International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Deep Learning Techniques for Ransomware Detection and Prevention

Kevin William Peoples

Abstract: ***Ransomware attacks are threatening to both corporate and personal data significantly. The computer users face privacy violation and verification issues, reputation damage, and financial losses posed by successful assaults. Hence, it is important to identify and prevent ransomware attacks smoothly and accurately. Previous studies have proposed various approaches to detect ransomware, with their pros and cons. The core objective of this study is discussing existing ransomware attacks and deep learning methods to prevent those assaults. Hence, this study covers types of ransomwares, assault timeline, and deep learning methods. It also offers comprehensive research on existing approaches to detect, prevent, recover from, and reduce ransomware attacks. This study is based on systematic analysis of previous studies conducted from 2000 to 2024 to provide up-to-date knowledge to readers about the most recent advancements in terms of ransomware detection and highlights advanced approaches to combat those attacks. To conclude, this study underscores possible research concerns and challenges in terms of ransomware detection and prevention.***

Keywords: ransomware detection, deep learning methods, ransomware attacks, assault timeline, privacy violation

1. Introduction

With the upsurge in ransomware cases, 72.7% organizations had faced those attacks by 2023 (Petrosyan, 2025). They acted as eye opener for cybersecurity experts worldwide to be watchful and come up with strategies for early mitigation. Ransomware is a malware evolving constantly with core aim to encrypt the files on digital devices to render them for future goals. A trojan malware, AIDS came to limelight in 1989 with the early reporting of the attack (Al-Rimy et al, 2018). Smart threat vectors have caused recent advances in ransomware attacks with transfiguration having various dimensions (Reshmi, 2021; Ye et al, 2017).

Ransomware developers use advanced techniques with complex techniques to obscure the actual intent. Modern anti-malware tools can find it challenging to scan, prevent, and detect them. With the rise of zero-day attacks, it has been challenging to detect the encrypted attacks at early stage. Using indiscernible approaches like bitcoin, cryptocurrencies, and anonymity leveraged by P2P vendors while accepting payments without any fear poses another issue of making it shatterproof (Cen et al, 2024). Ransomware is still an active cybersecurity threat emerging with its consequences.

There has been a significant rise in "Ransomware-as-a-Service (RaaS) over the years. With this model, anyone can launch attacks with ransomware, even without having technical knowledge. RaaS platforms are emerging as an option to choose the type of malware. There is even customer support available for people should they find any problem in launching attacks. It has led to a rise in variety and number of attacks, making cybersecurity a headache (Hope, 2024). The variant using the RaaS platform shows a reversal of policy in modern business models. This way, novice or non-technical attacks can attack easily. It further complicates the process of preventing those attacks (Meland et al, 2020). The ransomware malware poses irreversible damage as a serious threat vector to victim's data and leaves a grave dent to organization's reputation (Kok et al, 2022).

In addition, applications used in conducting those attacks are so smart that they can easily befool the victims and they fall prey. The irrecoverable damage has been done already before even they realize. It is vital to appeal prevention and early detection tools and make defense mechanisms to recover the damage with least risks while retaining the backup remotely at secured location to avoid significant financial losses because of ransomware (McIntosh et al, 2021). Table 1 lists some of the major ransomware attacks conducted in recent years (Cyber Management Alliance, 2024).

Table 1: Serious Ransomware Attacks happened by 2023

Targets	Damage
T-Mobile	API used in January 2023 to breach data of 37 million users and SSNs, account pins, etc. were used in March 2023
Acer	IntelBroker stole 160 GB of documents like software tools, technical manuals, and backend data
Intel	A "Money message extortion gang" stole 1.5 TB of data like source code, firmware, and databases followed by MSI breach and demanded ransom of $4 million
AT&T	Customer proprietary network was used to breach data of 9 million customers
Microsoft	Data breach of 30 million accounts by "Hacktivist Anonymous Sudan" and sold for $50,000
Toyota financial services	Financial and private data was stolen and leaked on dark web
Nickelodeon	Over 500 GB data was stolen and leaked
National British Library	Over 573 GB of employee data was published by Rhysida ransomware group on dark web

Source – Cyber Management Alliance (2024)

Cybersecurity is significantly affected by the rising threat of ransomware, which consists of metamorphism and polymorphism. The emergence of RaaS is a significant contributing factor, making smart attacks accessible to even novice users. So, robust detection techniques are needed to counter modern antimalware programs which cannot identify complex changes in ransomware. This study discusses different deep learning techniques to detect ransomware. It is based on real-time response and detection by combining deep learning and existing cybersecurity models. It aims to determine the efficiency of deep learning approaches in

ransomware detection, dive deeper into integrating them with existing security mechanisms, and future research directions to improve the resilience and scalability of ransomware detection solutions. Figure 1 illustrates the process used to conduct ransomware attacks with four stages – target, initialization, encryption, and ransomware.

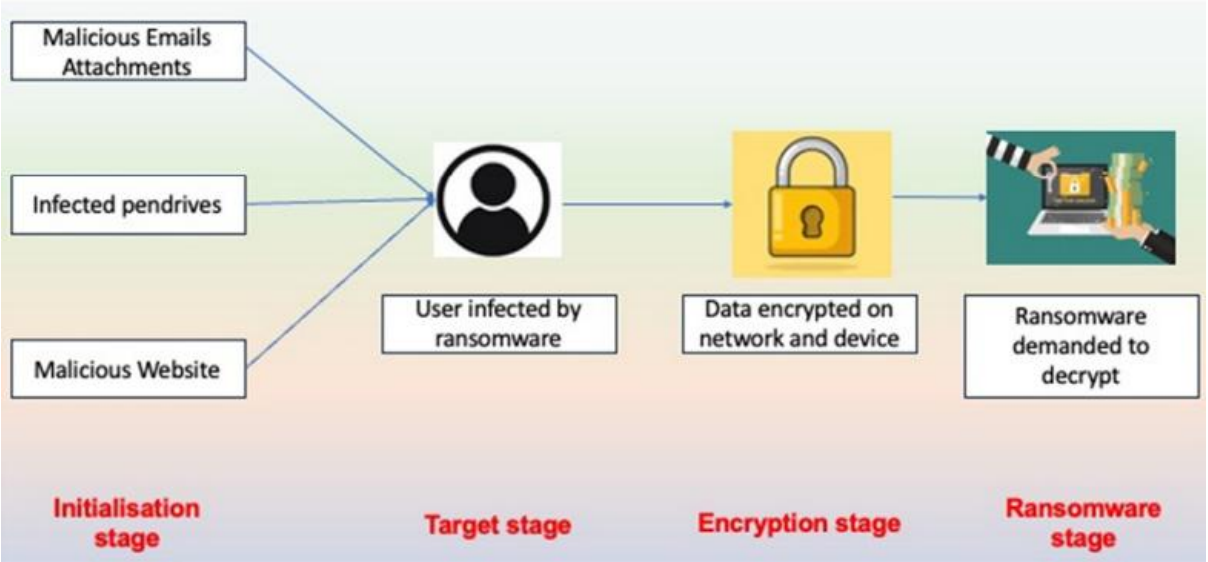

Figure 1: Stages of Ransomware Attack
Source: Kritika (2024)

Initialization consists of approaches used for sending malicious emails with malware as attachments, malicious websites, and infected pen drives. Target stage involves attacking gullible users by tricking them to download malicious files or putting infected drives and tricking them to visit malicious pages. Encryption stage involves availing confidential data of users on the network and encrypting devices with different methods to block their usage for victims. Finally, attackers demand heavy ransom to unlock files for those users or deny the accessibility of data until full payment is made. If organization denies the amount, the attackers may sell the data on dark web (Kritika, 2024).

The rapid propagation of attacks has been among the significant threats for organizations. Ransomware has been a very common tool for extortion from victims by cybercriminals with encryption of data and demanding ransom for an unlock code. The effect of ransomware has been observed across finance and healthcare to education and government. It is worth understanding the nature of attacks, the way they spread, and possible effects of falling victim to one due to high stakes covered (Celdrán, 2023). It is not possible to overstate the significance of research.

With increasing threats of attacks growing constantly, it is very important to dig deeper into the problem for practitioners to identify effective strategies for mitigation. This study aims to provide complete insight of threat landscape, investigate the factors contributing to the rise of ransomware, and explore potential research avenues. This study highlights this critical issue to help organizations and people to prevent ransomware attacks and reduce the possible damage due to these programs.

2. Literature Review

With increasing cases of data breaches and financial losses in different sectors, ransomware has become a widespread threat over the years. Ransomware has become a malware which encrypts files of victims and demands a ransom for decryption key. As a serious concern for practitioners and academics in cybersecurity, there is a need to detect and mitigate ransomware attacks. Deep learning approaches have shown increasing outcomes in classifying and identifying ransomware as they can draw complex categories and identification due to their potential to draw intricate characteristics and patterns from large datasets. Traditional ML methods like decision trees and support vector machines were employed most widely for malware detection in the beginning of 2000s (Idika and Mathur, 2007). With the availability of big and most popular datasets in deep learning, researchers started to focus on malware detection with deep learning approaches.

Saxe and Berlin (2015) proposed a deep neural network framework to detect malware with binary program from files that can be executed. The framework was 92% accurate on 10 ransomware families. However, there are some limitations of the study, such as, dependence on static analysis, limited dataset, and less interpretability, making it challenging to understand certain patterns or features resulting in ransomware detection. Limitations of the study underscore the need for more in-depth malware detection approaches.

Tobiyama et al. (2016) proposed a deep learning model for detecting malware, such as, ransomware, on the basis of static analysis. A stacked auto-encoder is used in the model for extracting features and they are classified with softmax classifier. The study has shown the potential for DL approaches for detecting malware but didn't focus majorly on detecting ransomware.

Akhter et al (2017). Investigated the use of deep neural networks for ransomware detection by analyzing network traffic. Their approach covered training of deep neural network on features of network traffic gathered from packet

payloads and headers. The study has focused on challenges to obtain datasets labeled for traffic and significance of feature engineering for detecting them properly.

There has been an increasing shift for analyzing behaviors in identifying ransomware. New approaches don't focus majorly on different signatures devoted to polymorphic malware to avoid the same and track activity of the users. It is known as intrusion for detecting some alterations. For example, a behavioral detection system has been proposed to identify ransomware with machine learning and user interaction in real-time. This approach has been helpful to reduce cases of false positives and newer strains are isolated which should be recorded in database (Wang and Zhang, 2024).

Another convincing achievement is implementing blockchain for security and authenticity of data in decentralized systems. Blockchain has enabled researchers to discover its use in building logs that are tamper-proof to capture movements of ransomware and real-time changes and effective approach for analyzing and responding to incidents (Doe et al, 2024). Along with identifying ransomware, this approach is also helpful in validating and restoring data to reduce inoperability of the system.

Ransomware is quite a vast phenomenon and there are new stimuli changing the vectors for protection and research. Occurrence of ransomware is one of the significant concerns in the evolution of attacks. It includes double extortion strategies. Along with encoding the information of the victim, it also steals victim's data and threatens victim to publish their private data to media for not paying the ransom. Ransomware attacks have been more serious and people may pay the ransom to avoid revealing data (Jones et al, 2024).

3. Types of Ransomware attacking Victims' Computers

Computers or information systems are encrypted by ransomware to keep authorized users from accessing the same. Ransomware attacks use techniques, processes and tactics to encrypt data or lock computers from PCs of victims and network systems. Commercial systems (with software and data), PCs, and industrial control solutions are possible targets for attacks from ransomware. In addition, there are different sensors used by Internet of Things (IoT) (Celdrán et al, 2023). A ransomware attack encrypts data with private key to keep authorized users from access of data or system unless they pay cash in Bitcoin (Chesti et al, 2020).

Ransomware operations may cover techniques for data exfiltration. Hackers steal private data from susceptible networks and threaten to release the same if ransom is not paid by the victim. The infection is dispersed with email attachments, malicious ads, and connections to rogue portals. The attacker sends files or documents with guidelines to pay the ransom. Decryption key is provided once payment is verified by the attacker (Philip et al, 2018). Extensions are widely included in files with ransomware or encryption infections, such as, Micro, Vault, Locky, Cryptolocker, TTTT, Encrypted, ZZZ, XYZ, and Petya. Extension of each file suggests ransomware type which has affected the same. Some of the common ransomware types are WannaCry.F, WannaCry, TorrentLocker, Fusob, CryptoTear, CryptoWall, and Reveton (Jegede et al, 2022). Figure 2 classifies ransomware into locker ransomware, crypto-ransomware, and scareware (Chesti et al, 2020; Jegede et al, 2022).

Figure 2: Classification of Ransomware types
Source: Chesti et al (2020); Jegede et al (2022)

3.1 Crypto Ransomware

It is the most prevalent ransomware targeting computer networks and systems. It encrypts data and files with asymmetric and symmetric encryption models. Even after removing malicious program from compromised storage or infected system, it is transferred to another system. The encrypted data is rendered by crypto-ransomware and becomes unusable. As malware doesn't corrupt imported data frequently, the victim can still use infected system to pay the ransom (Jegede et al, 2022)". Figure 3 illustrates crypto-ransomware which has been widely prevalent (Jegede et al, 2022).

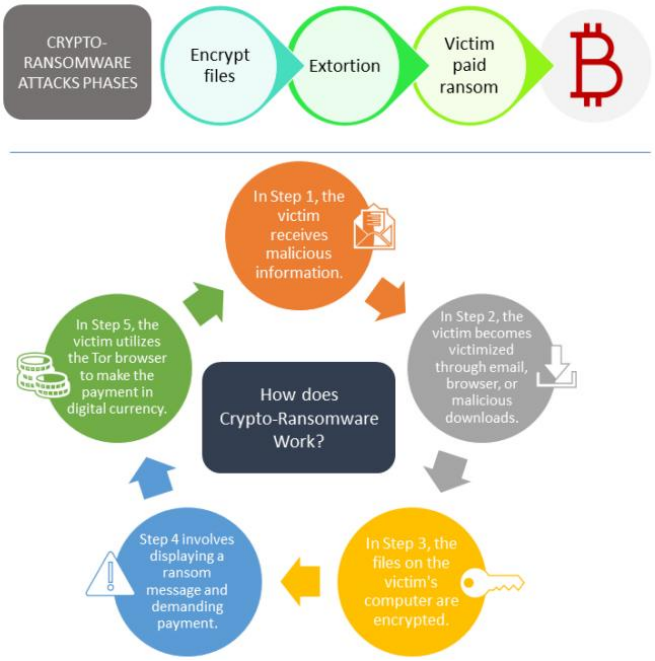

Figure 3: An illustration of crypto ransomware
Source: Jegede et al (2022)

3.2 Locker Ransomware

As the name suggests, locker ransomware simply locks a computer or other systems for money and preventing users from accessing it. The locker ransomware attacks the workstation, without rendering the saved data. After eliminating the malicious program, data remains unaffected. The infected storage device can be connected to another system to recover the data. Locker ransomware may not be used by people who want to extort money. Figure 4 illustrates a form of malicious program, locker ransomware which has been very prevalent (Jegede et al, 2022).

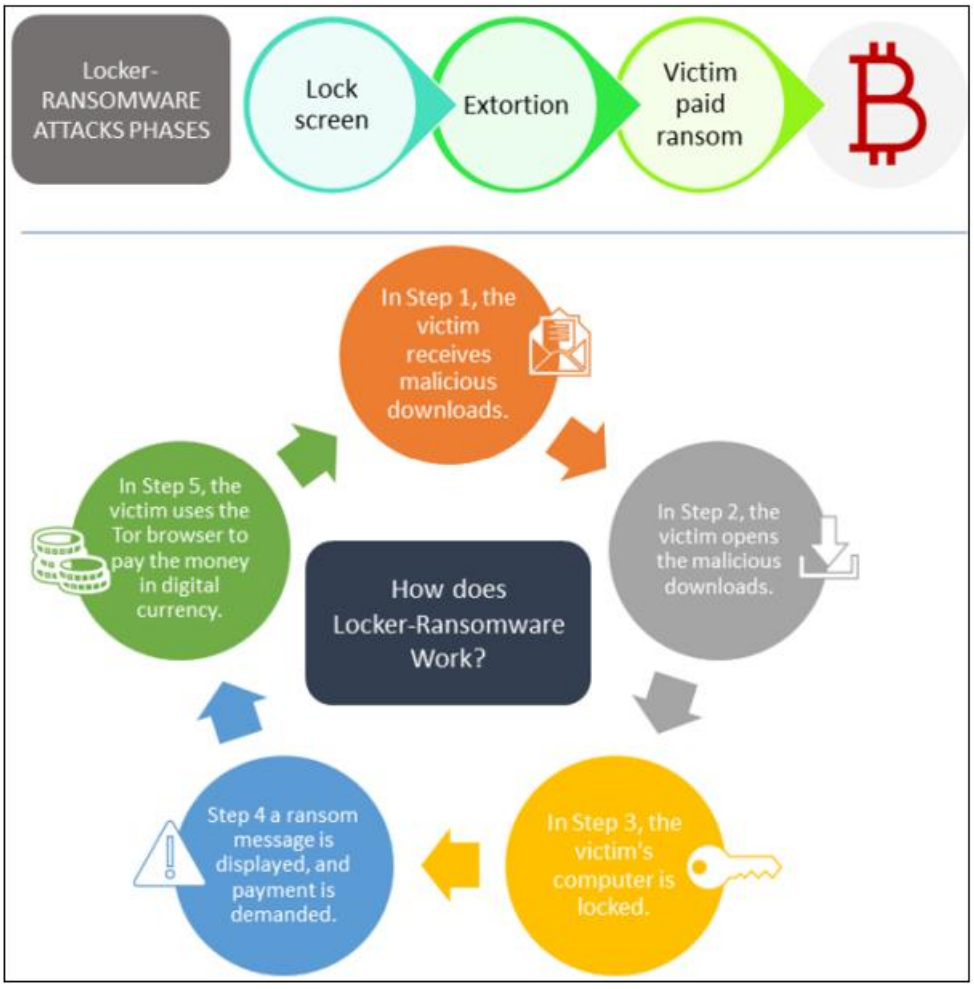

Figure 4: An illustration of Locker Ransomware
Source: Jegede et al (2022)

3.3 Scareware

This kind of malware preys on victim's computer by scaring them of being hijacked and promising to remove the malware with a fake anti-malware app which is made by the attacker himself. It lured several innocent users to download and install that fake program because of frequent pop-ups of alerts (Brewer, 2016). Manual ransomware and malware without data are different. Cybercriminals also use manual ransomware to break into cloud or network infrastructure, launch attacks on sensitive personal information, and conduct privilege escalation. Instead of just one program, entire organization is targeted. Usually, attackers access the entire IT system, exploit flaws, and move laterally through poor security configurations. In the same way, unauthorized access to credentials of privileged users causes assaults on IT programs enabling major corporate functions (Philip et al, 2018; Jegede et al, 2022). Figure 5 illustrates a form of malicious program being widely prevalent in cyberattacks, i.e., scareware (Jegede et al, 2022).

Figure 5: An illustration of scareware ransomware
Source: Jegede et al (2018)

Without files, ransomware uses a trusted and native machine for attacks. It is not easy to detect the attack as no code should be placed on the machine used by the victim for working. Hence, anti-ransomware approaches don't find doubtful files to trace in case of attack. As per the intentions of an attacker, human-based and file-based ransomware can leak, lock, or encrypt data (Chesti et al, 2020). Ransomware is a threat to files and technology. Compromised devices or files are locked until the ransom is paid. Even after paying the ransom, hackers usually withhold the decryption key if they want. They constantly attempt to use the key by the attacker to decrypt the information, which affects the stored files in the system.

Technological advances like RaaS, bitcoins, and ransomware development kits are the causes behind recent upsurge in attacks on networks, desktops, and even mobile devices (Chesti et al, 2020). Ransomware attacks cost hundreds of millions every year to individuals and businesses (Philip et al, 2018). New kinds of malwares are widely generated with ample cash benefits that are gained by hackers from assaults. A lot of variants of ransomware have been appeared since 2013. Hence, effective, new and reliable techniques are required to prevent, mitigate, and detect ransomware incidents.

Various strains of ransomware attacks cannot be generated with traditional antivirus program or other systems for intrusion detection. Companies and people face a lot of financial losses because of attacks. The encryption of data or computer system may cause permanent loss of data, which severely affect businesses and people at the same time. Even after paying the ransom, there is no guarantee that decryption key will be available. It poses further damage to the stored files in the system when attackers decrypt the files (Brewer, 2016).

4. Deep Learning Techniques for Ransomware Detection and Prevention

A lot of deep learning approaches are used to classify and detect ransomware. Studies have observed high accuracy rates from 81% to 99.8% in tests. These approaches are found to be helpful to combat the risk of ransomware. Deep learning models like "Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), Deep Belief Networks (DBNs), and Long Short-Term Memory (LSTM) networks have been promising in categorizing and detecting ransomware. These models can extract complex features and patterns from data, making them ideal for evolving and dynamic attacks (Kritika, 2024).

Combining various techniques like transfer learning, ensemble, and feature engineering have largely been discovered in hybrid models. For example, "Convolutional Autoencoder (CAE) and deep feature extraction spaces" are used by "CSPE-R framework", while dynamic and static features are used by "SwiftR framework" with LSTM and "Hierarchical Neural Network (HNN)" (Karbab et al, 2023; Zahoora et al, 2022). Various studies have addressed challenges related to ransomware detection, including lack of concept drift, labelled data, and evasion approaches like metamorphism and polymorphism. Techniques like "spline interpolation and Generative Adversarial Networks (GANs)" have been proposed to manage missing values and generate synthetic data (Urooj et al, 2023; Singh et al, 2023).

Application of deep learning and machine learning approaches has been explored in different areas like "Supervisory Control and Data Acquisition (SCADA) systems, Internet of Things (IoT), and network traffic analysis" (Alohali et al, 2023; Basnet et al, 2021; Li et al, 2020). Several deep learning techniques have been proposed in previous studies like ResNet, VGG16, and GoogLeNet to extract core features to represent the characteristics of ransomware (He et al, 2016; Simonyan and Zisserman, 2014; Szegedy et al., 2015).

When comparing the efficiency of deep learning models, F1 score, precision, accuracy, and recall are some of the important parameters. For quick and early detection, it is important to shorten time for detection and training. Some of the cons of approaches for ransomware detection are that it depends majorly on quality of features, existence of data overlap between benign and ransomware program, and challenge in generalizing to new versions. There is limited effectiveness against new attackers or complex attacks as they depend on already existing features and quality of core features (Cen et al, 2024). Table 2 lists deep learning techniques along with their outcome and limitations.

Table 2: Deep Learning Techniques used for ransomware detection

Framework	Outcome	Limitations	References
SwiftR	It employs dynamic and static features with LSTM and HNN, achieving F1 scores of 94%, 96%, and 98%.	Limited accessibility because of black box model for decision system.	Karbab et al (2023)
XRAN	It combines XAI and CNN models, LIME and SHAP with API calls to detect malicious activities with "True Positive Rate (TPR)" of 99.4%	Depends upon typical signature-based systems that cannot detect new ransomware and ignores models that are hard to comprehend for humans	Gulmez et al (2024)
Survey	Early detection approaches for attacks, explaining their types, evolution and comparison of current methods	Lack of proper data available for free, making ransomware detection a challenging affair	Cen et al (2024)
GAN	The proposed model performed better with 97% accuracy and 0.0088 false alarms with wGAN to generate synthetic data.	Lack of data available during the phase of pre-encryption related to ransomware attacks. Evasion approaches like metamorphism and polymorphism can defeat current solutions.	Urooj et al (2023)
CSPE-R	Uses deep feature extraction and CAE-based models to prevent zero-day attacks	Limited to certain ransomware family	Zahoora et al (2022)
SINN-RD	The "Spline Interpolation envisioned Neural Network-based Ransomware Detection Scheme (SINN-RD)" performed better than current schemes with 99% accuracy and security techniques.		Singh et al (2023)
SNN	Entropy features are used from binary files of ransomware and VGG-16 pre-trained network for meta-learning to find out similarity across images and similarity scores are generated while attaining 86% of F1-score	Imbalanced dataset with some classes with lack of relatable information	Zhu et al (2022)
LSTM, ANN	99.8% accuracy to detect malicious URLs with 405,836 records in dataset having a new feature using "https://www."	No comparison with other models	Alsaidi et al (2022)
CNN, LSTM, DNN, SCADA	DDoS attacks based on ransomware change SOC profile. DNN is the best choice against FDI attacks for minimal computational time with SCADA. LSTM is used for least variance and max CNN and AUC are used for high accuracy.	Various models are used for every feature. Best fit model is missing for all cases of selecting feature	Basnet et al (2021)
Deepware	It uses hardware performance and deep learning for ransomware detection, achieving recall score of 98.6% and average MCC score of 96.8% with 100ms snapshot. It is capable to detect unexpected families of ransomware like Ryuk, CoronaVirus, Dharma, and zero-day attacks	High-end storage and computational overhead and OC-SVM and RATAFIA source code and training data are not available	Ganfure et al (2022)

DRDT	Ransomware can be detected with TextCNN model. Trained with API, DRDT performs better than traditional approaches with F1 score of 0.959	Traditional approaches take a lot of time and can cause loss of sentence because of "max-over-time pooling"	Qin et al (2020)
GAN	Capable to deceive systems for ransomware detection while considering concept drift and longevity in training models.	Risks posed to heuristic models	Fernando et al (2020)
ARI-LSTM	The Attended Recent Inputs (ARI) are used to exploit repeat patterns in ransomware with 93% of accuracy with least false positive	Limited to Windows	Agrawal et al (2019)
DNN-BN, CAE, VAE	Hybrid feature engineering is performed with the use of VAE and CAE, while DNN-BN offers excellent generalization potential to improve decision engine's performance to detect dynamic ransomware behaviour	Used only in single host machine	Al-Hawawreh and Sitnikova (2019)
LSTM	Deep learning model is used by LSTM to detect ransomware with 97% accuracy in Android	Lack of comparable findings	Bibi et al (2019)

4.1 Ransomware Detection Methods

Manual and automated are two of the most common methods for ransomware detection. Automated methods include technologies to report and detect ransomware attacks. Usually, these tools can stop attacks. For manual detection, techniques mainly focus on scanning devices and data regularly for signs of attacks. There is a need to look at any changes to extensions when finding out if malware attack has not stopped authorized users or modified data from the access to their files or devices, accessibility of files or devices by verified users, and changes to extensions. Figure 6 illustrates the flow of techniques used for ransomware detection.

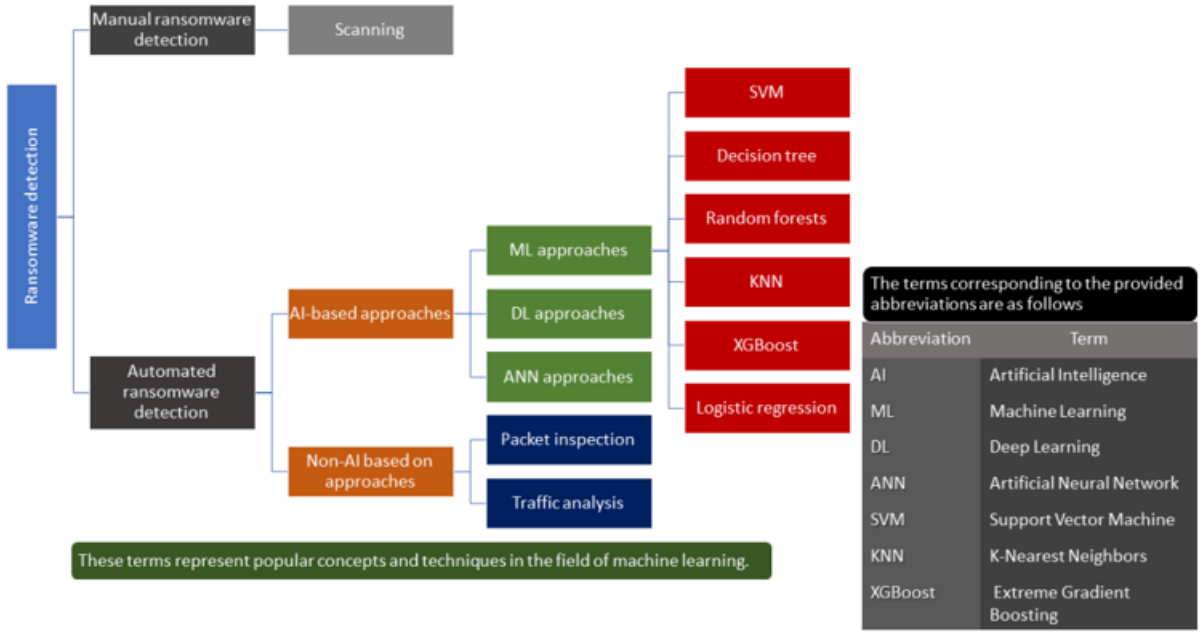

Figure 6: A taxonomy of ransomware detection techniques
Source: Alraizza and Algarni (2023)

4.1.1. Manual Detection

It refers to ransomware detection with human intervention and analysis instead of automated programs. It consists of analysis of network traffic, system logs, and other signs of compromise to detect behaviors and patterns related to ransomware attacks. While manual detection takes a lot of resources and time, it can complement automated approaches for detection, as it can detect unknown or new kinds of ransomware, which may not be observed by automated solutions (Aslan and Samet, 2020). There are some limitations related to manual ransomware detection, irrespective of its efficiency. It needs trained experts and can be labor-intensive to analyze network traffic and system logs. In addition, manual detection may not be scalable in large networks or companies where automated detection works even better (Aslan and Samet, 2020).

Scanning in manual detection is used with manual analysis of systems and files to detect malware. It consists of scanning systems or files for signs of activity like unusual traffic and encrypted files. Manual scanning can be used for automated scanning as it can detect unknown or new ransomware types which remain undetected by automated solutions (Aslan and Samet, 2020). There are some limitations with manual scanning. It takes effort and time when it comes to scan large systems or networks. In addition, false positives may be generated by manual scanning, which disrupts normal operations (Aslan and Samet, 2020).

4.1.2. Automated Detection

When it comes to ransomware detection, current approaches majorly consist of tracking the system at the level of file system. There are two major groups of automated ransomware detection approaches, i.e., based on AI and ones

not based on AI. AI-based approaches usually adopt deep learning and machine learning methods and artificial neural network techniques for ransomware detection. Some tools use variety of techniques or hybrid model combining multiple approaches to deal with the threat of those attacks.

Non-AI approaches depend on traffic analysis and packet inspection for ransomware detection. One of the major benefits of automated methods is that they can block, detect, and recover from attacks without human involvement. In addition, these tools are highly reliable and accurate in preventing, detecting, and recovering from those attacks (Akhtar and Feng, 2022).

AI-based approaches

AI techniques like deep learning, machine learning, and artificial neural networks have been widely used for detecting ransomware automatically. These techniques consist of using behavioral approaches like dynamic and static analysis to prevent and detect attacks. ML models can learn from previous attacks and detect new variations by tracking behaviors and patterns. Meanwhile, DL models can use neural networks for attack detection with analysis of big data. ANN can also identify ransomware by analyzing and processing various sources of data. These AI models provide more reliable and efficient way for preventing and detecting ransomware attacks, minimizing possible effect on people and businesses (Akhtar and Feng, 2022). Here are some of the AI-based approaches –

- **ML models** – ML-based ransomware detection is more advanced model depending upon training ML model for detecting ransomware on the basis of behavioral features or patterns. This approach relies on collection of big datasets of malicious and benign samples, training ML model and extracting relevant features to classify new samples as hostile or peaceful on the basis of their traits (Yamany et al, 2022a; 2022b). There are several benefits of malware detection based on ML, such as ability to detect unknown or new variants of ransomware without matching current patterns or signatures and to adapt to changing behavior of ransomware over time. This approach is less likely to face false positives as compared to heuristic- and signature-based detection. It detects actual patterns instead of static signatures. However, ML based detection is limited by its dependence on representative and large dataset of samples and it is also vulnerable to adversarial attacks which can manipulate the behavior or features of ransomware (Akhtar and Feng, 2022).

ML models for detecting ransomware – ML enables computers to improve performance on a specific role without being taught. Malicious malware encrypts files of the victims and demands ransom for the key. ML models are needed to stop and detect those attacks because of their rising severity and prevalence. Table 3 lists ML models which are used. Decision trees, SVM, K-nearest neighbors, random forests, logistics regression and XGBoost are some of the ML models used for ransomware detection. Each approach has pros and cons (Celdrán et al, 2023; Bello et al, 2021).

Table 3: ML models used for ransomware detection

ML Models	Characteristics	References
Random Forest	Ensemble methods are used with tree predictors to guarantee same distribution in the forest and it also relies on values of random vector. It can forecast and select the type of input data	Khammas, 2020; Ullah et al, 2020
Decision Tree	It can be trained on features like network traffic, modifications of file, and system to differentiate between benign software and ransomware behavior. Then, the decision tree can be used to detect malware.	Khammas, 2020; Ullah et al, 2020
Support Vector Machine (SVM)	They can be trained when data are high-dimensional	Ghouti and Imam, 2020; Arunkumar and Kumar, 2023
XGBoost	This robust ML model has gained a lot of popularity. It combines various decision trees to improve model accuracy. It is known for speed, scalability, and ability to manage complex datasets.	Saadat et al (2020)
K-nearest neighbor	K-NN is a strong ML model used in different fields of research. This non-parametric approach is useful for both regression and classification roles.	Mezquita et al, 2021; Selamat and Ali, 2019
Logistic Regression	LR is another common algorithm used in different fields. This linear model is useful for binary classification roles.	Noorbehbahani et al (2019)

- **DL Models** – DL models have been proposed to address the challenges of traditional tools for ransomware detection to improve the reliability and accuracy. These models use automated feature generation and best suited to manage unstructured datasets. They need no or minimal human intervention. They can effectively classify text, audio, and image data to detect image-based and textual ransomware data. However, a lot of data is needed to train deep learning models. So, they are not suitable for general applications, especially when there are small data sizes or datasets. High processing power is needed for deep learning to adapt with real-world datasets (Sharmeen et al, 2020).
- **Artificial Neural Network** – ANN models are best used for detecting several variants and types of ransomwares, such as, image and text variants, because of their different uses. Neural networks are best choice to adapt to new data and identify zero-day attacks due to their potential to learn consistently. Neural networks are highly versatile to detect various kinds of ransomwares and adapting to emerging threats. These approaches rely on hardware and are more vulnerable to dependencies, along with black box nature, which affects the ability of analysts to detect deviations and track data processing (Bello et al, 2021; Swami et al, 2021).

Non-AI based Approaches

Non-AI techniques like traffic analysis and pocket inspection can be used for ransomware detection. Anomaly detection is an effective model for ransomware detection. These models

track patterns and network traffic deviating from usual behavior. Unusual traffic patterns like sudden rise in encryption activity or plenty of outbound connections to suspicious IP are signs of ransomware attack. Network traffic can be compared to a baseline of behavior. Security teams can be identified instantly with anomaly-detection models to potential attacks (Chesti et al, 2020).

Othe non-AI approaches consist of signature-based malware detection, which consists of comparison of network traffic to common signatures and behavioral detection, which searches for behavioral patterns consistent with known attacks (Chesti et al, 2020). Another approach consists of using honeypots for tracking network activity and detecting ransomware. This method covers observing any anomalies and honeypot folder which may be the sign of ransomware. Ransomware detection is important to mitigate its effect and avoiding future damage (Chesti et al, 2020). It is worth noting that these techniques are not efficient and they must be used with other measures like regular backup, user education, and patches (Chesti et al, 2020).

To detect and prevent ransomware, an example of non-AI approach is antivirus software. Usually, it combines behavior-based and signature-based detection to block and identify malicious program. Signature-based detection consists of comparison of files over a database of popular malware signatures, while behavioral detection seeks malware activity. While antivirus program can detect and prevent attacks, there are some limitations. For instance, signature-based detection only works against popular signatures. It means unknown or new forms of malware can bypass antivirus program. In addition, some kinds of malwares can evade approaches on the basis of behavior (Wang et al, 2008).

- **Packet Inspection** – Packet inspection consists of determining contents of data packets as they pass through the network. This technique can detect malware by detecting packets having suspicious information or having inconsistent traits not matching normal traffic. For instance, packets with big data related to encryption or sent from suspicious addresses may suggest ransomware attack (Yang and Liu, 2019; Pimenta Rodrigues et al, 2017).
- **Traffic Analysis** – It consists of testing network traffic patterns over a certain time period. This technique can detect ransomware by tracking behavioral patterns which are common in ransomware attacks. For instance, sudden rise in traffic may be revealed in traffic analysis during off-peak hours or a lot of outbound connections to vulnerable IP addresses.

Traffic analysis and packet inspection are two of the major techniques that can detect malware. They cover examining network traffic to identify data patterns and packets of behavior which may be possibly harmful. By identifying patterns and network traffic suggesting malicious acts, these approaches can be helpful for organizations to protect their critical systems and data and detect ransomware attacks (Song et al, 2020; Cascarano et al, 2011)". They should also be adopted with security patches and backups.

4.1.3 Types of Ransomware Detection Approaches

Ransomware detection is a very important part of cybersecurity and several techniques have been emerged for detecting those attacks. This section explores several techniques for ransomware detection proposed earlier –

- **Signature-based Detection** – It is a traditional approach when it comes to identify some of the common patterns or signatures in the malware behavior or code. This approach relies on making database of known marks or signatures of ransomware and scanning the network or system to match patterns or signatures. The Ransomware is flagged as malicious once match is found and ideal actions are taken (Yamany, 2022a; 2022b). The effectiveness and simplicity to detect known variants of ransomware is one benefit of this type of detection. However, this approach cannot detect unknown or new variants of ransomware which don't match current patterns or signatures. In addition, attackers can easily modify ransomware behavior or code to evade signature-based detection (Akhtar and Feng, 2022).
- **Heuristic Detection** – Heuristic detection is more modern approach identifying anomalies or behavioral patterns which indicate malicious act. This approach creates heuristics or rules describing typical behavior and tracking the network or system for any anomalies or deviations from such rules. Once those anomalies or changes are found, the ransomware is flagged as malicious or suspicious and right actions are taken (Yamany, 2022a; 2022b). One of the benefits of this type of detection is that it can detect unknown or new variants not matching familiar patterns or signatures. In addition, this approach is not much prone to false positives as it depends majorly on detecting actual patterns. However, this type of detection depends on specified heuristics or rules, which may capture only some possible anomalies or behavioral patterns. In addition, attackers can evade detection based on heuristics by changing the ransomware behavior to prevent detection (Akhtar and Feng, 2022).
- **Network Detection** – With this approach, network traffic is monitored for malicious or suspicious activity which may indicate ransomware attack. This approach relies on tracking network traffic for patterns or anomalies which define ransomware, including huge volumes of unusual connections, outbound traffic, or encryption of network traffic (Yamany, 2022a; 2022b). One of the benefits of network detection is that it can detect ransomware even if system has not been infected yet or if the ransomware is relying on different encryption approaches. In addition, it is less vulnerable to false positives than other approaches as it detects actual patterns instead of specified rules or static code signatures. However, network-based detection depends upon tools used for analyzing network traffic which may not detect all activities. In addition, attackers can easily encrypt their traffic or with stealthy channels for communication (Akhtar and Feng, 2022).
- **Hybrid detection** – This approach combines various techniques for ransomware detection to improve overall speed and accuracy. It combines the strengths of heuristic, signature, ML, and network-based detection to create more effective and robust detection mechanism (Yamany, 2022a; 2022b). It can overcome the issues of individual approaches and improves overall speed and accuracy in detection. In addition, this method is less prone to false

negatives or positives. However, it needs resources and is very complex. It needs to coordinate and integrate with other detection tools (Akhtar and Feng, 2022).

5. Conclusion

Ransomware attacks have led to a huge damage to data and computer systems, causing unauthorized disclosure, destruction and access to sensitive and private data. Such attacks have resulted in significant reputational or financial losses for both businesses and people. Several approaches have been recommended to detect ransomware reliably, instantly, and accurately. This study provides timeline of ransomware attacks and discusses the context of deep learning techniques to detect ransomware. This study offers updated knowledge of automated approaches for ransomware detection. This knowledge will help readers to stay updated on latest advances in automated prevention, mitigation, and detection of ransomware. In addition, this study explores future research directions, highlighting potential research problems and open issues for the researchers.

Future studies could develop more accurate and robust machine learning models for ransomware detection to prevent a lot of variants and attack techniques. It can be achieved with modern techniques like ensemble and deep learning. Real-time ransomware-detection techniques must adopt real-time capabilities to prevent and identify attacks.

References

[1] Hope, A. (2024). Ransomware Trends and Predictions for 2024. CPO Magazine. Available at https://www.cpomagazine.com/cyber-security/ransomware-trends-and-predictions-for-2024
[2] Petrosyan, A. (2025). Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2025. Statista. Available at https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate
[3] 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.
[4] Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. International Journal of Information Management Data Insights, 1(2), 100013.
[5] Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. ACM Computing Surveys (CSUR), 50(3), 1-40.
[6] Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. Computer Networks, 239, 110138.
[7] Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers & Security, 92, 101762.
[8] Kok, S. H., Abdullah, A., & Jhanjhi, N. Z. (2022). Early detection of crypto-ransomware using pre-encryption detection algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5), 1984-1999.
[9] Cyber Management Alliance (2024). Biggest Cyber Attacks 2023, Top Data Breaches & Ransomware Attacks. Available at https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-2023-top-data-breaches-ransomware-attacks
[10] McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. ACM Computing Surveys (CSUR), 54(9), 1-36.
[11] Kritika, E. (2024). A comprehensive literature review on ransomware detection using deep learning. Cyber Security and Applications, 3, 100078.
[12] Celdrán, A. H., Sánchez, P. M. S., Castillo, M. A., Bovet, G., Pérez, G. M., & Stiller, B. (2023). Intelligent and behavioral-based detection of malware in IoT spectrum sensors. International Journal of Information Security, 22(3), 541-561.
[13] Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. Purdue University, 48(2), 32-46.
[14] Saxe, J., & Berlin, K. (2015, October). Deep neural network based malware detection using two dimensional binary program features. In 2015 10th international conference on malicious and unwanted software (MALWARE) (pp. 11-20). IEEE.
[15] Tobiyama, S., Yamaguchi, Y., Shimada, H., Ikuse, T., & Yagi, T. (2016, June). Malware detection with deep neural network using process behavior. In 2016 IEEE 40th annual computer software and applications conference (COMPSAC) (Vol. 2, pp. 577-582). IEEE.
[16] Akhter, M.N., Hamid, M.R. and Rahman, M.S. (2017). Ransomware detection using deep learning. International Conference on Networking, Systems and Security (NSysS), IEEE, pp. 1-5.
[17] Wang, H. and Zhang, Y. (2024). Real-time behavioral-based ransomware detection system. J. Comput. Virol. Hack. Techniques, 15(4), pp. 321-335.
[18] Doe, J., Smith, A. and Lee, C. (2024). Blockchain-based solutions for ransomware detection and response in decentralized environments. J. Cybersecur., 12(1), pp. 45-59.
[19] Jones, B., Smith, A. and Lee, C. (2024). Hybrid models for ransomware detection: a comparative study, Cybersecurity Adv., 8(3), pp. 102-117.
[20] Celdrán, A. H., Sánchez, P. M. S., Castillo, M. A., Bovet, G., Pérez, G. M., & Stiller, B. (2023). Intelligent and behavioral-based detection of malware in IoT spectrum sensors. International Journal of Information Security, 22(3), 541-561.
[21] Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020, October). Evolution, mitigation, and prevention of ransomware. In 2020 2nd International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
[22] Philip, K., Sakir, S., & Domhnall, C. (2018). Evolution of ransomware. IET Netw, 7(5), 321-327.
[23] Jegede, A., Fadele, A., Onoja, M., Aimufua, G., & Mazadu, I. J. (2022). Trends and future directions in automated ransomware detection. J. Comput. Soc. Inform, 1(2), 17-41.
[24] Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network security, 2016(9), 5-9.

[25] Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y. U., Jauro, F., Khan, A., ... & Abdulhamid, S. I. M. (2021). Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8699-8717.
[26] Gulmez, S., Kakisim, A. G., & Sogukpinar, I. (2024). XRan: Explainable deep learning-based ransomware detection using dynamic analysis. Computers & Security, 139, 103703.
[27] Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. Computer Networks, 239, 110138.
[28] Karbab, E. B., Debbabi, M., & Derhab, A. (2023). SwiftR: Cross-platform ransomware fingerprinting using hierarchical neural networks on hybrid features. Expert Systems with Applications, 225, 120017.
[29] Urooj, U., Al-Rimy, B. A. S., Zainal, A. B., Saeed, F., Abdelmaboud, A., & Nagmeldin, W. (2023). Addressing behavioral drift in ransomware early detection through weighted generative adversarial networks. Ieee Access, 12, 3910-3925.
[30] Singh, J., Sharma, K., Wazid, M., & Das, A. K. (2023). SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme. Computers and Electrical Engineering, 106, 108601.
[31] Zahoora, U., Khan, A., Rajarajan, M., Khan, S. H., Asam, M., & Jamal, T. (2022). Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier. Scientific reports, 12(1), 15647.
[32] Zhu, J., Jang-Jaccard, J., Singh, A., Welch, I., Al-Sahaf, H., & Camtepe, S. (2022). A few-shot meta-learning based siamese neural network using entropy features for ransomware classification. Computers & Security, 117, 102691.
[33] Alsaidi, R. A., Yafooz, W. M., Alolofi, H., Taufiq-Hail, G. A. M., Emara, A. H. M., & Abdel-Wahab, A. (2022). Ransomware detection using machine and deep learning approaches. International Journal of Advanced Computer Science and Applications, 13(11).
[34] Ganfure, G. O., Wu, C. F., Chang, Y. H., & Shih, W. K. (2022). Deepware: Imaging performance counters with deep learning to detect ransomware. IEEE Transactions on Computers, 72(3), 600-613.
[35] Qin, B., Wang, Y., & Ma, C. (2020, June). API call based ransomware dynamic detection approach using textCNN. In 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) (pp. 162-166). IEEE.
[36] Fernando, D. W., Komninos, N., & Chen, T. (2020). A study on the evolution of ransomware detection using machine learning and deep learning techniques. IoT, 1(2), 551-604.
[37] Agrawal, R., Stokes, J. W., Selvaraj, K., & Marinescu, M. (2019, May). Attention in recurrent neural networks for ransomware detection. In ICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP) (pp. 3222-3226). IEEE.
[38] Al-Hawawreh, M., & Sitnikova, E. (2019, November). Leveraging deep learning models for ransomware detection in the industrial internet of things environment. In 2019 military communications and information systems conference (MilCIS) (pp. 1-6). IEEE.
[39] Bibi, I., Akhunzada, A., Malik, J., Ahmed, G., & Raza, M. (2019, August). An effective Android ransomware detection through multi-factor feature filtration and recurrent neural network. In 2019 UK/China Emerging Technologies (UCET) (pp. 1-4). IEEE.
[40] Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. Big Data and Cognitive Computing, 7(3), 143.
[41] Alohali, M. A., Elsadig, M., Al-Wesabi, F. N., Al Duhayyim, M., Hilal, A. M., & Motwakel, A. (2023). Optimal Deep Learning Based Ransomware Detection and Classification in the Internet of Things Environment. Computer Systems Science & Engineering, 46(3).
[42] Basnet, M., Poudyal, S., Ali, M. H., & Dasgupta, D. (2021, September). Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. In 2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America) (pp. 1-5). IEEE.
[43] Li, Z., Rios, A. L. G., & Trajković, L. (2020, October). Detecting internet worms, ransomware, and blackouts using recurrent neural networks. In 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2165-2172). IEEE.
[44] Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE access, 8, 6249-6271.
[45] Celdrán, A. H., Sánchez, P. M. S., Castillo, M. A., Bovet, G., Pérez, G. M., & Stiller, B. (2023). Intelligent and behavioral-based detection of malware in IoT spectrum sensors. International Journal of Information Security, 22(3), 541-561.
[46] Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y. U., Jauro, F., Khan, A., ... & Abdulhamid, S. I. M. (2021). Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8699-8717.
[47] Khammas, B. M. (2020). Ransomware detection using random forest technique. ICT Express, 6(4), 325-331.
[48] Ullah, F., Javaid, Q., Salam, A., Ahmad, M., Sarwar, N., Shah, D., & Abrar, M. (2020). Modified decision tree technique for ransomware detection at runtime through API calls. Scientific Programming, 2020(1), 8845833.
[49] Ghouti, L., & Imam, M. (2020). Malware classification using compact image features and multiclass support vector machines. IET Information Security, 14(4), 419-429.
[50] Arunkumar, M., & Kumar, K. A. (2023). GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment. International Journal of Information Technology, 15(3), 1653-1660.
[51] Selamat, N., & Ali, F. (2019). Comparison of malware detection techniques using machine learning

algorithm. Indones. J. Electr. Eng. Comput. Sci, 16(1), 435-440.

[52] Noorbehbahani, F., Rasouli, F., & Saberi, M. (2019, August). Analysis of machine learning techniques for ransomware detection. In 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC) (pp. 128-133). IEEE.

[53] Mezquita, Y., Alonso, R. S., Casado-Vara, R., Prieto, J., & Corchado, J. M. (2020, June). RETRACTED CHAPTER: A Review of k-NN Algorithm Based on Classical and Quantum Machine Learning. In International symposium on distributed computing and artificial intelligence (pp. 189-198). Cham: Springer International Publishing.

[54] Saadat, S., & Joseph Raymond, V. (2020). Malware classification using CNN-XGBoost model. In Artificial Intelligence Techniques for Advanced Computing Applications: Proceedings of ICACT 2020 (pp. 191-202). Singapore: Springer Singapore.

[55] Sharmeen, S., Ahmed, Y. A., Huda, S., Koçer, B. Ş., & Hassan, M. M. (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access, 8, 24522-24534.

[56] Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y. U., Jauro, F., Khan, A., ... & Abdulhamid, S. I. M. (2021). Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8699-8717.

[57] Swami, S., Swami, M., & Nidhi, N. (2021). Ransomware detection system and analysis using latest tool. Int. J. Adv. Res. Sci. Commun. Technol, 7, 2581-9429.

[58] Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020, October). Evolution, mitigation, and prevention of ransomware. In 2020 2nd International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

[59] Wang, X. B., Yang, G. Y., Li, Y. C., & Liu, D. (2008, September). Review on the application of artificial intelligence in antivirus detection system i. In 2008 IEEE Conference on Cybernetics and Intelligent Systems (pp. 506-509). IEEE.

[60] Yang, B., & Liu, D. (2019, March). Research on network traffic identification based on machine learning and deep packet inspection. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 1887-1891). IEEE.

[61] Pimenta Rodrigues, G. A., de Oliveira Albuquerque, R., Gomes de Deus, F. E., de Sousa Jr, R. T., de Oliveira Júnior, G. A., Garcia Villalba, L. J., & Kim, T. H. (2017). Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection. Applied Sciences, 7(10), 1082.

[62] Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., ... & Su, J. (2020). A software deep packet inspection system for network traffic analysis and anomaly detection. Sensors, 20(6), 1637.

[63] Cascarano, N., Ciminiera, L., & Risso, F. (2011). Optimizing deep packet inspection for high-speed traffic analysis. Journal of Network and Systems Management, 19(1), 7-31.

[64] Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. Symmetry, 14(11), 2304.

[65] Yamany, B., Elsayed, M. S., Jurcut, A. D., Abdelbaki, N., & Azer, M. A. (2022a). A new scheme for ransomware classification and clustering using static features. Electronics, 11(20), 3307.

[66] Yamany, B., Azer, M. A., & Abdelbaki, N. (2022b). Ransomware clustering and classification using similarity matrix. In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 41-46). IEEE.