NIET Journal of Engineering & Technology (NIETJET)

Volume **, Issue Winter / Summer YYYY **ISSN: 2229-5828 (Print)**

An Innovative Strategy for Efficiently Retrieving Data from Ransomware Attacks

Dr. Rashmi Sharma[1], Dr. Himani Garg[2], Dr. Chitvan Agrawal[3]

[1]Deptartment of CSE, Noida Institute of Engineering and Technology, Gr. Noida, India
[2]Deptartment of ECE, Ajay Kumar Garg Engineering College, India
[3]Department of CSE, Noida Institute of Engineering and Technology, Gr. Noida, India

Abstract *The frequency of ransomware attacks has surged, disrupting regular business operations and resulting in data theft and loss, which has raised significant concerns about brand reputation and information security. This study scrutinizes existing methodologies for recovering data post-ransomware attacks across diverse industries. It also presents an innovative framework aimed at securing critical data stored in servers through network segmentation, the utilization and deployment of a honeypot device for log collection, and machine learning-driven devices. The proposed network architecture targets early detection of ransomware attacks and automated response, reducing reliance on manual intervention. Validation of the framework is conducted using ransomware attack datasets, with machine learning algorithms compared for their efficacy in detecting attacks based on behavioural analysis of network traffic. Performance evaluation metrics measure the effectiveness of the deployed machine learning algorithms, revealing that the XGBoost technique surpasses others in early ransomware attack detection.*

Keywords - Ransomware attacks, Data Recovery, Honeypot, Network Segmentation, Support Vector Machine (SVM), Artificial Neural Network (ANN), XGBoost

1. Introduction

Ransomware, a form of malware, is utilized to seize and withhold victim information until a ransom is paid. This malicious software targets critical data, rendering files, directories, and other crucial information inaccessible. Ransomware is meant to proliferate across networks, generating substantial revenue, sometimes in the billions of dollars, for cybercriminals. This poses a significant threat to businesses, governmental bodies, and non-governmental organizations alike. Ransomware typically employs asymmetric encryption, where the attacker holds the private key, only releasing it to the victim upon payment of the ransom. Users data is essentially locked and inaccessible until the full ransom amount is paid, presenting a significant. This represents a major contemporary threat to businesses. In 2022, ransomware attacks accounted for a major portion of cyberattacks, emerging as the predominant form of cyber assault. Cybercrime has undergone significant transformation over time, leaving victims computer data and other critical assets vulnerable to ransomware attempts [1].

Ransomware attacks primarily require payment of ransom for access to private keys. Nowadays, such attacks are prevalent, emphasizing the need for businesses to implement robust backup and heightened safety measures to minimize the risk of data stealing and leakage. However, these attacks are pervasive and often take precedence in average attack detection, leaving organizations with limited time to address other threats and prevent potential impending attacks. Ransom payments have significantly increased, constituting a substantial portion of the overall cost associated with ransomware attacks.

1.1 Types of ransomware

The types of ransomware are encrypting ransomware, crypto-ransomware, locker ransomware and scareware. Encrypting ransomware and crypto-ransomware, both of which withhold user data until a ransom is paid. The

**Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.**

encryption key, necessary for decrypting the data and restoring access, is provided to the user only after the ransom is paid. The locker ransomware effectively bars the victim from accessing their device or system, denying access to all files, applications, and even the entire operating system. The victim regains access after paying the demanded ransom.

TABLE 1. Major Types of Ransomware

Type	Description	Impact
Encrypting Ransomware/ Crypto-Ransomware	Encrypts user data and withholds the decryption key until ransom is paid.	Data inaccessible until payment; risk of permanent data loss.
Locker Ransomware	Locks users out of their devices or systems, denying access to all files and applications.	Complete loss of device/system access; restored only after payment.
Scareware	Uses fake security alerts and warnings to mislead users into believing their system is at risk.	Coerces users into unnecessary payments; often does not encrypt data.
Mobile Ransomware	Specifically targets smartphones and tablets, often via malicious apps or phishing.	Device lockout or file encryption; ransom demand to restore access.
Leakware (Doxware)	Threatens to publicly release sensitive or confidential data unless ransom is paid.	Risk of data exposure, reputational and legal consequences.
Destructive Ransomware	Not only encrypts but also deletes or irreparably corrupts data and systems.	Permanent data loss, system inoperability, severe financial and reputational damage.

There may be serious repercussions, including significant financial loss and damage to the impacted firms' reputations. In addition to monetary gain, harmful ransomware attacks may be motivated by retaliation, sabotage, or ideological goals. These attacks are frequently quite complex, using cutting-edge methods to avoid detection and get past security measures.

Ransomware attacks present a severe threat to companies, potentially resulting in substantial financial losses and significant data breaches. Perpetrators often target data breaches as a primary objective in ransomware attacks. Consequently, companies suffer reputational damage, impacting their standing within industries and among stakeholders. Countless files suffer damage, with many being crucial to the company's reliability and operations. Attackers typically render these files inoperable, inaccessible, obscure, and impermissible. If the ransom demanded is not paid in full, these encrypted files become irretrievably lost, containing crucial data and mandatory credentials, making recovery impossible. Recovering data and essential information holds paramount significance as it constitutes the critical aspects and ultimate objectives of most ransomware strategies. Given the significant loss of crucial data in ransomware attacks, the implementation of these recovery methodologies is vital and indispensable. Companies often have dedicated security teams assigned to handle data retrieval and safeguarding crucial information. Once operations are reinstated and normalcy returns, the restoration of the system to its regular operations involves a combination of challenging and straightforward processes. Decryption and encryption represent crucial techniques employed in the recovery of encrypted files and data [3]. Real-time protection stands as a pivotal defence against all ransomware attacks targeting end hosts. This type of extortion-based attack underscores the effectiveness of endpoint defence in both preventing and recovering from its destructive and devastating impact [4].

1.2 Protection from ransomware

There are cybersecurity methods available to protect our data and sensitive information in a contained setting before it is integrated into a network and becomes unchangeable storage. IBM uses several recovery techniques to minimize data loss and improve a thorough defense against ransomware assaults. Often used as a cyber-resilient tactic, the IBM Cloud Cyber Recovery technique successfully removes ransomware attacks while providing useful and workable solutions. It is noteworthy as the best recovery approach selected to create a robust solution against ransomware, enabling the recovery of data in different IT settings and departments.

With the support of protective scanning tools, IBM's selected methodology offers a comprehensive approach that guarantees ongoing recovery and secure backups. This proactive strategy improves detection capabilities and more successfully thwarts ransomware and malware threats. With thorough tracking of all data, data security, and protection continue to be of utmost importance. This recovery architecture is used to ensure regulatory requirements and rules are followed in the case of any problems and the need to protect isolated data [5]. Point-in-time measures have been incorporated into recovery procedures with data gaps to provide coverage for cyber outages. Adding more virtual sandboxes is part of the plan to quickly protect all data in case of a ransomware attack. With dedicated access to safe, virtualized environments and fully managed services, the IBM cloud recovery solution has developed into a more advanced and exciting strategy. By employing methods developed by IBM, this crucial security solution improves efficacy and agility in combating ransomware attacks.

Software licensing that is largely focused on automated solutions is utilized by one or more solution architects. To thwart ransomware attacks, various techniques are employed, including the utilization of cybersecurity systems to manage regular incidents. Some companies implement incident response plans to ensure the effective execution of these measures, thus minimizing the risk of ransomware attacks. Numerous new strategies are accessible for implementation, collectively safeguarding organizations against such ransomware threats [6].

Evolutionary strategies like zero trust approaches are accessible to combat ransomware, disrupting current attack sequences and shielding companies from malware and cyber threats. Numerous recovery methods are employed by companies, with a focus on detecting and preventing ransomware attacks.

Key methods include early prevention measures and maintaining critical backups for swift deployment during emergencies, ensuring minimal disruption to normal operations and business continuity. Companies primarily employ isolation and containment techniques to manage such attacks, disconnecting all computers from affected networks. Increased scrutiny is applied to assess and validate all assets, spanning both front-end and back-end components, to promptly remove infected files. Failure to do so could result in widespread computer damage and ransomware-induced disruptions, particularly impacting extensive storage devices. Therefore, companies employ such attack protection methodologies to safeguard crucial data and important information from such threats.

2. Literature Review

Various mitigation strategies exist for preventing and addressing ransomware threats, including zero-day strategies designed to detect and counter cyber threats. These strategies aim to protect companies from financial losses and reputational damage caused by ransomware attacks. Cybersecurity teams play a pivotal role in simplifying the critical ransomware response, transforming it into a manageable challenge [7].

Amoeba, as the primary recovery and backup SSD, stands out for its superior performance and minimal overhead, making it a promising solution for ransomware defense. The timely removal of ransomware is crucial, as intelligent variants can inflict severe damage by compromising vital data [8].

Mitigation techniques play a pivotal role in recovering data, employing various data recovery tools, and addressing associated issues stemming from ransomware attacks [9].

A data recovery framework is being developed utilizing the Autopsy digital forensics platform to address various challenges and offer a robust defense against ransomware attacks. This innovative architecture serves as the primary framework for creating common data models, demonstrating the practicality of the Autopsy framework. Given that ransom payments do not always guarantee full data restoration, the implementation of data recovery procedures and protocols is imperative and mandatory[10].

Numerous software solutions are employed for the dissemination and implementation of mitigation strategies against ransomware threats. One prominent type of software is crypto virology software, designed primarily to disclose vital information to victims and restore access to files once the ransom is paid. This software encrypts all files, ensuring their protection until the ransom amount is fully settled [11].

Encryption is one of the most important techniques for data protection and guaranteeing its security, confidentiality, and integrity. With an emphasis on synchronizing data across memory and other subsystems, a cutting-edge data management solution is presently under development. The goal of this proof of concept is to incorporate encryption while minimizing the impact on other applications' performance. It is impossible to overestimate the significance of early prevention given the prevalence of ransomware assaults nowadays. Numerous preventative measures are in place, necessitating ongoing data monitoring and automation. Focusing on halting data exfiltration is an even more successful strategy for preventing ransomware. [12–16]

3. Proposed Framework for Data Recovery in Ransomware Attacks

To address the formidable challenges posed by ransomware attacks, our solution is designed to strengthen the development of effective countermeasures. This contributes to the broader mission of eliminating ransomware and protecting both data and businesses from its damaging effects. We have developed comprehensive, multifaceted strategies that provide robust protection and recovery options for organizations and individuals. Each component of our approach is crafted to deliver an interactive and practical method for mitigating ransomware’s impact, offering a range of techniques and solutions for its detection, removal, and prevention. [17-18]

3. 1 Key features of our holistic strategy include:

3.1.1. Layered Defense Architecture
Which integrates network segmentation, honeypot deployment, and continuous monitoring to limit ransomware spread and provide early detection.

3.1.2 Intelligent Anomaly Detection
It Utilizes advanced machine learning models to identify and respond to suspicious behaviour in real time, and minimizing the risk of data compromise.

3.1.3 Automated, Encrypted Backups
It ensures that critical data is regularly backed up, securely stored, and readily recoverable, even in the event of a sophisticated attack.

3.1.4 Interactive Recovery Protocols
It offers guided, user-friendly recovery processes that enable rapid restoration of operations and minimize downtime.

3.1.5 Comprehensive Countermeasures

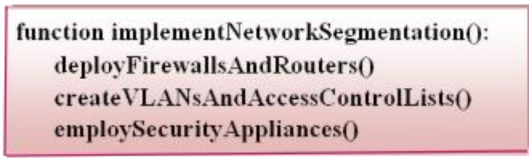
Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

Combines prevention, detection, and remediation techniques, including proactive threat intelligence and incident response planning.

This integrated approach not only mitigates the immediate effects of ransomware but also strengthens long-term resilience, empowering organizations and individuals to maintain business continuity and data security in the face of evolving cyber threats.

3.2 Network Segmentation

Network segmentation serves as a foundational strategy to prevent the lateral propagation of ransomware within organizational IT environments. By dividing the network into isolated zones, segmentation restricts unauthorized movement and access, thereby containing threats and safeguarding critical assets. This approach not only improves the efficacy of ransomware defense but also enhances the accessibility and manageability of network resources. This robust segmentation strategy incorporates strategic deployment of security appliances, implementation of routers and firewalls, access control lists (ACLs) and VLANs, continuous monitoring and automated response.



```
function implementNetworkSegmentation():
    deployFirewallsAndRouters()
    createVLANsAndAccessControlLists()
    employSecurityAppliances()
```

Fig. 1. Network segmentation facet of the proposed model

Figure 1 demonstrates the way to setup the routers and firewalls, along with the way to setup Virtual Local Area Networks and access control lists. Furthermore, strategic placement of security appliances reinforces the overall approach for safeguarding systems from ransomware attacks.

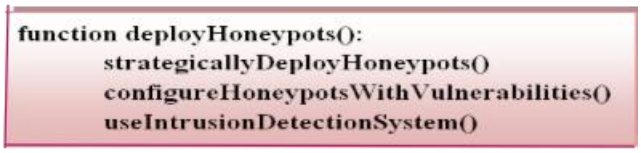
A modern, robust segmentation strategy incorporates the following key elements: Strategic Deployment of Security Appliances, Implementation of Routers and Firewalls, Access Control Lists (ACLs) and VLANs, Continuous Monitoring and Automated Response

3.3 Honeypot Deployment for Server Shielding

The installation of honeypots is an additional approach that follows network segmentation.The honeypots are placed at strategic locations over the entire network architecture. These kinds of honeypots configure and improve all systems, eliminating vulnerabilities via their potential impacts and services. Systems for intrusion detection are employed for enhancing the proposed technique while detecting the consequences of ransomware. By setting up necessary layers, these frameworks offer an additional versatile security towards hazards.

Intrusion detection systems (IDS) have been employed to facilitate this kind of approach to enhance the detection of ransomware activity. The technologies provide the network with a quicker reaction to the emerging risks due to the introduction of an extra safety barrier.

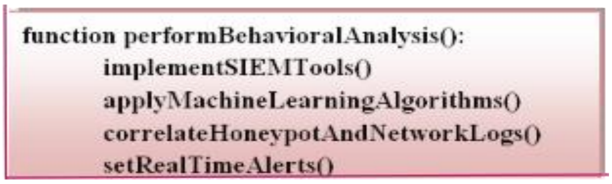
Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.



```
function deployHoneypots():
        strategicallyDeployHoneypots()
        configureHoneypotsWithVulnerabilities()
        useIntrusionDetectionSystem()
```

Fig. 2. strategic placement and configuration of honeypots

Figure 2 demonstrates the way to incorporate systems that detect intrusions and carefully place and set up honeypots.



```
function performBehavioralAnalysis():
        implementSIEMTools()
        applyMachineLearningAlgorithms()
        correlateHoneypotAndNetworkLogs()
        setRealTimeAlerts()
```

Fig. 3. Analysis of behaviour and anomaly detection with the honeypot logs facet of the proposed model

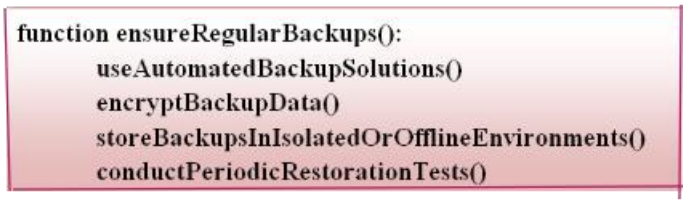
Figure 3 shows the process of behavioral analysis and the incorporation of specialized tools to the proposed model. These tools are well orchestrated to make use of machine learning algorithms to facilitate the correlation and interpretation of data acquired in honeypot logs. One of the prominent aspects of this arrangement is the timely provision of updates and notifications in real time because it highlights the essence of swiftness in terms of detection and preparation of threats that appear.

3.4 Regular Automated Backups

The next element of our strategy is focusing on utilizing automated backups that will be developed regularly to ensure the data is recoverable as time goes by. This does the following:

- Installing stable backup systems that carry out backup automatically to make sure the backups take place on a regular basis without having to do it manually.
- Backup data encryption to sustain confidentiality and avoid disclosure of sensitive data during ransomware activities.
- Regular and scheduled inspection of backup procedures to ascertain its consistency and performance to the effect that a data recovery is possible in case of organizational requirements.

This all-inclusive backup plan is vital in reducing downtime and losses of data in case of ransomware attack, which strengthens organizational resilience.



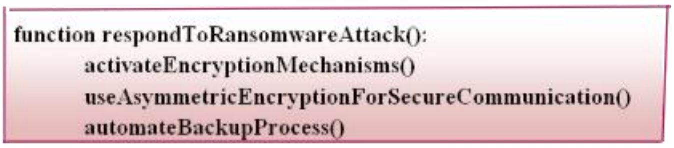
```
function ensureRegularBackups():
        useAutomatedBackupSolutions()
        encryptBackupData()
        storeBackupsInIsolatedOrOfflineEnvironments()
        conductPeriodicRestorationTests()
```

Fig. 4. The regular automated backup facet of the proposed model

Figure 4 outlines the process of regular updates and backups emphasizing on the encryption of the data and carrying out periodic restoration tests. Automatic backup solutions have been implemented to add more wholeheartedness to the strategy, which in the long run would make the backup process effective.

3.5 Encryption and Data Backup During an Attack

Lastly, encryption is very critical in this process, and this involves application of data backup and encryption techniques of converting data to ciphertext and vice versa when needed. Programmable encryption techniques are adopted to streamline implementation and enhance accessibility. These mechanisms protect critical data, effectively mitigating vulnerabilities to ransomware attacks. Secure communication is maintained across all channels and backup storage solutions. Additionally, asymmetric encryption methods are employed, along with supplementary safeguards, to ensure comprehensive data security.



```
function respondToRansomwareAttack():
        activateEncryptionMechanisms()
        useAsymmetricEncryptionForSecureCommunication()
        automateBackupProcess()
```

Fig. 5: Encryption and Data Backup During an Attack

Figure 5 depicts the encryption strategies implemented for generating backups in the midst of a ransomware attack, as well as the range of encryption methods applied to facilitate secure data recovery.

4. Results and Discussion

The methodology we used relies on 62,485 records of ransomware attacks with a dataset that permits using machine learning algorithms to aid the process of recovering information. The utilized algorithms are Artificial Neural Networks (ANN), Support Vector Machines (SVM) and XGBoost, which optimize data recovery of the ransomware and make the whole process efficient and reliable. The dataset is separated into training and test sets and the input and output data are utilized to train the model as well as test our model.

4.1 Accuracy

Accuracy is a quantitative index, and it represents the general functioning of every machine learning framework including ANN, SVM, and XGBoost, by calculating the number of accurate predictions in a test series of models. Figure 6 makes a comparative analysis between accuracy of Artificial Neural Networks (ANN), Support Vector Machines (SVM) and XGBoost using a proportion. They all are effective algorithms that bring important assessments and background to the table. The accuracy is measured on the basis of some parameters and they are graphically indicated in the figure.

.

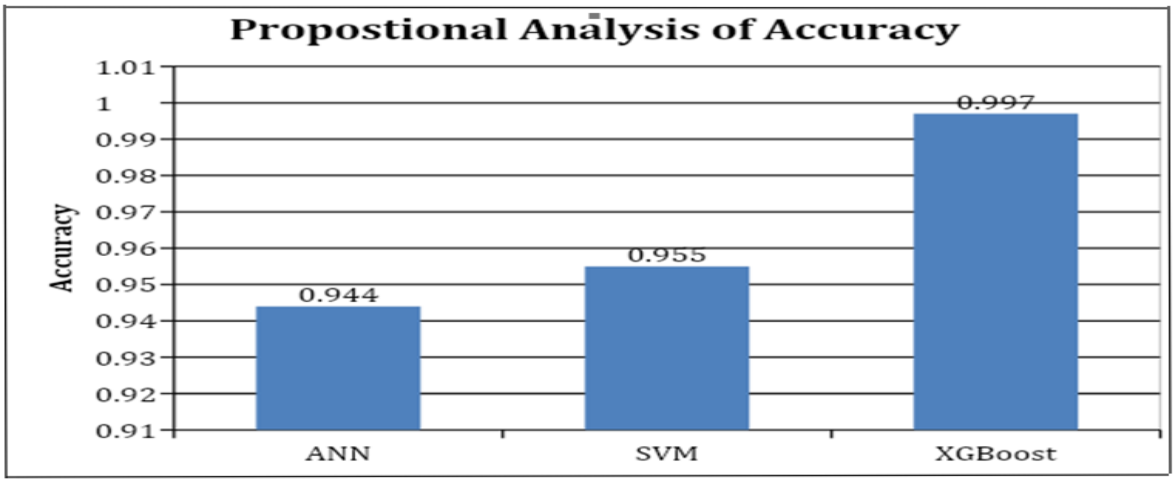


FIG. 6: COMPARATIVE ACCURACY ANALYSIS OF MACHINE LEARNING ALGORITHMS

4.2 Precision

The precision allows measuring how the model makes positive predictions, which is an essential measure indicating how effective a model is. It indicates the clarity by which the model discriminates between results that are pertinent, which makes it an important measure of performance. The precision of all the machine learning algorithms being considered has been illustrated in figure 7. This mark would contribute to more certain and stable analysis, and, accordingly, the level of credibility of the results would increase. XGBoost algorithm is also a highly accurate algorithm since it is the only algorithm performing better than ANN and SVM when it comes to accuracy. This great performance attracts the stability and reliability of the XGBoost, making this tool the safest and most accurate one in the context of the implementation of the functions related to the ransomware data recovery in the machine learning context.

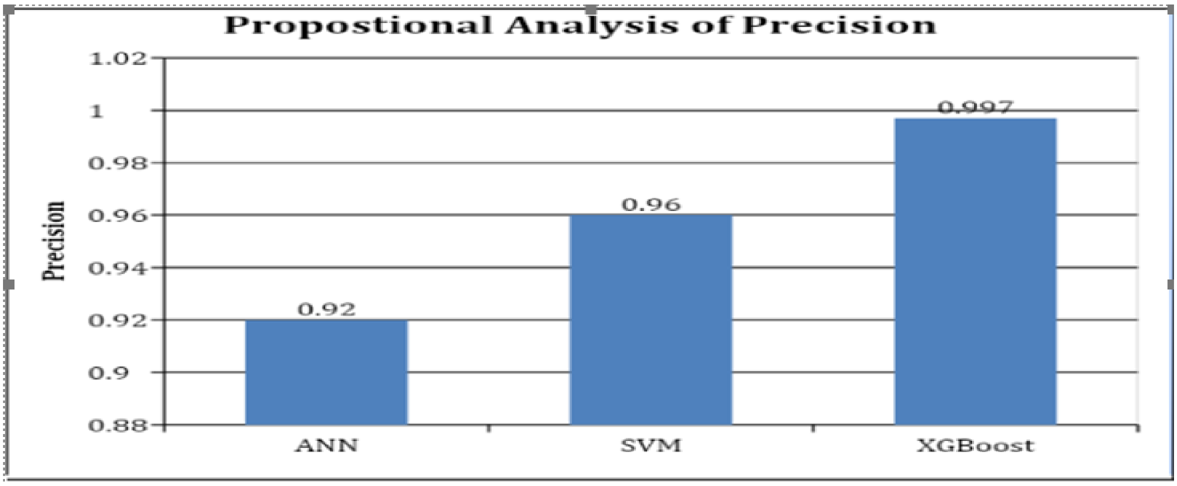


Fig. 7: Comparative Precision Analysis of Machine Learning Algorithms

4.3 F1 Score

F1 metric is a vital score in statistics as well as machine learning and provides an informative account of the

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

model performance. F1 score is a mixture of precision and positive predictive value that enables one to have a balanced view of the model's ability to generate positive results. The implication of such a measurement is that it is very helpful towards making the trade-off between false negative and false positive, and this adds more value and seriousness to the decision at hand.

As Figure 8 shows, the side-by-side comparison of each of the machine learning models (ANN, SVM, and XGBoost) is located. Through the discussion, it can be seen that it is relevant to consider accuracy and F1 score as a single measure to get an understanding of how the model works. It is important to mention that when compared, the XGBoost algorithm has a higher F1 score than the other statistical algorithms hence showing significance of this algorithm in addition to the fact that it can measure well in the various performance scores.

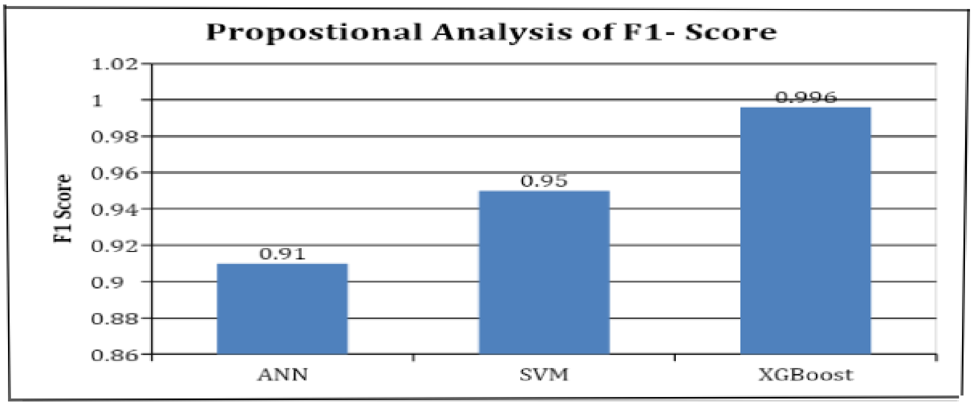


Figure 8. Proportional analysis of F1-score for Artificial neural network (ANN), support vector machine (SVM), and XGBoost.

4.4 Recall

Recall is an essential measure of examining the true positive of the rate of the classification models. It is a way of measuring how well a model is able to distinguish real positive cases probes into how well a model reflects the proportion of true positives to the total number of real positive cases. According to Figure 9, we get an extensive overview of the recall rates of machine learning models Artificial Neural Networks (ANN), Support Vector Machines (SVM), and XGBoost. Of these, the support vector machine is likely to exhibit a higher recall level, which means that they are more certain in predicting positive outcomes.

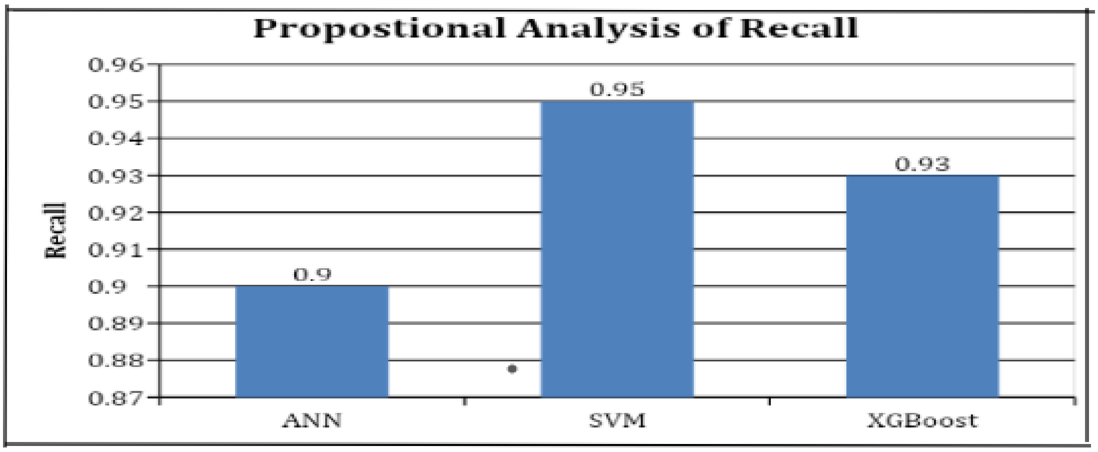


Fig. 9. Proportional analysis of recall for Artificial neural network (ANN), support vector machine (SVM), and XGBoost.

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.

CONCLUSION

Hackers usually use ransomware to infiltrate industries and institutions, locking important information and imposing massive losses of finances and reputation on businesses. This paper contains a new model of data recovery and this model combines segmentation of the network and safeguarding of data-sensitive information servers through honeypots. In addition, the improved machine learning techniques also allow ransomware defense attacks to be anticipated early to deploy countermeasures as models are trained on honeypot logs. The ransomware set is an essential element in the restoration process of the data in the ransomware recovery machine. As cases of ransomware attacks crop up every now and then, their main agenda is to cause serious interference with the usual running of businesses, which sometimes even leads to a loss of much-needed credentials and documentation. It is an urgent necessity to discuss securing our data against ransomware attacks. This study is attempting to illuminate the machine learning paradigms adopted to identify and reduce risks of ransomware adoption in the future.

REFERENCES

[1] P. O’Kane, S. Sezer, and D. Carlin, Evolution of ransomware, *Iet Networks, vol. 7, no. 5, pp. 321–327, 2018.*

[2] 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, *Comput Secur, vol. 74, pp. 144–166, 2018.*

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in *Computer Security–ESORICS 2009: 14th European Symposium on Research in Computer Security, Saint- Malo, France, September 21-23, 2009. Proceedings 14*, 2009, pp. 355–370.

[4] Kharraz, A. and Kirda, E. Redemption: Real-Time Protection against Ransomware at End-Hosts. In: Dacier, M., Bailey, M., Polychronakis, M. and Antonakakis, M., Eds., *Research in Attacks, Intrusions, and Defenses. RAID 2017. Lecture Notes in Computer Science,* Vol. 10453, Springer, Cham, 98-119.

[5] A. A. Somwanshi and S. A. Joshi, Implementation of honeypots for server security, *International Research Journal of Engineering and Technology (IRJET), vol. 3, no. 03, pp. 285–288, 2016.*

[6] Navdeep S. Chahal, Preeti Bali, Praveen Kumar Khosla, A Proactive Approach to assess web application security through the integration of security tools in a Security Orchestration Platform, *Computers & Security, Volume 122, 2022, 102886, ISSN 0167-4048,*

[7] A. Fagioli, Zero-day recovery: the key to mitigating the ransomware threat,*Computer Fraud & Security, vol. 2019, no. 1, pp. 6–9, 2019.*

[8] D. Min *et al.*, Amoeba: An autonomous backup and recovery SSD for ransomware attack defense, *IEEE Computer Architecture Letters, vol. 17, no. 2, pp. 245–248, 2018.*

[9] R. D’Arco, R. Pizzolante, A. Castiglione, and F. Palmieri, On the file recovery in systems infected by Ransomware, *Advances in Intelligent Systems and Computing, 2020, pp. 1412–1425.*

[10] S. C. Nayak, V. Tiwari and B. K. Samanthula, Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform, 2023 *IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, NV, USA, 2023, pp. 0605-0611.

[11] I. Sarwar, L. A. Maghrabi, K. Nisar, and I. Khan, Crypto virology Ransomware: A Review of Dissemination and Mitigation Techniques, *Inf. Sci.* Lett, vol. 12, no. 11, pp. 2277– 2288, 2023.

[12] K. Takeuchi, H. Fujima, T. Kumamoto, and Y. Yoshida, RansomCillin: Leveraging NTFS Spare Space to Recover from Ransomware Attacks, *Authorea Preprints*, 2023.

[13] A. A. Elkhail *et al.*, Seamlessly Safeguarding Data Against Ransomware Attacks, IEEE *Trans Dependable Secure Comput, vol. 20, no. 1, pp. 1–16, 2023.*

[14] I. Sharma and K. R. Ramkumar, Routing Methods for Wireless Networks Using MIMO Support: A Survey and Future Scope, in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2020, pp. 469–473.

[15] I. Sharma and K. R. Ramkumar, Analysis of MANET Payload Delivery Behaviour with Parallel Routing through MIMO, in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1–4.*

[16] M. Mundt and H. Baier, Threat-based simulation of data exfiltration toward mitigating multiple ransomware extortions, *Digital Threats: Research and Practice, vol. 4, no. 4, pp. 1–23, 2023.*

[17] L. Albshaier, S. Almarri, M.M.H. Rahman, Earlier Decision on Detection of Ransomware Identification: *A Comprehensive Systematic Literature Review. Information 2024, 15, 484.*

[18] Ojo, A. Olasunkanmi, Ransomware trends and mitigation strategies: A comprehensive review, *Global Journal of Engineering and Technology Advances, 2025, 22(03), 009-016*

Publisher: Noida Institute of Engineering & Technology,
19, Knowledge Park-II, Institutional Area, Greater Noida (UP), India.