INTERNATIONAL JOURNAL OF RESEARCH AND REVIEWS IN SOCIAL AND APPLIED SCIENCES

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

MACHINE LEARNING AND DEEP LEARNING TECHNIQUES FOR RANSOMWARE DETECTION: A COMPARATIVE STUDY

Akpughe Hillard A.[1], Asagba Prince O.[2] & Onuodu Friday [3]
[1, 2,3] Department of Computer Science, University of Port Harcourt
EMAIL: Hillard_akpughe@uniport.edu.ng[1]; pasagba@yahoo.com[2] gonuodu@gmail.com[3]

D.O.I: 10.5281/zenodo.18457341

ARTICLE INFORMATION

Received: 25th Sept., 2025
Accepted: 28th Oct., 2025
Published: 25th Nov., 2025

KEYWORDS: Ransomware Detection, Machine Learning, Deep Learning, LSTM, Random Forest, Cybersecurity, Malware Analysis

DOI:

How to cite this article: Hillard A.A., Prince A.O. & Friday, O. (2025). Machine Learning and Deep Learning Techniques for Ransomware Detection: A Comparative Study. *International Journal of Research and Reviews in Social and Applied Sciences*, 2(1), 389-412. DOI:

ABSTRACT

Ransomware has emerged as one of the most destructive cybersecurity threats, necessitating intelligent and adaptive detection mechanisms beyond traditional security approaches. This study presents a comparative analysis of machine learning and deep learning techniques for ransomware detection, with emphasis on Artificial Neural Networks, Multilayer Perceptrons, Random Forest classifiers, and Long Short-Term Memory networks. The methodology adopted involved an extensive literature review of existing ransomware detection techniques, followed by an analytical comparison of traditional signature-based, behavior-based, and intelligent detection approaches. Experimental evidence from existing and proposed systems was examined to evaluate detection accuracy, precision, recall, and overall model performance. Feature-based datasets were analyzed, preprocessed, and evaluated using standard validation techniques to ensure consistency and reliability of results. The study highlights the strengths and limitations of each model, demonstrating that while machine learning algorithms offer efficiency and interpretability, deep learning models excel in capturing temporal ransomware behavior. Hybrid approaches combining deep learning and ensemble classifiers were found to deliver superior performance. The findings emphasize the necessity of intelligent ransomware detection frameworks capable of adapting to evolving attack patterns. This study contributes to cybersecurity research by providing a structured comparative framework and practical insights for selecting appropriate detection models.

1. INTRODUCTION

The continuous advancement and widespread adoption of Internet of Things (IoT) and fifth-generation (5G) communication technologies have significantly transformed the global cyberspace landscape. The expansion of spectrum usage from sub-3 GHz frequencies in 4G to frequencies approaching and exceeding 100 GHz has enabled wider bandwidths, ultra-low latency, and

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

massive device connectivity. Cyberspace defined as a global domain comprising interdependent information system infrastructures such as the Internet, telecommunication networks, computer systems, and embedded controllers has consequently become a critical pillar of economic growth, social development, and national security. However, this increasing dependence on interconnected digital systems has also expanded the attack surface, making cyberspace security a growing concern. Recent technological innovations have empowered cyber adversaries with sophisticated tools such as automatic malware generation frameworks, code obfuscation, and polymorphism techniques, which allow malicious programs to present identical interfaces while concealing varying underlying behaviors. These developments enable attackers to launch more damaging cyberattacks at reduced cost and effort. As a result, malicious software including ransomware, viruses, worms, trojans, cross-site scripting (XSS) exploits, backdoor attacks, Emotet trojans, and Stuxnet worms has continued to increase exponentially over the years.

Cyberattacks are commonly defined as malicious activities launched by individuals or groups to compromise the confidentiality, integrity, or availability of data and systems within a network (Iftikhar, 2024). These attacks target not only corporate and governmental infrastructures but also individual users. Andreea (2015) observed that technological evolution inherently fuels the progression of cybercrime, as attackers continuously devise new methods to infiltrate complex systems, evade detection, and remain anonymous. Among the various forms of cyber threats, ransomware has emerged as one of the most disruptive and economically damaging. Despite increasing public awareness and the deployment of advanced cybersecurity solutions, ransomware continues to pose a greater existential threat to organizations than many other cyberattacks. Coburn et al. (2018) noted that ransomware attacks have escalated in frequency, scope, and sophistication, often targeting enterprises with low tolerance for operational downtime. Even when system functionality is not completely paralyzed, ransomware attacks can severely compromise data integrity and confidentiality, affecting both Information Technology (IT) and Operational Technology (OT) infrastructures across public and private sectors.

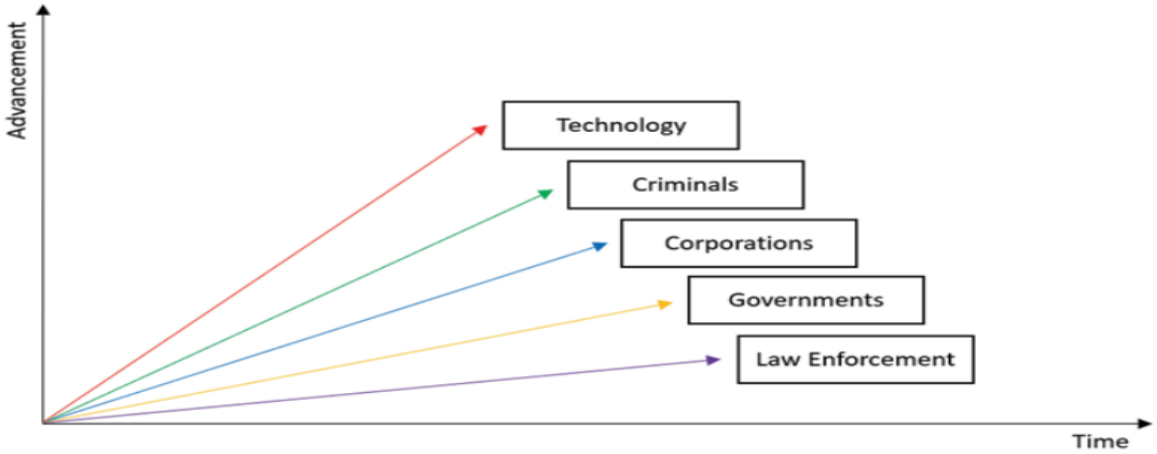

Figure 1: Speed of technology adoption (Matthew, 2021)

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

The disparity between the rapid pace of technological adoption and the slower evolution of defensive mechanisms further exacerbates this challenge. Matthew (2021) highlighted that attackers often require mastery of a single effective technique, whereas defenders must possess extensive multidisciplinary knowledge spanning networking, software engineering, law enforcement, and human behavior (see figure 1). This imbalance suggests that offensive capabilities are likely to outpace defensive responses, as illustrated by the accelerating speed of technology adoption. In response to these challenges, machine learning (ML) and deep learning (DL) techniques have gained prominence as effective approaches for ransomware detection. Unlike traditional signature-based methods, ML-based techniques learn patterns directly from data and are capable of identifying previously unseen attacks. Janaka et al. (2021) emphasized that ML models can derive classifiers from limited training datasets, eliminating the need for manually crafted signatures, which are often labor-intensive and ineffective against zero-day attacks. Consequently, a growing body of academic and industrial research has explored various ML and DL techniques for ransomware detection, necessitating a systematic comparative analysis of their effectiveness, strengths, and limitations.

Statement of the Problem

The rapid expansion of Internet connectivity, cloud computing, and IoT ecosystems has introduced unprecedented convenience and efficiency, but it has simultaneously intensified cybersecurity threats. Ransomware, in particular, has evolved into one of the most destructive forms of cyberattacks, continuously adapting to evade detection mechanisms. Despite extensive research and development efforts, existing ransomware detection approaches remain insufficient to address its growing sophistication. Traditional signature-based detection techniques are inherently limited to known ransomware variants and are ineffective against zero-day attacks. Static analysis methods are easily bypassed through code obfuscation and packing techniques, while dynamic and behavior-based approaches often suffer from high computational overhead and delayed detection. These delays frequently allow ransomware to execute encryption processes before mitigation measures can be applied. Even recent machine learning and deep learning models have largely focused on post-encryption behaviors, offering limited protection against irreversible data loss (Cen et al., 2024). Furthermore, emerging attack techniques such as steganographic malware where malicious payloads are concealed within benign digital media pose additional challenges to conventional detection systems. The availability of steganography tools has significantly increased, with over 1,200 applications readily accessible, many of which are freely downloadable (Barwise, 2018). This accessibility has contributed to a surge in steganography-based attacks, including campaigns such as Stegoloader, Vawtrak, and Stegano, which exploit legitimate platforms to distribute hidden malware (McMillen, 2017). Although machine learning and deep learning techniques have shown promise in improving ransomware detection, there remains a lack of comprehensive comparative studies that critically evaluate their performance, scalability, adaptability, and robustness against evolving ransomware variants. This gap hinders informed decision-making regarding the selection and deployment of optimal detection techniques. Addressing this challenge requires a systematic comparison of existing ML and DL-based

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

ransomware detection approaches to identify their limitations and highlight directions for more proactive, efficient, and resilient defense mechanisms.

Aim and Objectives of the Study

The aim of this study was to analyze and compare traditional and intelligent ransomware detection techniques, emphasizing ML and DL models. Specifically:

1. Review signature-based, behavior-based, and ML-based detection
2. Analyze ANN, LSTM, Random Forest, and MLP models
3. Highlight strengths and limitations of each technique

2. LITERATURE REVIEW

Overview of Network Security

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security standards should be set for any organization setting up or providing a wireless network. (Modesta & Ifeyinwa 2016). There are many features in computer networks, which plays a main part in verifying the level of network security. Safe network has turn into a requirement for most organization management. The security risk is rising day-by-day as well as to make high speed wired/wireless network. Sachin et al (2021) noted that a secure network has turn into a must requirement for any organization presently. The world is becoming more interconnected with the advent of the Internet and new networking technologies. Internet itself is now acting as a data store which has information related to personals, commercial, military and government sectors. The securing of this kind of data is taken as a serious aspect. Modesta & Ifeyinwa (2016) stated that fundamentally there are two different types of networks:

1. Synchronous Network 2. Data Network.

The internet is considered a data network. Since the current data network consist of computer-based routers, information can be obtained by Synchronous Network and Data Network. The internet is considered a data network. Since, information can be obtained by special programs, such as “Trojan horses,” planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet

Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices (Jaiswal, 2014). In order to come up with measures that make networks more secure, it is important to learn about the vulnerabilities that could exist in a computer network and then have

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

an understanding of the typical attacks that have been carried out in such networks (Meghanathan, 2014).

Network Security Attacks

Network attacks are unauthorized actions on the digital assets within an organizational network. Malicious parties usually execute network attacks to alter, destroy, or steal private data. Perpetrators in network attacks tend to target network perimeters to gain access to internal systems. These network security attacks can be categorized into two types

1. Passive Attacks 2. Active Attacks

Passive Attacks: This type of attacks involved attempts to crack the system by utilizing observed information. The following is attributes of passive attacks. Interception: attacks secretly like eavesdropping, "man-in-the-middle" attacks. Traffic Analysis: attacks privately, or silently. it can be involved trace back on a network - Sachin et al (2021). A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose of a passive attack is to gain information about the system being targeted; it does not involve any direct action on the target. A passive attack is characterized by the interception of messages without modification or change in data. The user might be oblivious to the fact that his data packets are being monitored by an external person. This type of activity is termed traffic analysis. Because there may be no evidence that an attack has taken place, prevention is a priority. Traffic analysis, however, may be a legitimate management activity because of the need to collect data showing usage of services, for instance. Some interception of traffic may also be considered necessary by governments and law enforcement agencies interested in the surveillance of criminal, terrorist and other activities. These agencies may have privileged physical access to sites and computer systems. Figure 2 shows a diagrammatic explanation of passive attacks.

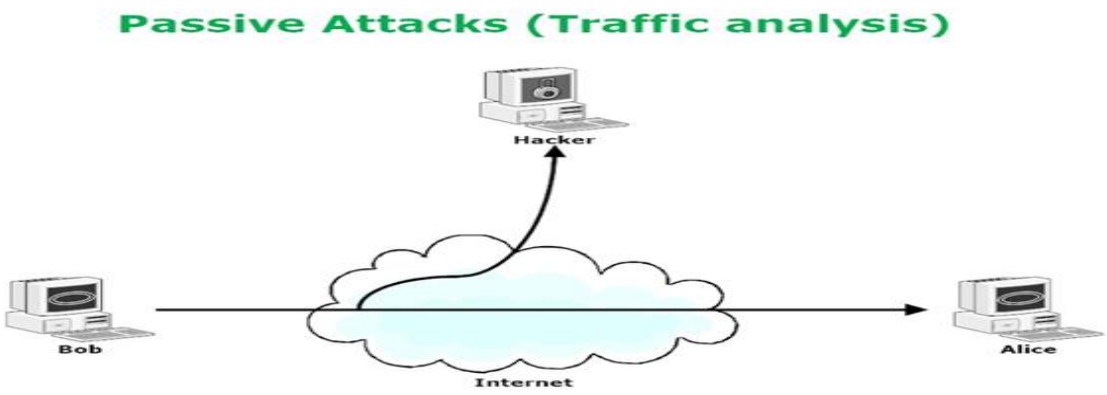

Figure 2: Passive Network Attack (Martin & Pavel, 2020).

Active Attacks: This kind of attack needs the attacker to share information to one or another of the parties, or block the flow of information in one or both directions. Interruption: attacks

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

accessibility. Modification: attacks sincerity. Fabrication: attacks authenticity. An active attack involves using information gathered during a passive attack to compromise a user or network. There are many types of active attacks. In a masquerade attack, an intruder will pretend to be another user to gain access to the restricted area in the system. In a replay attack, the intruder steals a packet from the network and forwards that packet to a service or application as if the intruder were the user who originally sent the packet. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are also examples of active attacks, both of which work by preventing authorized users from accessing a specific resource on a network or the internet (for example, flooding a web server with more traffic than it can handle). Figure 3 shows a diagrammatic explanation of active attacks.

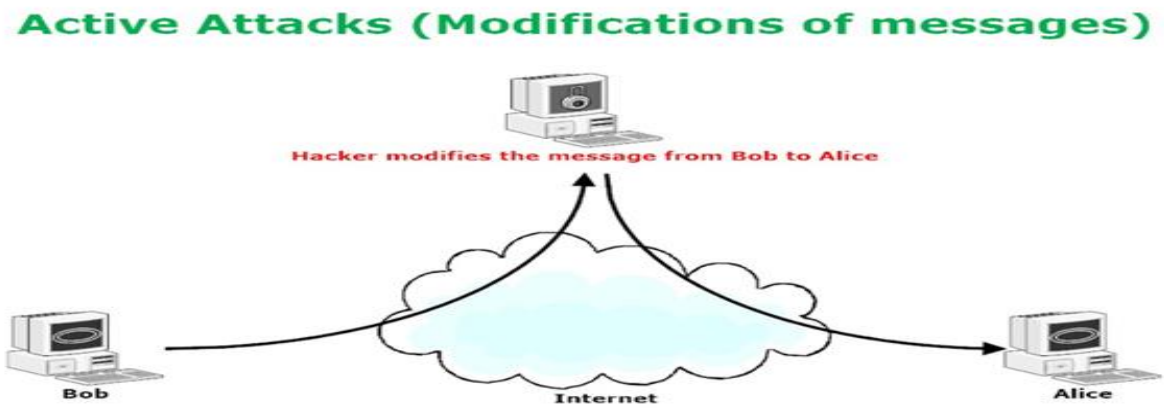

Figure 3: Active Network Attack (Martin & Pavel, 2020).

Technology for Network Security

In the 1950s, some developed countries began to study the application of computer technology in business management, management, design, manufacturing, etc., and information technology gradually evolved from stand-alone, information islands to enterprise information integration (Aidong et al, 2018). From the 1980s, China began to apply information technology to various fields. Due to its late start, the resources of foreign information communication network equipment were generally borrowed and introduced in the process of information construction. In February 2014, the central government established the "Network Security and Informatization Leading Group", which highlighted the important position of information network security in national security. Network security and informatization are a daunting task because it involves all network devices, and device security is an important aspect of overall network security. Wentao et al (2019), gave the definition of cloud computing as the delivery and usage mode of IT infrastructure, which means to obtain the required resources by means of the network. Generalized cloud computing according to Wentao et al (2019), refers to the delivery and usage patterns of services, which in turn refers to obtaining the required services through the network in an on-demand and scalable manner. This service can be IT and software, Internet related, or any other services. In terms of technology, the security and reliability of cloud computing technology is an important

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

prerequisite for the further promotion and security of cloud computing in various industries. However, along with the rapid development of cloud computing technology, its security issues faced by growing. As the computer network develops, the problems of mail bombs, hacking programs and remote listening are gradually highlighted, which seriously affect the security of computer networks. The cloud computing environment refers to the integration of terminal devices, such as computers distributed on the Internet, to realize hardware and software resources by means of some kind of network calculation.

Factors that affect network security

Lack of core software technology: At present, most developing countries lacks independent technology in computer information network security, which leads to three security vulnerabilities in modern network environment. These security technologies need to be imported from developed countries, resulting in poor computer information network security rate posing huge hidden dangers.

No safety assessment system has been established: Whether the computer information network can resist hacker intrusion is the evaluation criterion of information security. The quality of security evaluation mainly depends on whether to build a scientific and accurate network information security prevention evaluation system. Then conduct a feasibility assessment based on these strategies. However, China has not established a complete security assessment system in computer information network technology.

Lack of preventive systems: Due to the lack of core technology and the lack of safety assessment system, many small and growing enterprises fail to build a good scientific and reasonable prevention system. In this computer information network environment, network criminals often take advantage of the enterprise network security management loopholes to steal corporate secrets. That is to say, it is the lack of network security management system in the process of operation and management that leads to the occurrence of these undesirable situations. Make the internal personnel of the enterprise because of certain interests and take risks, violate the relevant laws of the country.

Weak safety awareness: In daily life, people often like to use computers and mobile phones for study, entertainment, work and so on. These activities are inseparable from the Internet. However, in the practical application, people lack correct cognition of network information security. Even if the network itself has some protection measures, but these protection measures are too simple, belongs to the basic protection. It has no effect on the actual situation of more complex network attacks. These various factors are shown diagrammatically in figure 4.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Figure 4: Factors that affect network security (Wenfu Y., 2020)

3. RANSOMWARE: CONCEPTS, CLASSIFICATIONS, AND EVOLUTION

Ransomware

Throughout the period of globalization, governments, corporations and the public have rapidly adopted new computer-based systems, software platforms and Internet-enabled devices. The global market for consumer technologies and personal electronic devices continues to grow exponentially through the continuous product development cycles for new Internet-enabled devices, mobile phones, Internet of Things (IoT) devices and Internet-enabled Operational Technologies (OT). Whilst consumers have been quick to adopt these emerging technologies, they have generally been slow to recognize the security-related threats associated with these emerging technologies and platforms. An underlying trait of the cybersecurity discourse is that applying the necessary security controls is inherently considered to be a reactive, not proactive, process. Natively, organizations have large attack surfaces with complicated internal structures and processes, whereas cybercriminals are astute and positioned to rapidly exploit security control deficiencies and vulnerabilities.

Classification of Ransomwares Attacks

Analyzing technically, ransomware attacks are more broadly classified as a type of malware. Malware is a commonly used term to describe a piece of malicious software or file that is intentionally designed to be harmful to a computer or electronic device. Malware is typically designed to be a pre-packaged exploitation of a known or unknown vulnerability. Once activated, the malware is designed to deliver a "payload" of actions and instructions. The instructions can include details about what the system should do after it has been compromised. The activation mechanism can vary between requiring the user to click a link or enable hidden content, or it may be remotely activated by the attacker. Some types of malware also employ additional functions such as worms, which contain a set of instructions that enable an automated self-reproduction cycle

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

to rapidly propagate the attack. Analysis of ransomware attacks and source code indicates that ransomware attacks could be further categorized as:

1. Targeted attacks 2. Non-targeted attacks.

Targeted Ransomware Attacks: Targeted attacks occur when the attacker develops a ransomware attack for a specific target. The reasoning behind the target selection can range from being purely financially motivated, revenge, geographical location or simply because the individual or organization may be using a vulnerable application or device. The language used may also be another indicator of the desired target and the origin of the attacker.

Non-Targeted Ransomware Attacks: Non-targeted attacks are indiscriminate and have no predefined infection limitations. These types of ransomware attacks typically utilize a worm or similar propagation mechanism to rapidly spread the infection through large numbers of user systems and devices. However, despite being classified as non-targeted ransomware, this may have limited impact on victim geography versus targeted attacks. This is because the largest number of consumer devices, networks and IoT are operated in these areas; thus, the attack surface is much larger due to the volume of devices.

Attackers have developed a way to monetize files already on a victim's computer. They accomplish this through encrypting select files and then charging for access to the key. This type of malware has spawned a new classification, crypto-ransomware, but is more commonly known by the name of most prevalent version, Crypto-Locker, or its variants Tesla-Crypt and Crypto-Wall (Maurya et al, 2018).

Famous Cases of Ransomware attacks:

I. In August 2016, Bournemouth University was successfully attacked and corrupted files by ransomware 21 times during previous 12 months.

II. In April 2016, A Network Hospital of MedStar Health in Maryland, was attacked and blocked working by the SamSam ransomware.

III. In February 2016, Hollywood Presbyterian Medical Center was attacked by Locky ransomware and disrupted working for two weeks until they paid 40 Bitcoin (about $17,000) to recover its files.

IV. On 6 April 2022, Bet9ja a sports-betting platform suffered a cyber-attack that rendered the platform inaccessible to users. As a result of this, users were unable to access their accounts and/or place bets on the platform.

Table 1 shows the evolution of a few popular ransomware attacks in recent times, its various techniques and general characteristics also how these have affected users.

Table 1: Evolution of Ransomware Attacks

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Year, Name	Description
Nova Ransomware, August 2025	Clinical Diagnostics in Rijswijk paid undisclosed fee to ransomware group who demanded millions of euros—to prevent the release of medical data from about 485,000 Dutch women.
Blue Locker, August 2025	Pakistan Petroleum Limited foiled a ransomware attempt, suspending non-critical services to contain the threat and protect critical systems and data.
Akira, July 2025	Russian alcohol retailer WineLab shut down its retail and online services after a ransomware attack by the Akira gang, which crippled its IT infrastructure and customer support.
Babuk Locker, 2024	A ransomware attack on supply chain management software provider Blue Yonder affected the scheduling and payroll capabilities of 11,000 Starbucks stores across the USA.
Brain Cypher, December 2024	A ransomware group claimed to have obtained over 1TB of data belonging to Deloitte UK, raising concerns about the security preparedness of major consulting firms.
Synnovis, June 2024	A ransomware attack on Synnovis canceled over 800 surgeries, diverted patients, and left doctors unable to match blood types, forcing reliance on type O and causing a shortage.
LockBIt, June 2023	LockBit ransomware hit MCNA Dental, exposing data of 9 million people after a $10M ransom demand went unpaid.
LockBit, January 2023	The attack crippled international mail delivery, froze online services, and even caused printers at a Royal Mail center in Northern Ireland to churn out LockBit's ransom notes.
DarkSide, May 2021	Colonial Pipeline suffered a ransomware attack that disrupted fuel supply across the U.S. Southeast, causing panic buying even in unsafe containers and leading the company to pay a $4.4 million ransom.
Babuk, April 2021	The NBA was attacked with claims to have stolen 500 GB of confidential Houston Rockets data and threatened to leak financial and contract documents if their demands of $50 Million were not met.
Robinhood, May 2019	Baltimore was hit by Robinhood ransomware, causing $18M in damages, a demand of 13 bitcoins ($400,000), citywide system shutdowns, and took weeks of recovery.
Jeff, 2017	It attacked in May 2017 with spam mail and collected money in form of bitcoin.
Locky, July 2016	Added a failsafe mechanism that begins encrypting files even if the ransomware cannot request a unique encryption key from the criminals' servers due to the target computer either being offline or blocking the communications (Constantin, 2016c).
Jigsaw, 2016	Embeds an image of the clown from the Saw movies into a spam email. ransom payment of $150, according to Webroot.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

KeRanger, Jan, 2016	KeRanger is first ransomware attack targeting Apple system; It takes three days to activate and is designed to encrypt more than 300 file types.
2015, Tor sites	As the name implies, it targets Linux systems. It encrypts both data files and files associated with web applications. It does this by overwriting the master boot record (MBR) of the infected computer. Without the MBR, the operating system cannot reconstruct the unencrypted files.

4. TRADITIONAL RANSOMWARE DETECTION TECHNIQUES

Detecting attacks by ransomware on computer systems and networks is the goal of ransomware detection techniques. These methods use a variety of detection techniques to find indications of compromise (IOCs) linked to ransomware activity (Masum et al., 2023). Here are some typical methods to detect ransomware within a network:

Signature-based detection: This technique relies on known signatures or patterns of known ransomware strains. Antivirus software and intrusion detection systems (IDS) use signature databases to identify known ransomware based on these patterns. However, it may be less effective against new or modified ransomware variants.

Behavior-based detection: Behavior-based detection focuses on monitoring the behavior of programs and processes in real-time to identify malicious activities. It looks for behaviors associated with ransomware, such as mass file encryption, rapid file access, or attempts to delete or modify critical system files.

Heuristic analysis: Heuristic-based detection involves analyzing the behavior of programs and files to identify suspicious or malicious activities. This technique looks for characteristics commonly found in ransomware, such as file encryption, unusual network communication, or unauthorized system modifications.

Network traffic analysis: Monitoring network traffic for suspicious patterns can help detect ransomware activities. This includes analyzing network packets for indicators like high data volume, unusual communication patterns, or connections to known malicious IP addresses or domains.

Endpoint monitoring: Monitoring endpoints (individual devices or servers) for signs of ransomware can involve techniques like file activity monitoring, registry monitoring, or system call monitoring. This approach can detect file encryption, changes to system settings, or other ransomware-related activities.

5. MACHINE LEARNING–BASED RANSOMWARE DETECTION

Machine learning and AI-based detection: Machine learning algorithms can be trained to identify ransomware based on patterns and characteristics observed in known ransomware

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

samples. These algorithms can learn to detect previously unseen ransomware variants by analyzing features like file attributes, network traffic, or system behaviors.

Random Forest which is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes (classification) or the mean prediction (regression) of the individual trees. Given data on predictor variables (inputs, X) and a continuous response variable (output, Y) build a model for: Predicting the value of the response from the predictors. Understanding the relationship between the predictors and the response e.g. predict a person's systolic blood pressure based on their age, height, weight, etc. Some examples of pairs a random forest can predict are

1. Y: income, X: age, education, sex, occupation, …
2. Y: crop yield, X: rainfall, temperature, humidity, …
3. Y: test scores, X: teaching method, age, sex, ability, …
4. Y: selling price of homes, X: size, age, location, quality, …

To perform classification using random forest, binary trees are grown where at each node, the data is split into two daughter nodes based on a chosen splitting criterion. Terminal nodes are reached at the bottom of the tree. In regression, the predicted value at a node is the average response variable for all observations in the node, while in classification, the predicted class is determined by the majority vote of classes in the node. Additionally, for classification trees, it's possible to obtain estimated probabilities of membership in each of the classes. Figure 5 illustrates the classification process in a Random Forest model. That begins with the original dataset, from which multiple bootstrap samples are drawn through sampling with replacement. Each bootstrap sample is then used to train a separate decision tree, with random feature selection applied at every split to ensure diversity among the trees. Once the trees are built, they each make independent predictions. Finally, the results are combined through majority voting, where the class with the highest number of votes across all trees is selected as the final classification output.

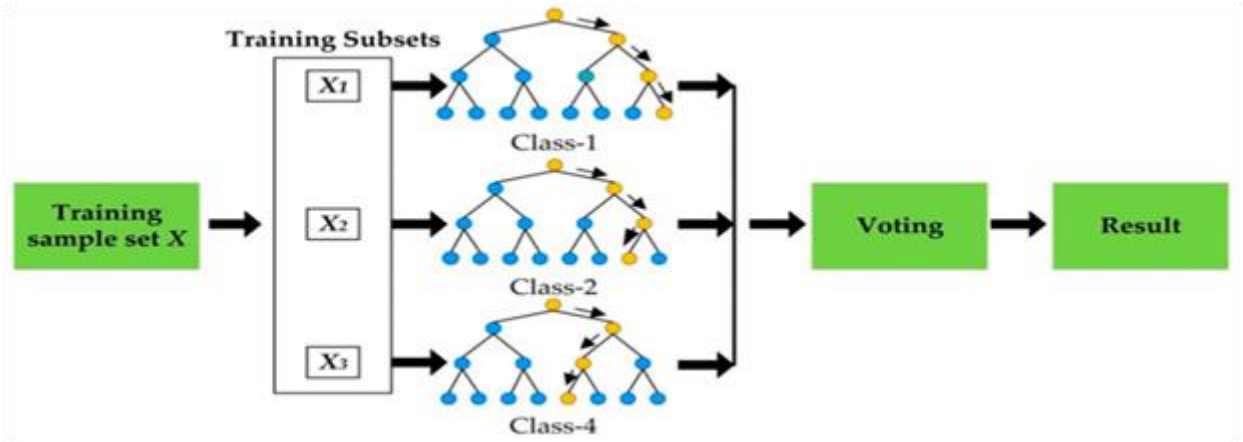

Figure 5: Random Forest Classification Process (Wu et al, 2019)

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Artificial Neural Networks (ANN): An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information (Waleed & Sivaram, 2017). It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons. ANN takes inputs from historical data that enables the network to learn the relationships between inputs that characterize the phenomena being mode. Artificial neural networks are a subset of machine learning and are at the heart of deep learning algorithms. Artificial neural networks (ANNs) are comprised of a node layer, containing an input layer, one or more hidden layers, and an output layer. Each node, or artificial neuron, connects to another and has an associated weight and threshold. If the output of any individual node is above the specified threshold value, that node is activated, sending data to the next layer of the network. Otherwise, no data is passed along to the next layer of the network. Figure 6 shows the architecture of an artificial neural network. An ANN has one input layer and one output layer, the hidden layers in the network can be more than one for a more refined output result.

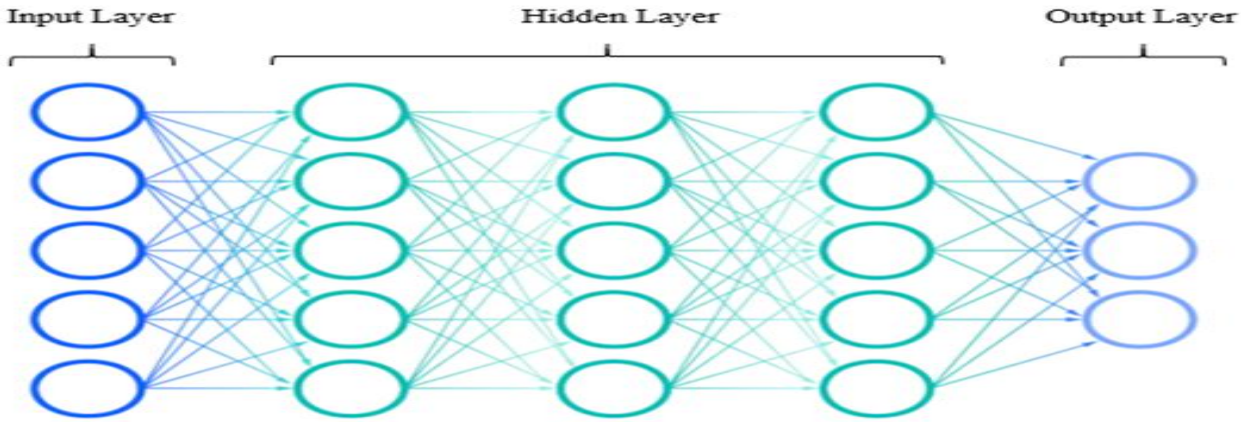

Figure 6: Architecture of an Artificial Neural Network (Julia, 2022).

Multilayer Perceptron (MLP): Multilayer perceptron is one of the most used types of artificial neural network – Balabanov et al (2018). Multilayer perceptron is weighted directed graph organized in layers. When multilayer perceptron is fully connected each neuron from a single layer is connected with each neuron from the next layer. Neurons are the nodes in the graph where links between nodes are weighted. The calculating power of multilayer perceptron is in its weights. Finding proper values for the weights is a global optimization problem. We always have to remember that the value of a neural network is completely dependent on the quality of its training. Without abundant, diverse training data and an effective training procedure, the network will never "learn" how to classify input samples - Balabanov et al (2018).

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

6. DEEP LEARNING TECHNIQUES FOR RANSOMWARE DETECTION

There are several types of artificial neural networks. These types of networks are implemented based on the mathematical operations and a set of parameters required to determine the output. Some of the various types of the artificial neural network are:

Recurrent Neural Network (RNN):

The Recurrent Neural Network also known as Long Short-Term Memory, works on the principle of saving the output of a layer and feeding this back to the input to help in predicting the outcome of the layer. Here, the first layer is formed similar to the feed forward neural network with the product of the sum of the weights and the features. The recurrent neural network process starts once this is computed; this means that from one time step to the next each neuron will remember some information it had in the previous time-step. This makes each neuron act like a memory cell in performing computations. In this process, we need to let the neural network to work on the front propagation and remember what information it needs for later use. Here, if the prediction is wrong, we use the learning rate or error correction to make small changes so that it will gradually work towards making the right prediction during the back propagation. – (Balachandra, 2021). Figure 7 shows an architecture of RNN classifier. RNN is the extension of feedforward NN with the presence of loops in hidden layers. RNN takes the input with the sequence of samples and identifies the time relationship between the samples.

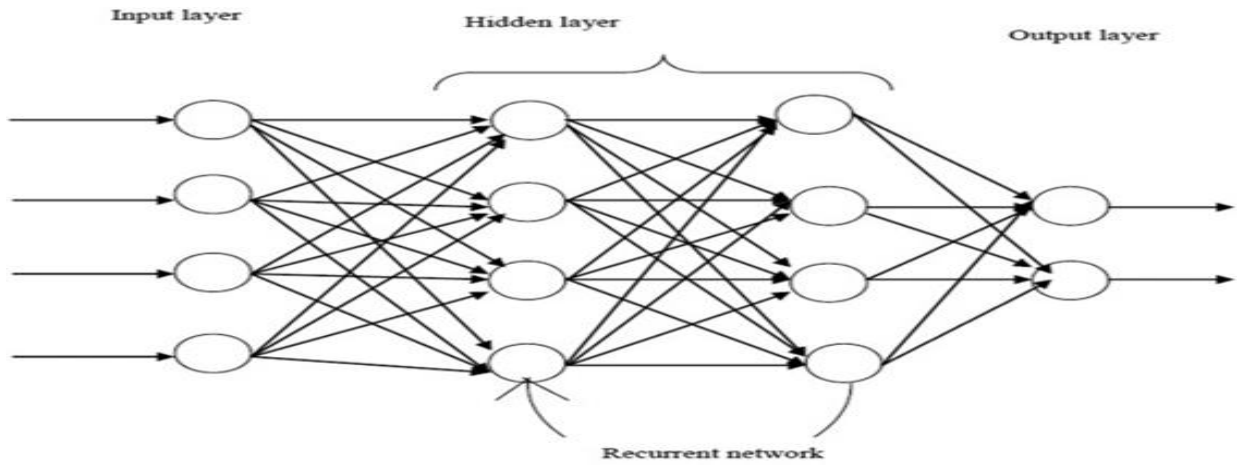

Figure 7 Architecture of RNN classifier. (Balachandra, 2021)

Long Short-Term Memory (LSTM):

Long Short-Term Memory (LSTM) is a special type of Recurrent Neural Network (RNN) that is designed to learn and remember patterns in sequential data. Unlike traditional RNNs, which often suffer from vanishing or exploding gradient problems, LSTMs use gating mechanisms to control the flow of information, making them capable of capturing both short-term and long-term dependencies in data. This ability makes LSTM a powerful technique for detection tasks,

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

especially where data is temporal or sequential. LSTM has been proven useful in detection problems often require recognizing patterns over time rather than analyzing static features alone. Many real-world systems produce data in the form of sequences or time series, where the meaning of current data points depends on past observations. For example, in fraud detection, a single transaction may not indicate fraud, but a sequence of unusual transactions over time could reveal fraudulent behavior. Common areas where LSTM is applied for detection include:

a. Anomaly detection in network traffic or sensor readings - Li et al, 2022.
b. Fraud detection in financial transactions – Onyeoma et al, 2024.
c. Intrusion detection systems (IDS) in cybersecurity – Volpe et al, 2024.
d. Fault detection in industrial systems – Zhao et al, 2018.
e. Speech or activity detection from time-series signals - Pei et al, 2022.

Among the different variants of LSTM, four stand out as the most widely used due to their effectiveness in real-world detection tasks. The Vanilla LSTM is the basic and most commonly applied form, consisting of a single LSTM layer that captures temporal dependencies in sequential data. The Stacked (Deep) LSTM extends this idea by placing multiple LSTM layers on top of one another, allowing the model to learn higher-level temporal patterns and improving its ability to detect complex anomalies. Another popular type is the Bidirectional LSTM (BiLSTM), which processes data both forward and backward, enabling it to capture context from both past and future states within a sequence—this makes it especially powerful in fields like text classification, intrusion detection, and fault diagnosis. Finally, the Convolutional LSTM (ConvLSTM) combines convolutional layers with LSTM units, making it suitable for spatio-temporal data such as videos, medical imaging, and sensor networks, where both spatial and temporal features are important for accurate detection.

In an LSTM cell, the computation at each time step depends on three main inputs that collectively determine how information flows and is updated. First, it receives the cell state from the previous step, c_{t-1}, which represents the long-term memory of the network and carries forward important contextual information across time steps. Second, it takes in the previous hidden state, s_{t-1} (sometimes denoted as h_{t-1}), which captures the short-term representation of the sequence up to the last time step and influences how the network responds to the current input. Third, it processes the current input, x_t, which is the new observation or data point at the present time step. These three components interact through the LSTM's gating mechanisms—namely the forget gate, input gate, and output gate—to decide what information should be discarded, updated, or retained. The outcome of these computations produces a new cell state, c_t, which updates the memory to reflect both past and present information. From this updated memory, the LSTM then generates the new hidden state, s_t, which is passed forward to influence predictions or to serve as input for the next time step in the sequence. However, the input, output, and the forget gate activation is scaled using the sigmoid function, and the output of the hidden state is filtered using the hyperbolic function. Figure 8 shows the diagrammatic representation of an LSTM Cell.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

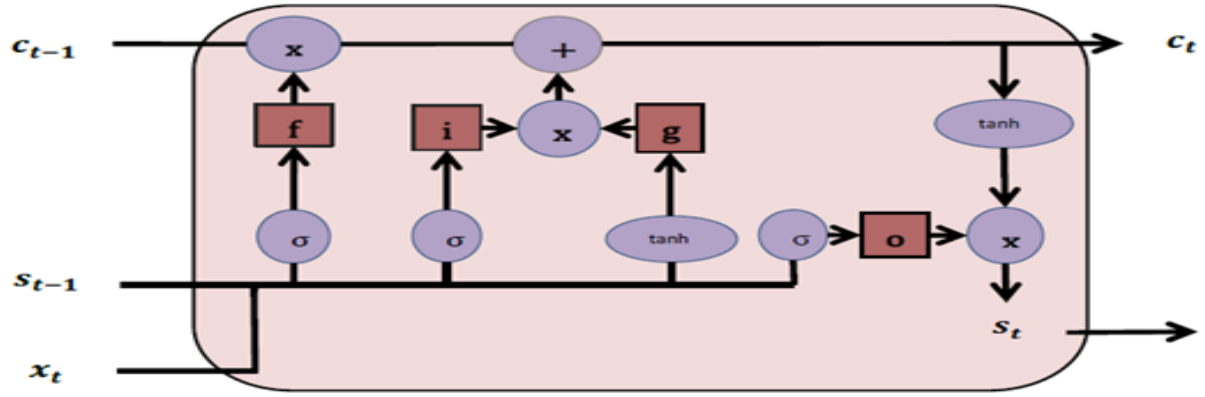

Figure 8: Memory Cell of LSTM. (Avci et al, 2023)

7. COMPARATIVE ANALYSIS OF ML AND DL MODELS

We evaluated algorithms used in training ANN based on the following standard performance measures:

True Positive (TP): Number of correctly identified malicious code,

False Positive (FP): Number of wrongly identified benign code, when a detector identifies benign file as a malware.

True Negative (TN): Number of correctly identified benign code.

False Negative (FN): Number of wrongly identified malicious code, when a detector fails to detect the malware because the virus is new and no signature is yet available.

True detection Rate (TP rate): Percentage of correctly identified malicious code.

$$TP\ Rate = \frac{TP}{TP+FN} \qquad (1)$$

where TP is the number of correctly identified codes also known as precision, FN is the number of wrongly identified codes.

False alarm Rate (FP rate): Percentage of wrongly identified benign code, given by:

$$FP\ Rate = \frac{FP}{FP+TN} \qquad (2)$$

where FP is the number of wrongly identified benign codes also known as recall, TN is the number of correctly non-identified codes.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

F-Measure: It is a measure of a test's accuracy by combining recall and precision scores into a single measure of performance, usually it is between 0.0 and 1.0 closer to 1 is good and closer to 0.0 is poor.

$$F = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (3)$$

F-measure becomes the final measure of test accuracy.

Overall Accuracy: Percentage of correctly identified code, given by:

$$Overall\ Accuracy = \frac{TP+ TN}{TP + TN + FP + FN} * 100 \quad (4)$$

However, ransomware attacks pose a serious threat to Internet resources due to their far-reaching effects. Badejo et al (2018), presented water current prediction using Artificial Neural Networks (ANNs). The Back Propagation (BP) technique with feed forward architecture and optimized training algorithm known as Levenbergq-Marquardt to develop a Neural Network Water Current Prediction model-(NNWLM) in a MATLAB programming environment. The Commodore channel which is also referred to as the Lagos harbor is a navigation channel in Lagos, Nigeria and is located near Beecroft and Wilmot point. The terrain elevation above sea level is 0 meter. It is situated on Latitude: 60 24'0'' and Longitude: 30 24'0''. It was dredged by British royal Engineers in 1908 for ships coming into the Lagos harbor which makes it one of the most important parts of the Lagos lagoon. The training process requires a set of examples of proper network behavior, that is network inputs *p* (current and water level data designated as input) and target outputs *t (*current designated as output). During training, the weights and biases of the network are iteratively

Berrueta et al. (2022), proposed a tool that detect and block crypto-ransomware activity based on file-sharing traffic analysis. The tool monitors the traffic exchanged between the clients and the file servers and using machine learning techniques it searches for patterns in the traffic that betray ransomware actions while reading and overwriting files. Berrueta et al. (2022), extracted features from network traffic that describe the activity opening, closing, and modifying files. The features allow the differentiation between ransomware activity and high activity from benign applications. They went further to train and test the detection model using a large set of more than 70 ransomware binaries from 33 different strains and more than 2,400 hours of 'non-infected' traffic from real users. The training, optimization and evaluation process were been carried out using SMBv2 (a windows filesharing protocol) traffic. Their neural network model using T=30s can detect ransomware binaries in SMBv2, SMBv3 and NFS scenarios, even when being trained using only traffic from the first one. Comparing the different ransomware detection approaches and techniques. (Yamany et al., 2022) investigated the criteria, parameters, and tools used in the ransomware detection ecosystem. They also presented the main recommendations and best practices for ransomware mitigation. Also proposing an efficient ransomware indexing system that provides search functionalities, similarity checking, sample classification, and clustering.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Jenkins et al (2018), noticed how there is a lack of approaches to derive qualitative scenarios automatically for the testing of Autonomous Drive systems. And how machine learning provides the possibility to automate such tasks. Using data from both in-vehicle systems and also from vehicle to infrastructure stating how they could also be used toward the modelling and generation of accident scenarios to deliver test data for Autonomous Drive testing. In other domains solutions for prediction of wind speed to improve efficiency of wind turbines and the generation of handwriting text have been achieved using ANNs called recurrent neural networks (RNNs). Their goal was to develop a prototype tool to model accident data and then generate new accident scenarios without manual specification, avoiding randomized alternations of existing scenarios and achieve more realistic scenario generation. Their results show that the variables speed, direction, and the state of traffic lights were enough to produce valid results. The use of x and y coordinates were not needed nor yielded improved results. Only a small number of frames of data were needed to make accurate predictions, beyond three frames, the accuracy decreased. Their prototype demonstrates successful generation of accident scenarios using recurrent neural networks. The accuracy to which the prototype can reproduce an unseen scenario from the training sets.

With the aim to extend an open-source Intrusion Detection System (IDS) to detect network-based covert channels, Gunadi & Zander (2017) researched on the Comparison of IDS Suitability for Covert Channels Detection. They compared Snort, Suricata, and Bro based on a number of important features such as type of IDS, extensibility, capacity per instance, scalability, user base, active development and their licenses. Bro not being the most popular IDS; it has a decent number of users and there is significant development activity. Bro is open source and release under the liberal BSD license. Based on the comparison they propose to use Bro as the open-source IDS that we will extend with covert channels detection. Akten & Grierson (2016), highlighted how artificial neural networks with recurrent connections learn temporal regularities and model sequences. However, they stated that current generative RNN techniques do not allow real-time interactive control of the sequence generation process, thus aren't well suited for live creative expression. They then proposed the use of character-based LSTM networks and a gestural interface allowing users to 'conduct' the generation of text. According to Akten & Grierson (2016) Long Short-Term Memory (LSTM) is a recurrent architecture that overcomes the problem of gradients exponentially vanishing or exploding and allows RNNs to be trained many time-steps into the past, to learn more complex programs. Now, with increased compute power and large training sets, LSTMs and related architectures are proving successful not only in sequence classification, but also in sequence generation in many domains such as music, text, handwriting, images, machine translation, speech synthesis and even choreography. Different architectures for each model were used in training depending on the size of the training data, ranging from a single LSTM layer with 256 dimensions, to three LSTM layers each with 512 dimensions. We use LSTM cells with input, output and forget gates, without peepholes or skip connections between layers. They built an interactive prediction and visualization system which mixes each model's predicted probability distributions via mixture weights, controlled in real-time via a user's gestures.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

8. EXPERIMENTAL EVIDENCE FROM EXISTING AND PROPOSED SYSTEMS

Analysis of the Existing System

It is important to state that good efforts had been made in the work of Cen et al (2024) in the development of a ransomware (malware) cyber-attack detection and prevention. Their work provides a comprehensive overview of ransomware as a growing cybersecurity threat and emphasizes the shortcomings of traditional detection systems. It reviews existing approaches such as signature-based detection, static analysis, and dynamic analysis, highlighting their limitations in handling zero-day variants, obfuscation, and high computational overhead. Cen et al (2024) correctly pointed out that ransomware has become increasingly sophisticated, rendering conventional methods less effective, and motivating the need for machine learning–based solutions. Their work is the bases of discussions of the existing system and from there we intend to build on the areas that can be improved upon to ensure more level of speed and accuracy in the process of detection and prevention. Their developed system was based on RNN, this is a common approach for processing sequential data, such as time series or sequences of instructions and activities which the dataset has now been converted to. Due to the constant changing pattern of ransomware, they focused on system-level behavioral features and used this in the development of their ransomware detection model, these were primarily derived from file system activities, process behaviors, and registry modifications. These features were chosen because ransomware typically interacts heavily with system resources during its lifecycle.

Dataset used for testing and training was sourced from public malware repositories such as VirusShare and VirusTotal, while the benign samples were drawn from standard software applications all put together to form one dataset. The malware samples were crossed checked using antivirus engines to ensure they were genuine ransomware families (e.g., WannaCry, Locky, Cerber), and then they executed in a virtual environment to safely capture their behavioral traces. Dataset contained features that aren't in a numerical format (such as text or categorical data) needed to be preprocessed to make it suitable for machine learning. While their dataset had limited scale, scope, and realism, a gap was created that can be filled by incorporating larger, more diverse, and real-world datasets enriched with multi-modal features already tested and uploaded. Their model scans feature in the packet and matches with the existing feature dictionary and words that matches the list of features were retrieved and frequency of its occurrence were counted and an output based on this is given for either a ransomware or a benign-ware. The process involving the analysis of network traffic packets to classify them as either potentially carrying ransomware or being benign (safe). Network packets are units of data that are transmitted over a network and contain information about the communication between devices. A feature dictionary in this instance is a collection of known characteristics or patterns associated with different types of network traffic. This dictionary is created based on historical data and knowledge about typical behaviors of benign and malicious network traffic. The model keeps track of how frequently these matching features occur within the packet. This frequency count helps in assessing the significance and strength of the evidence for classifying the packet. Figure 9 shows a view of the architectural structure the

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

existing system by Cen et al (2024). The data flow, feature engineering, learning, and decision-making components were capture.

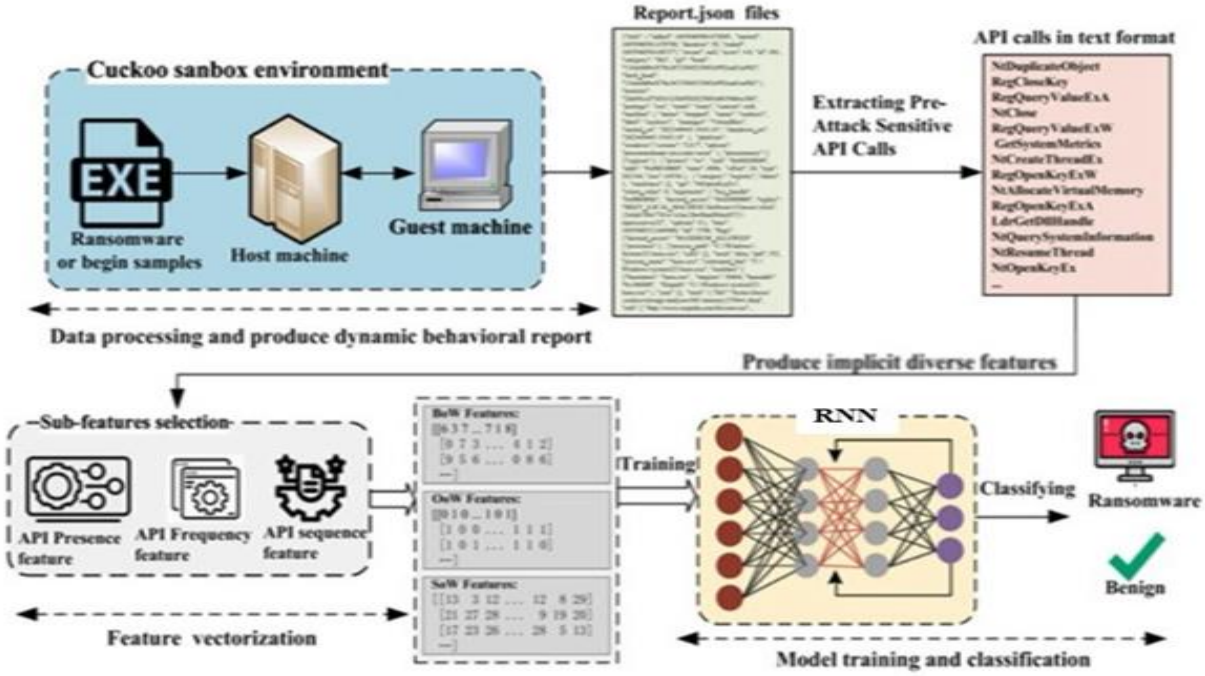

Figure 9: Architecture of an Existing System (Cen et al, 2024).

Analysis of the Proposed System

The proposed ransomware detection and prevention system is developed using the Object-Oriented Analysis and Design Methodology (OOADM), which emphasizes modeling the solution as a collection of interacting objects, each with clearly defined roles and responsibilities. By applying OOADM, the design ensures modularity, extensibility, and reusability, which are critical in cybersecurity solutions where threat patterns evolve continuously. The system is structured into three core functional layers: data analysis, detection/classification, and prevention. These functions are encapsulated in different objects, enabling clear separation of concerns and enhancing maintainability of the overall architecture. This study would be focuses on modifications and part replacement of the existing detection and prevention model as applied to ransomware using the OOAD approach. These visual models would make it easier for stakeholders, including developers, designers, and non-technical members of our team, to understand and communicate about the software system. This approach also allows for easier modification and adaptation of the software as requirements and data evolve or change with time. By having a clear understanding of the system's architecture and design, we can make informed decisions when making modifications. The proposed system design would describe an automated data analysis, detection and prevention system as a model that can be utilized within a network of users. The system model would be able to filter data packets based on certain criteria and determine whether to grant access to the packet

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

into the network or deny access. Figure 10 shows the architecture of the proposed system and it captures how the system is designed to automatically analyze and process data within a network for the purposes of detecting and preventing potential threats or unwanted activity. It combines three functionalities:

a. Data Analysis b. Detection c. Prevention

Through techniques like use case diagrams and scenarios, OOAD would help in capturing and defining the functional and non-functional requirements of our software system. However, the proposed system architecture presents the structure of the system; presenting the various systems segments and components. Figure 10 shows an architectural design for the proposed system:

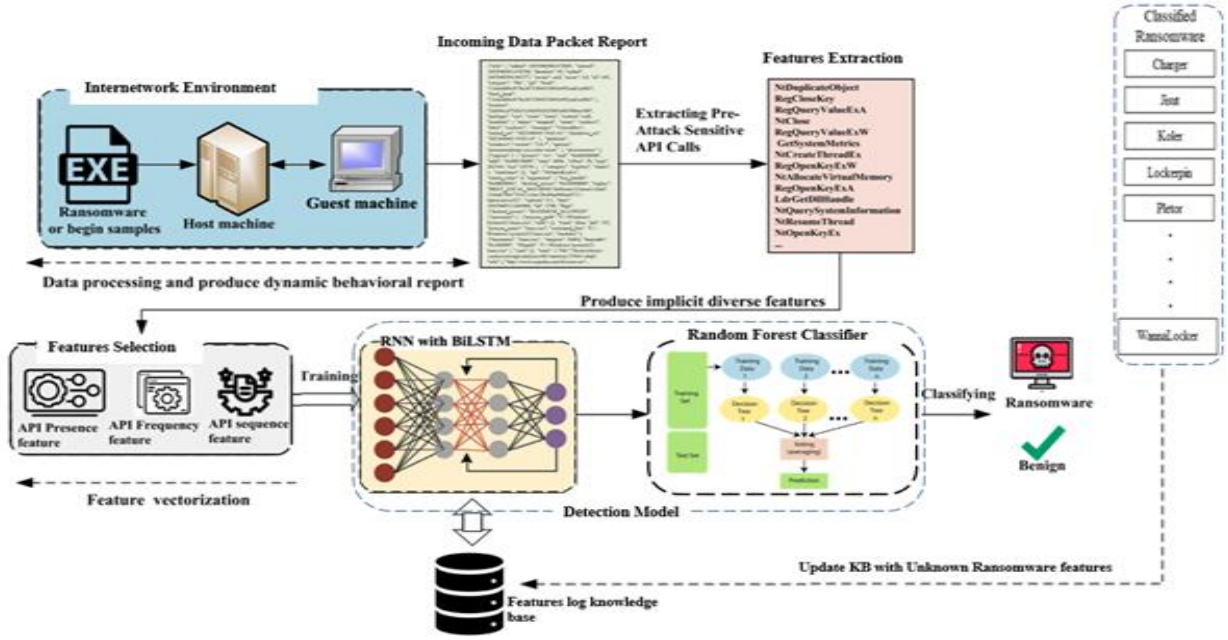

Figure 10: Architecture of the Proposed System.

9. CONCLUSION

This study presented a comprehensive comparative analysis of traditional, machine learning, and deep learning techniques for ransomware detection, with particular emphasis on Artificial Neural Networks, Long Short-Term Memory networks, Random Forest classifiers, and Multilayer Perceptrons. From the literature review through experimental evidence drawn from existing and proposed systems, it is evident that traditional detection mechanisms such as signature-based and heuristic approaches are increasingly ineffective against modern and evolving ransomware variants. Machine learning techniques improve detection accuracy by leveraging feature-based classification, yet they often struggle with sequential and time-dependent attack behaviors. Deep

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

learning models, especially LSTM and BiLSTM architectures, demonstrate superior capability in learning temporal patterns inherent in ransomware activities, leading to improved detection performance and reduced false positives. The comparative results further show that ensemble and hybrid approaches, such as combining deep learning with Random Forest classifiers, offer a balanced trade-off between accuracy, robustness, and interpretability. Overall, the study confirms that intelligent detection techniques significantly outperform traditional methods and that hybrid ML–DL frameworks represent a promising direction for ransomware defense. Future research should focus on adaptive learning models, real-time deployment, and lightweight architectures that can operate efficiently in large-scale network environments.

RECOMMENDATIONS

Based on the findings of this study, several recommendations are made. Firstly, it is recommended to cybersecurity researchers and academic institutions to focus future studies on hybrid machine learning and deep learning frameworks, particularly those that integrate temporal learning models such as LSTM with ensemble classifiers like Random Forest, as these approaches have demonstrated superior detection capabilities. Secondly, it is recommended to network administrators, organizations, and security practitioners to adopt intelligent ransomware detection systems that leverage machine learning and deep learning techniques rather than relying solely on traditional signature-based tools, which are ineffective against zero-day and polymorphic ransomware attacks. Implementing such systems can significantly enhance early detection and prevention capabilities within enterprise networks. Thirdly, it is recommended to software developers and cybersecurity solution providers to develop lightweight, scalable, and real-time ransomware detection applications that can be deployed as services or integrated into existing security infrastructures. Emphasis should be placed on usability, continuous model training, and automated updates to ensure resilience against emerging ransomware threats. Collectively, these recommendations aim to bridge the gap between research and real-world deployment while strengthening ransomware defense mechanisms.

Limitations, Validity, and Credibility

Despite its contributions, this study has certain limitations. The analysis relied on available datasets, which may not fully capture all emerging ransomware variants. Additionally, computational requirements for deep learning models may limit deployment in resource-constrained environments. However, the validity of the study is strengthened through the use of standard evaluation metrics and comparative analysis with existing systems. Credibility is ensured by grounding the findings in established literature, validated models, and empirical results derived from systematic experimentation.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

REFERENCES

Aboshady, D., Ghannam, N. E., Elsayed, E. K., & Diab, L. S. (2023). APKOWL: An Automatic Approach to Enhance the Malware Detection. Mobile Networks and Applications. https://doi.org/10.1007/s11036-023-02159-x

Aboud, M. A., & Mariyappn, K. (2021). Investigation of Modern Ransomware Key Generation Methods: A Review. 2021 International Conference on Computer Communication and Informatics (ICCCI), 1–5. https://doi.org/10.1109/ICCCI50826.2021.9402680

Aidong X., Kai F. & Hang Y. (2018). Power Network Security Technology and Protection. International Symposium on Water System Operations (ISWSO), MATEC Web of Conferences. 246(1), 1-3.

Almomani, I., Alkhayer, A., & El-Shafai, W. (2022). A Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices. Sensors, 22(6), 2281. https://doi.org/10.3390/s22062281

Alrabaee, S., Karbab, E. B., Wang, L., & Debbabi, M. (2019). BinEye: Towards Efficient Binary Authorship Characterization Using Deep Learning (pp. 47–67). https://doi.org/10.1007/978-3-030-29962-0_3

Avci, C., Tekinerdogan, B., & Catal, C. (2023). Analyzing the performance of long short- term memory architectures for malware detection models. Concurrency and Computation: Practice and Experience, 35(6), 1–1. https://doi.org/10.1002/cpe.7581

Badejo O., Jegede O., Kayode H., Durodola O. & Akintoye S. (2018). Modelling And Prediction of Water Current Using Artificial Neural Networks: A Case Study of The Commodore Channel. Nigerian Journal of Technology (NIJOTECH). 39 (3), 942 - 952.

Balabanov T., Zankinski I. & Kolyu K. (2018). Multilayer Perceptron Training Randomized by Second Instance of Multilayer Perceptron. 13th Annual Meeting of the Bulgarian Section of SIAM (Society for Industrial and Applied Mathematics). 14, 2 – 5.

Balachandra K. (2021). Artificial Intelligence in Data Mining: Theories and Applications. Elsevier Inc. Academic Press. DOI:10.1016/C2019-0-01255-1

Baldwin, J., & Dehghantanha, A. (2018). Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware. In Advances In Information Security (pp. 107–136). https://doi.org/10.1007/978-3-319-73951-9_6

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Barwise, I. (2018). Digital steganography as an advanced malware detection evasion technique. Retrieved from https://medium.com/@IanBarwise/digital-steganography-as-an-advancedmalware-detection-evasion-technique-40d4eeb19830

Camille S., Christopher K. and Ole V., (2020). Ransomware 2020: Attack Trends Affecting Organizations Worldwide. Retrieved from: https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

Cen, M., Jiang, F., & Doss, R. (2024). RansoGuard: A RNN-based framework leveraging pre-attack sensitive APIs for early ransomware detection. In Computers & Security (Vol. 150, p. 104293). Elsevier BV. https://doi.org/10.1016/j.cose.2024.104293

Chakraborty S. (2023). Android Ransomware Detection, [Data set]. Kaggle. https://doi.org/10.34740/KAGGLE/DSV/4987535

Chen, J., Wang, C., Zhao, Z., Chen, K., Du, R., & Ahn, G.-J. (2018). Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection. IEEE Transactions on Information Forensics and Security, 13(5), 1286–1300. https://doi.org/10.1109/TIFS.2017.2787905

Clarke, D. J. B., Jeon, M., Stein, D. J., Moiseyev, N., Kropiwnicki, E., Dai, C., Xie, Z., Wojciechowicz, M. L., Litz, S., Hom, J., Evangelista, J. E., Goldman, L., Zhang, S., Yoon, C., Ahamed, T., Bhuiyan, S., Cheng, M., Karam, J., Jagodnik, K. M., … Ma'ayan, A. (2021). Appyters: Turning Jupyter Notebooks into data-driven web apps. Patterns, 2(3), 100213. https://doi.org/10.1016/j.patter.2021.100213

Farhat, D., & Awan, M. S. (2021). A Brief Survey on Ransomware with the Perspective of Internet Security Threat Reports. 2021 9th International Symposium on Digital Forensics and Security (ISDFS), 1–6. https://doi.org/10.1109/ISDFS52919.2021.9486348

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. https://doi.org/10.3390/iot1020030

Fleischer, Y., Biehler, R., & Schulte, C. (2022). Teaching and learning data-driven machine learning with educationally designed jupyter notebooks. Statistics education research journal, 21(2), 7. https://doi.org/10.52041/serj.v21i2.61

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Genç, Z. A., Lenzini, G., & Ryan, P. Y. A. (2018). No Random, No Ransom: A Key to Stop Cryptographic Ransomware. In Lecture Notes In Computer Science (pp. 234–255). https://doi.org/10.1007/978-3-319-93411-2_11

Geman, S., Bienenstock, E., & Doursat, R. (1992). Neural Networks and the Bias/Variance Dilemma. Neural Computation, 4(1), 1–58. https://doi.org/10.1162/neco.1992.4.1.1

Gibson, C. P., & Banik, S. M. (2017). Analyzing the Effect of Ransomware Attacks on Different Industries. 2017 International Conference on Computational Science and Computational Intelligence (CSCI), 121–126. https://doi.org/10.1109/CSCI.2017.20

Herrera-Silva, J. A., & Hernández-Álvarez, M. (2023). Dynamic Feature Dataset for Ransomware Detection Using Machine Learning Algorithms. Sensors, 23(3), 1053. https://doi.org/10.3390/s23031053

Hsu, F., Chen, H., Ristenpart, T., Li, J., & Su, Z. (2006). Back to the Future: A Framework for Automatic Malware Removal and System Repair. 2006 22nd Annual Computer Security Applications Conference (ACSAC'06), 257–268. https://doi.org/10.1109/ACSAC.2006.16

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science, 10, 1772. https://doi.org/10.7717/peerj-cs.1772

Jaiswal M. (2014). IP Security architecture, application, associated database, and mode. International Journal of Research and Analytical Reviews (IJRAR), 1(1), 446-453.

Jha, S., Prashar, D., Long, H. V., & Taniar, D. (2020). Recurrent neural network for detecting malware. Computers & Security, 99, 102037. https://doi.org/10.1016/j.cose.2020.102037

Johnson, S., Gowtham, R., & Nair, A. R. (2022). Ensemble Model Ransomware Classification: A Static Analysis-based Approach. In Lecture Notes In Networks And Systems (pp. 153–167). https://doi.org/10.1007/978-981-16-6723-7_12

Julia G. (2022). Mathematical Neural Networks. Multidisciplinary Digital Publishing Institute (MDPI). 11 (80). 22-38. doi.org/10.3390/axioms11020080.

Kamboj, A., Kumar, P., Bairwa, A. K., & Joshi, S. (2023). Detection of malware in downloaded files using various machine learning models. Egyptian Informatics Journal, 24(1), 81–94. https://doi.org/10.1016/j.eij.2022.12.002

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Kamil, S., Siti Norul, H. S. A., Firdaus, A., & Usman, O. L. (2022). The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. 2022 International Conference on Business Analytics for Technology and Security (ICBATS), 1–7. https://doi.org/10.1109/ICBATS54253.2022.9759000

Karbab, E. B., Debbabi, M., Derhab, A., & Mouheb, D. (2018). MalDozer: Automatic framework for android malware detection using deep learning. Digital Investigation, 24, S48–S59. https://doi.org/10.1016/j.diin.2018.01.007

Lee, J., & Lee, K. (2022). A Method for Neutralizing Entropy Measurement-Based Ransomware Detection Technologies Using Encoding Algorithms. Entropy, 24(2), 239. https://doi.org/10.3390/e24020239

Lee, K., Lee, S.-Y., & Yim, K. (2019). Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems. IEEE Access, 7, 110205–110215. https://doi.org/10.1109/ACCESS.2019.2931136

Li, Y., Xu, Y., Cao, Y., Hou, J., Wang, C., Guo, W., Li, X., Xin, Y., Liu, Z., & Cui, L. (2022). One-Class LSTM Network for Anomalous Network Traffic Detection. Applied Sciences, 12(10), 5051.

Maestre Vidal, J., Sotelo Monge, M. A., Martinez Monterrubio, S. M., Barona Lopez, L. I., & Valdivieso Caraguay, A. L. (2019). Profits at the Dawn of Cybercrime-as-a-Service. 2019 International Conference on Information Systems and Software Technologies (ICI2ST), 71–78. https://doi.org/10.1109/ICI2ST.2019.00017

Masum, M., Jobair Hossain Faruk, M., Shahriar, H., Qian, K., Lo, D., & Islam Adnan, M. (2023). Ransomware Classification and Detection With Machine Learning Algorithms. *School of Data Science, Kennesaw State University*.

Matthew R. (2021). Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Advances in Information Security George Mason University, Fairfax, VA, USA. Springer Nature Switzerland AG. ISBN 978-3-030-66582-

Maurya A., Kumar N., Alka A., & Raees A. (2018). Ransomware Evolution, Target and Safety Measures. International Journal of Computer Sciences and Engineering (IJCSE). 6(1), 80-85

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Modesta E. E. & Ifeyinwa N. N. (2016). Network Security and Privacy in Medium Scale Businesses in Nigeria. International Journal of Advanced Engineering, Management and Science (IJAEMS). 2(9), 1484-1488.

Mudzfirah A., Azizi A. & Khairul A. (2019). Recurrent Neural Network for Malware Detection. International Journal for Advance Software Computer Application (IJASCA), 11 (1), 46-63.

Negrini, L., Shabadi, G., & Urban, C. (2023). Static Analysis of Data Transformations in Jupyter Notebooks. Proceedings of the 12th ACM SIGPLAN International Workshop on the State Of the Art in Program Analysis, 8–13. https://doi.org/10.1145/3589250.3596145

Oghenekaro L. & Ugwu C. (2016). A Novel Machine Learning Approach to Credit Card Fraud Detection. International Journal of Computer Applications (IJCA). 140 (5), 45 – 50.

Onyeoma C. F., Rafiq H., Jeremiah D., Ta T. V., Usman M. (2024). Credit Card Fraud Detection Using Deep Neural Network with Shapley Additive Explanations. Department of Computer Science, Edge Hill University Ormskirk, UK

Pant, D., & Bista, R. (2021). Image-based Malware Classification using Deep Convolutional Neural Network and Transfer Learning. Proceedings of the 3rd International Conference on Advanced Information Science and System, 1–6. https://doi.org/10.1145/3503047.3503081

Patel, A., & Tailor, J. (2020). A malicious activity monitoring mechanism to detect and prevent ransomware. Computer Fraud & Security, 2020(1), 14–19. https://doi.org/10.1016/S1361-3723(20)30009-9

Pei H., Song K. and Zhu T., (2022). Speech recognition method based on DNN-LSTM combined with Wiener filtering algorithm, 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), Dali, China, 4, 1467-1472.

Pushpendra D. and Hariom S., (2021). Analysis and Detection of Evolutionary Malware: A Review. International Journal of Computer Applications (IJCA). 174 (20), 42 – 45.

Raizza, A., & Algarni, A. (2023). Ransomware Detection using Machine Learning: Survey. *Preprints.Org* , 10–29.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

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. https://doi.org/10.1016/j.jjimei.2021.100013

Rustam, F., Ashraf, I., Jurcut, A. D., Bashir, A. K., & Zikria, Y. Bin. (2023). Malware detection using image representation of malware data and transfer learning. Journal of Parallel and Distributed Computing, 172, 32–50. https://doi.org/10.1016/j.jpdc.2022.10.001

Sachin B., Yogeshkumar S. & Sahil J. (2021). Research Paper on Modern Network Security: Issues and Challenges. Emerging Advancement and Challenges in Science, Technology and Management, Contemporary Research in India (ISSN 2231-2137). 215-219.

Sangher, K. S., Singh, A., & Pandey, H. M. (2023). Signature based ransomware detection based on optimizations approaches using RandomClassifier and CNN algorithms. International Journal of System Assurance Engineering and Management. https://doi.org/10.1007/s13198-023-02017-9

Schonlau, M., & Zou, R. Y. (2020). The random forest algorithm for statistical learning. The Stata Journal: Promoting Communications on Statistics and Stata, 20(1), 3–29. https://doi.org/10.1177/1536867x20909688

Sekhar C. & Meghana P. (2020). A Study on Backpropagation in Artificial Neural Networks. Asia-Pacific Journal of Neural Networks and Its Applications. 4 (1), 21-28.

Shawon, R. & Alain, L. (2021). Security Professionals Must Reinforce Detect Attacks to Avoid Unauthorized Data Exposure. INFORMATION TECHNOLOGY IN INDUSTRY, 8(1). https://doi.org/10.17762/itii.v8i1.76

Shenoy, A., & Appel, J. M. (2017). Safeguarding Confidentiality in Electronic Health Records. Cambridge Quarterly of Healthcare Ethics, 26(2), 337–341. https://doi.org/10.1017/S0963180116000931

Stiawan, D., Daely, S. M., Heryanto, A., Afifah, N., Idris, M. Y., & Budiarto, R. (2021). Ransomware Detection Based On Opcode Behavior Using K-Nearest Neighbors Algorithm. Information Technology and Control, 50(3), 495–506. https://doi.org/10.5755/j01.itc.50.3.25816

Subedi K. P., Daya R. B., Chenx B. & Dasguptaz D. (2017). Ransomware Defense Strategy by Using Stealthily Spare Space. IEEE Symposium Series on Computational Intelligence (SSCI),3 (20), 1-8.

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Takeuchi, Y., Sakai, K., & Fukumoto, S. (2018). Detecting Ransomware using Support Vector Machines. Proceedings of the 47th International Conference on Parallel Processing Companion, 1–6. https://doi.org/10.1145/3229710.3229726

Tommaso Z., Andrea C. & Andrea B. (2021). Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application. Institute of Electrical and Electronics Engineers (IEEE), University of Florence – 50134 Florence, Italy. 34 (4), 54 – 67.

Torres-Calderon, H., Velasquez, M., & Mauricio, D. (2022). Method for Designing Countermeasures for Crypto-Ransomware Based on the NIST CSF. In Smart Innovation, Systems And Technologies (pp. 365–380). https://doi.org/10.1007/978-981-16-3637-0_26

Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Computers & Security, 81, 123–147. https://doi.org/10.1016/j.cose.2018.11.001

Ugwu C. & Onwuachu C. (2014). A Hybrid Factor Based Neural Network Model Application for Stock Price Prediction, International Journal of Engineering Research & Technology (IJERT), 3 (4), 2721 – 2730.

Vidyarthi D., Kumar C., Subrata R. & Shailesh C. (2019). Identifying Ransomware - Specific Properties using Static Analysis of Executables. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE). 8 (4), 358 - 368. https://doi.org/10.17148/IJARCCE.2019.8461

Volpe, G., Fiore, M., la Grasta, A., Albano, F., Stefanizzi, S., Mongiello, M., & Mangini, A. M. (2024). A Petri Net and LSTM Hybrid Approach for Intrusion Detection Systems in Enterprise Networks. Sensors, 24(24), 7924.

Waleed K. & Sivaram P. (2017). Activity Based Costing System. International Journal of Recent Scientific Research. 8 (7), 18288-18306. DOI: 10.24327/IJRSR

Wenfu Y. (2020). Computer Information Network Security Technology and Security Precaution Measures Based on Computer. Malaysian Society for Automatic Control Engineers (MACE), Journal of Physics: Conference Series. 1744(1), 259-268. doi:10.1088/1742-6596/1744/4/042008

Wentao Y., Sai W. & Chengyuan W., (2019). The realization of network security technology based on cloud computing environment. International Conference on Computer Information Science and Application Technology (CISAT), 1345(520), 1-8. doi:10.1088/1742-6596/1345/5/0520222

ISSN: 3121 - 6765 | https://ijois.com/index.php/ijrrsas | VOLUME 2. ISSUE 1. (NOVEMBER, 2025)

Wu, X., Gao, Y., & Jiao, D. (2019). Multi-Label Classification Based on Random Forest Algorithm for Non-Intrusive Load Monitoring System. Processes, 7(6), 337. https://doi.org/10.3390/pr7060337

Yamany, B., Elsayed, M. S., Jurcut, A. D., Abdelbaki, N., & Azer, M. A. (2022). A New Scheme for Ransomware Classification and Clustering Using Static Features. *Electronics*, *11*(20), 3307. https://doi.org/10.3390/electronics11203307

Yamany, B. E. M., & Azer, M. A. (2021). SALAM Ransomware Behavior Analysis Challenges and Decryption. 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS), 273–277. https://doi.org/10.1109/ICICIS52592.2021.9694154

Yin, H., Song, D., Egele, M., Kruegel, C., & Kirda, E. (2007). Panorama. Proceedings of the 14th ACM Conference on Computer and Communications Security, 116–127. https://doi.org/10.1145/1315245.1315261

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. https://doi.org/10.1038/s41598-022-19443-7

Zhang T., Antunes H. & Aggarwal S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. IEEE Internet Things. 1(1), 10–21.

Zhao, H., Sun, S., & Jin, B. (2018). Sequential Fault Diagnosis Based on LSTM Neural Network. IEEE Access, 6, 12929–12939.

Zheng C., Dellarocca N., Andronio N., Zanero S. & Maggi F. (2016) GreatEatlon: Fast, static detection of mobile ransomware. International Conference on Security and Privacy in Communication Systems (ICSPCS), Guangzhou, China, 10 (12), 617–636.