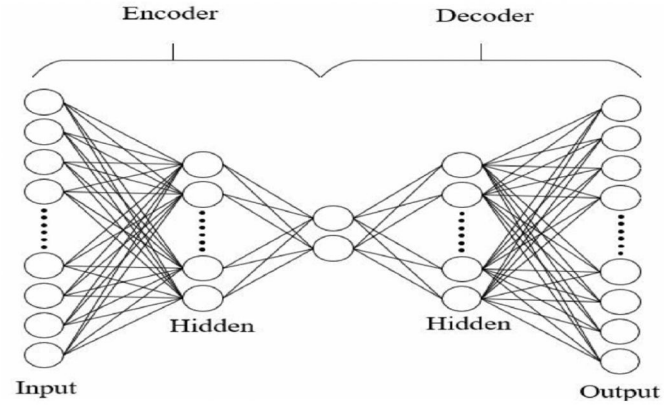


Fig. 4. Autoencoder Schematic depiction

VI. RESULTS

This research explores how well supervised and unsupervised machine learning can stop ransomware attacks. Decision Tree, Random Forest and XGBoost models used supervised learning. These models showed varying success using labeled datasets of normal and ransomware-infected file activity. Ensemble methods, such as Random Forest and XGBoost, usually performed better than a single Decision Tree, achieving greater accuracy and fewer false positives. Advanced ensemble methods successfully identified highly detailed patterns in file system activity, process execution and network communication; these patterns were strongly characteristic of ransomware. Support Vector Machines showed potential in differentiating between benign and malicious activity, particularly with optimized kernel functions[8]. Supervised approaches were complemented by several unsupervised learning techniques and these techniques detected anomalies indicative of ransomware attacks without requiring pre-labeled data. Isolation Forest detected unusual file access patterns and system calls, thereby identifying potentially malicious activity. Using normal file behavior for training, One-Class SVM effectively detected deviations from the created pattern, presenting its potential for identifying new ransomware variations. To advance the research, autoencoders developed multiple condensed representations of typical file activity[15]. Ransomware may have been the cause of anomalous behavior indicated by file activity reconstruction errors that differed from the expected pattern. Unsupervised methods effectively detected new ransomware, but generally required precise adjustments to minimize inaccurate results, as well as performed best when used with rule-based or signature-based systems for greater accuracy.

VII. CONCLUSION

In conclusion, our research explores how machine learning can help defend against ransomware attacks. It includes testing several special methods. These included supervised learning, where the computer is taught about what ransomware looks like and unsupervised learning, where the computer learns normal behavior and flags anomalies. Random Forest and XGBoost, highly effective supervised machine learning methods using multiple decision trees, proved considerably more effective at ransomware detection, owing to their demonstrably superior capacity to manage complex data compared to single decision trees. Support Vector Machines performed well, but were considerably slower. Isolation Forest, along with One-Class SVM, unsupervised methods, successfully detected several abnormal file access patterns, including those from novel ransomware. Autoencoders identified anomalies based on data that deviated from the learned pattern of normal behavior. While these unsupervised methods look promising, they can cause false alarms and are most effective when used with other security protocols.

Several supervised machine learning methods and also employed some unsupervised machine learning techniques were used. The ransomware defenses improved. Supervised methods successfully identify known ransomware, while unsupervised methods are better at detecting new and emerging threats. This approach provides considerably improved data protection, safeguarding all data from such attacks. Subsequent research attempts will considerably refine these techniques. This will greatly improve their accuracy and it will also improve their efficiency.

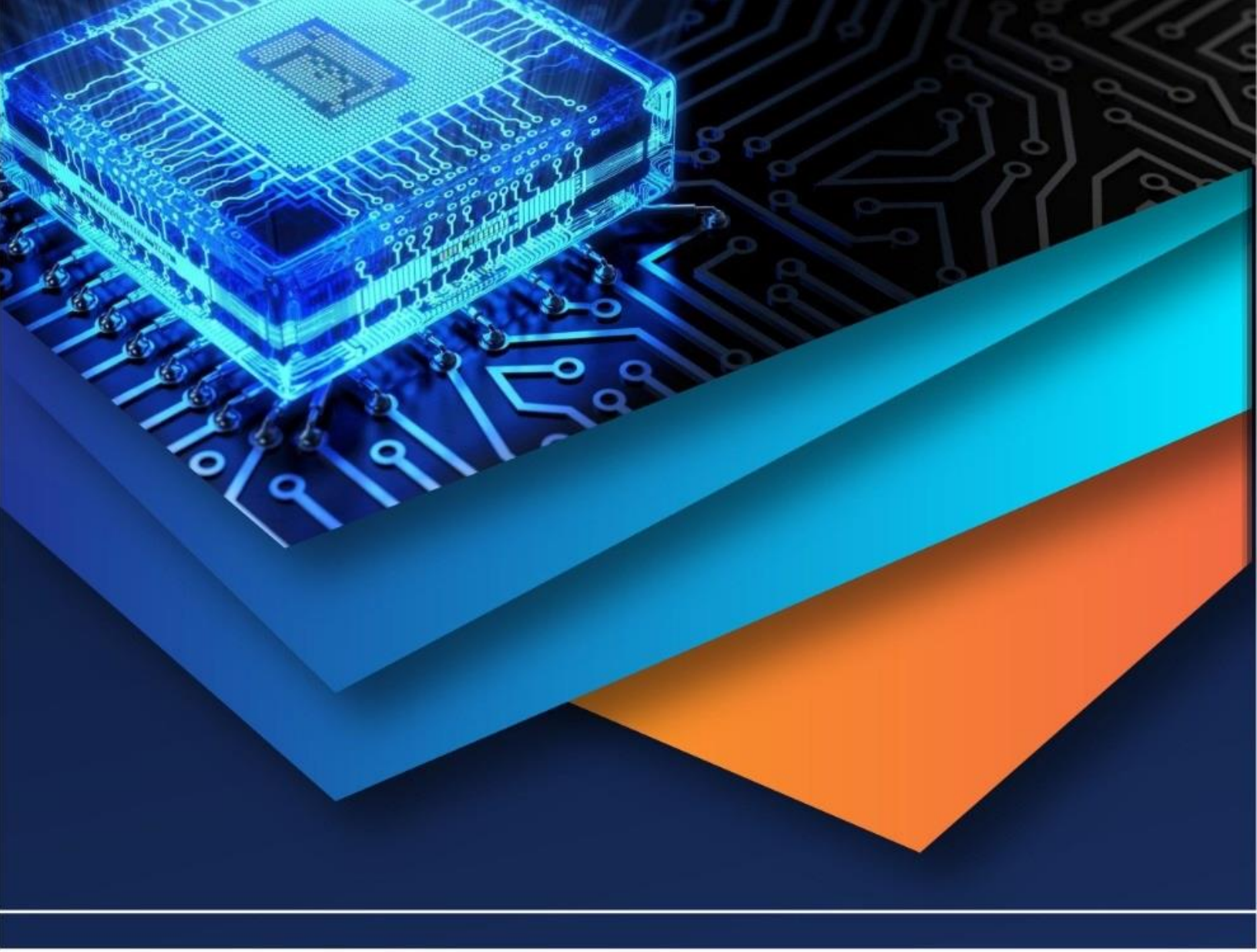
VIII. FUTURE SCOPE

This research on early ransomware detection with machine learning points to several promising avenues for future work. The combination of the strengths of several machine learning models, including supervised and unsupervised methods, is important for developing stronger and more accurate detection systems. Low-latency analysis of system activity is required for rapid detection and rapid detection is important for preventing common encryption. Effective ransomware countermeasures require many flexible learning systems that automatically change to several new ransomware variations and attack techniques. A thorough investigation of explainable AI (XAI) considerably improves transparency and trust in these systems, enabling security analysts to fully understand the reasons behind detections[25]. Furthermore, developing user-friendly tools and interfaces is necessary for common adoption, thereby enabling many organizations of all sizes to benefit from these advanced detection capabilities. Considerably increased cybersecurity collaboration and substantially improved data sharing can greatly accelerate the development and improvement of effective ransomware prevention strategies.

REFERENCES

[1] Popli N, Girdhar A. Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware. In Verma,Nishchal K, Ghosh, A. K. (eds) Computational Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80. Ransomware Attack: A Growing Havoc Cyberthreat. InData Management, Analytics and Innovation 2019 (pp. 403-420).
[2] Zimba A, Chishimba M. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. European Journal for Security Research. 2019 January;4(1):3-31.
[3] BBC-News 2019, Baltimore ransomware attack: NSA faces questions, BBC-News, viewed 28 December 2019, https://www.bbc.com/news/technology-48423954/
[4] Wikipedia 2019, Wikipedia, viewed 28 December 2019, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack/
[5] Goyal, P.; Kakkar, A.; Vinod, G. & Joseph, G. Crypto- Ransomware Detection Using Behavioral Analysis Reliability, Safety and Hazard Assessment for Risk-Based Technologies, Springer, 2020, 239-251.
[6] Grant L., Parkinson S. Identifying File Interaction Patterns in Ransomware Behavior. In: Parkinson S, Crampton A, Hill R. (eds) Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham. 2018;14:317-335.
[7] Kok SH, Abdullah A, Jhan Jhi NZ, Supramaniam M. Prevention of Crypto-Ransomware Using a Pre- Encryption Detection Algorithm. Computers.
[8] Caporusso N, Chea S, Abukhaled R. A game-theoretical model of ransomware. In: Proceedings - International Conference on Applied Human Factors and Ergonomics 2018 Jul 21 (pp. 69-78). Springer, Cham.
[9] Morgan, Steve. "Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics." Cybercrime Magazine Cisco and Cybersecurity Ventures. 2019, https://www.cybersecurityventures.com/cybersecurity.
[10] Maccari M, Polzonetti A, Sagratella M. Detection: Definition of New Model to Reveal Advanced Persistent Threat. InProceedings of the Future Technologies Conference 2018 Nov 15 (pp. 305-323). Springer, Cham.
[11] Al-rimy B, Maarof M, Shaid S. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers and Security.
[12] Celdrán, A.H.; Sánchez, P.M.S.; Castillo, M.A.; Bovet, G.; Pérez, G.M.; Stiller, B. Intelligent and behavioral-based detection of malware in IoT spectrum sensors. Int. J. Inf. Secur. 2022, 22, 541–561. [CrossRef]
[13] Chesti, I.A.; Humayun, M.; Sama, N.U.; Jhanjhi, N. Evolution, mitigation, and prevention of ransomware. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6.
[14] Philip, K.; Sakir, S.; Domhnall, C. Evolution of ransomware. IET Netw. 2018, 7, 321–327. Jegede, A.; Fadele, A.; Onoja, M.; Aimufua, G.; Mazadu, I.J. Trends and Future Directions in Automated Ransomware Detection. J. Comput. Soc. Inform. 2022, 1, 17–41. [CrossRef]
[15] Brewer, R. Ransomware attacks: Detection, prevention and cure. Netw. Secur. 2016, 2016, 5–9.
[16] E. Berrueta, D. Morato, E. Magaña, and M. Izal, "A survey on detection techniques for cryptographic ransomware," IEEE Access, vol. 7, pp. 144925– 144944, 2019.
[17] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid. Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions.
[18] R. S. Abujassar, M. Sayed, and H. Yaseen, "A new algorithm to enhance security against cyber threats for internet of things application," International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 4, pp. 4452–4466, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4452-4466.
[19] Y. Ayachi, Y. Mellah, M. Saber, N. Rahmoun, I. Kerrakchou, and T. Bouchentouf, "A survey and analysis of intrusion detection models based on information security and object technology-cloud intrusion dataset," IAES International Journal of Artificial Intelligence (IJ-AI), vol. 11, no. 4, pp. 1607–1614, Dec. 2022, doi: 10.11591/ijai.v11.i4.pp1607-1614.

[20] W. Liu, "Modeling ransomware spreading by a dynamic node-level method," IEEE Access, vol. 7, pp. 142224–142232, 2019, doi: 10.1109/ACCESS.2019.2941021.
[21] S. Adam, "The state of ransomware 2022," Sophos News, 2022. https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/ (accessed Nov. 25, 2023).
[22] U. Urooj, B. A. S. Al-rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, "Ransomware detection using the dynamic analysis and machine learning: A survey and research directions," Applied Sciences, vol. 12, no. 1, Dec. 2021, doi: 10.3390/app12010172.
[23] A. Wani and S. Revathi, "Ransomware protection in IoT using software defined networking," International Journal of Electrical and Computer Engineering (IJECE), vol. 10, no. 3, pp. 3166–3175, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3166-3175.
[24] M. Hassan, F. Abrar, and M. Hasan, An explainable AI-driven machine learning framework for cybersecurity anomaly detection. 1st Edition, Routledge, 2023.
[25] S. Mehnaz, A. Mudgerikar, and E. Bertino, "RWGuard: a real-time detection system Against cryptographic ransomware", in RAID 2018: Research in Attacks, Intrusions, and Defenses, 2018, pp.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY