International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

Role of Machine Learning in the Development of a Ransomware Detection Framework: A Review

Research Scholar Mr. Narender Kumar, Associate Professor Dr. Pramod Kumar
Department of Computer Science & Engineering, Ganga Institute of Technology & Management, V.P.O. Kablana, Jhajjar , Haryana.

Abstract — The primary objective of this research is to develop and evaluate an effective machine learning-based framework for the early detection of ransomware attacks. The study investigates a range of machine learning techniques, including supervised classification, anomaly detection, and clustering methods, to distinguish ransomware activities from legitimate system behavior. It focuses on extracting and analyzing critical behavioral features such as file access patterns, process execution characteristics, and network communication activities to train predictive models capable of achieving high detection accuracy while minimizing false positive rates.

Keywords— Behaviour, Machine Learning, Ransomware, Cyber security, Encryption etc

I. INTRODUCTION

Machine Learning provides the ability to learn from data, detect anomalies, and predict threats by analyzing complex patterns in system behaviour. ML algorithms can be trained on features such as file activity, CPU usage, system calls, and network traffic to distinguish between normal and malicious operations. This data-driven approach enables the early identification of ransomware attacks, including zero-day variants that exhibit behaviours not seen before. Given this backdrop, the integration of machine learning into ransomware detection frameworks has garnered increasing research interest. The goal is not only to improve detection accuracy but also to reduce false positives and provide scalable, real-time protection across diverse computing environments. This research builds on these efforts by analyzing the effectiveness of various ML models and designing an optimized detection technique capable of identifying ransomware activities at an early stage.

Ransomware is a form of malware that encrypts a victim's files or systems and demands a ransom payment for their release. Attackers often threaten to publish sensitive data or permanently lock access unless payment is made. Ransomware can spread through phishing emails, malicious websites, or infected software. Variants such as WannaCry, Petya, and Ryuk have caused widespread disruption across sectors.Ransomware detection is a critical component of modern cybersecurity strategies, aimed at identifying and mitigating ransomware threats before they can cause irreversible damage to digital systems and data. As ransomware attacks become increasingly sophisticated and stealthy, traditional detection mechanisms—often reliant on static signatures or known threat patterns—struggle to keep up with the rapid evolution of malware variants. Consequently, there is a growing emphasis on intelligent, proactive detection methods capable of identifying both known and novel ransomware behaviors. Effective ransomware detection typically involves monitoring system activities, analyzing behavioral patterns, and recognizing deviations that suggest malicious intent. These activities may include unusual file encryption behavior, rapid file modifications, unauthorized access attempts, and suspicious network communication. However, due to the evolving nature of ransomware, relying solely on predefined rules or databases of known malware signatures is no longer sufficient.

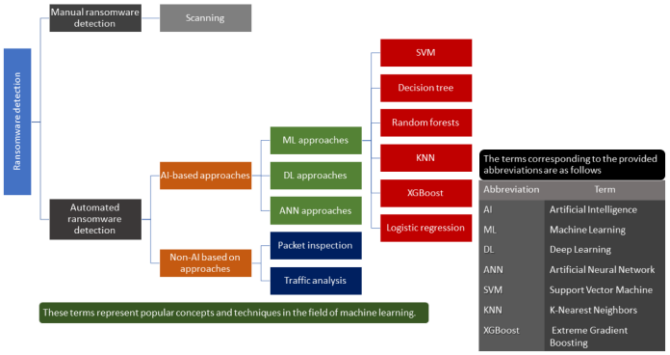

Figure 1. Integration of Machine Learning in Ransomware Detection Pipeline

To address these limitations, Machine Learning (ML) has emerged as a powerful tool in ransomware detection. ML-based detection systems can be trained on large datasets containing both benign and malicious activity, enabling them to learn and generalize patterns associated with ransomware attacks.

There are two main approaches to ML-based ransomware detection:

- Static Analysis: This method involves analyzing files without executing them, often by extracting features from code structure, byte sequences, and metadata. While fast and resource-efficient, static analysis may be evaded by obfuscated or polymorphic ransomware.
- Dynamic Analysis: This approach monitors the behavior of files or processes during execution in a controlled environment (sandbox). It is more effective at detecting unknown threats but is resource-intensive and slower compared to static methods.

Advanced ML techniques, including supervised learning (e.g., Random Forest, Support Vector Machines), unsupervised learning (e.g., clustering, anomaly detection), and deep learning (e.g., LSTM, CNNs), have shown significant promise in detecting ransomware. These models can be integrated into host-based intrusion detection systems (HIDS), network monitoring tools, or cloud-based security platforms to provide real-time threat intelligence and response capabilities.

This research aims to analyze the effectiveness of these machine learning approaches and design a robust ransomware detection model that balances accuracy, speed, and adaptability. The ultimate goal is to create a scalable solution capable of identifying emerging threats before data loss or encryption occurs, thereby strengthening the overall cybersecurity posture of digital environments. Ransomware is a type of malware attack in which the attacker locks and encrypts the victim's data, important files and demands a payment to unlock and decrypt the data. This type of attack takes advantage of human, system, network, and software vulnerabilities to infect the victim's device- which can be a computer, printer, Smartphone and other endpoint. Nowadays, the attackers use intelligent techniques to create new profitable malware type. One of these attacks which highly spread recently is ransomware. Ransomware is irreversible and difficult to stop not like other security problems. Ransomware is a type of malware that restricts access to the infected computer system and it has generated much interest from cybercriminals because of its successful attack and direct financial interest. Malware objective is to block its victim from accessing their own resources by locking the OS or encrypting targeted files that seem valuable in the victim, such as images, spreadsheets and presentations. It is used to digitally extort victims into payment of a specific fee. This type of digital extortion can be broadly classified into two main categories, which can then be further divided into subcategories based on the families they represent. The two main types of ransomware are those that lock people out of their system of restrict access to them, and those that encrypt, obscure, or restrict access to files. These dangers can affect any number of devices and is not restricted to any particular type of operating system. Your Winders PCs, iOS devices and Android devices are all susceptible to this kind of ransomware exploitation.

The rate of cyber-attacks has increased as a result of the COVID-19 epidemic. Attackers used phishing emails with COVID-19 themed ransomware to target people into paying some ransom amount as the paradigm of workplace leads to work from home scenario leading to more vulnerability of these people and thus ending into giving important information or private banking details from their home laptop or PCs. For instance, numerous phishing efforts instructed users to click particular URLs to access private information about a COVID 19 vaccine, surgical mask scarcity, etc. False COVID-19-related information was affectively used as a hook by attackers to start effective phishing attempts. Another issue that drives people to engage in cybercrime, such as initiating ransomware attacks and interrupting vital IT services, in order to support themselves is highly unemployment rates.In locker ransomware, the access to the victim's device is blocked by generally locking the display or the keyboard. Instead, crypto-ransomware blocks the access to the information on the device by ciphering the victim's files and documents. In both cases, an economical ransom is demanded to the victim to restore the normal access to the locked devices. Locker-ransomware can be easily dismantled through various systems, restore techniques and tools.Scareware may use pop-up ads to manipulate users into thinking that they need to install additional software to work with a certain application efficiently or to open a file, thereby using coercion techniques for downloading malware. In scareware, the cyber crooks exploit the fear rather than lock the device or encrypt any data.
Types of Ransomware Detection Techniques

Ransomware detection techniques can be broadly categorized based on the underlying methodology and the stage at which detection occurs. Each technique offers distinct advantages and limitations, and their effectiveness often depends on the type of ransomware and the system environment. The major types of ransomware detection techniques are as follows:

Signature-Based Detection
Signature-based detection is one of the earliest and most widely used methods in traditional antivirus solutions. It relies on identifying known patterns or "signatures" of malware by scanning files for specific byte sequences or hash values.

- Advantages: Fast and accurate for known ransomware variants.
- Limitations: Ineffective against new, unknown (zero-day), or obfuscated ransomware. Requires constant updating of signature databases.

Heuristic-Based Detection

- Heuristic detection uses predefined rules or algorithms to detect suspicious behaviors that may indicate ransomware activity, such as rapid file encryption or unauthorized system access.
- Advantages: Can detect previously unseen variants by identifying suspicious patterns.
- Limitations: High false-positive rates; attackers can bypass heuristics by mimicking legitimate behavior.

Behavior-Based Detection

Behavior-based detection monitors system activities in real time to detect anomalous actions typically associated with ransomware, such as mass file renaming, high CPU usage, or unusual network traffic.

- Advantages: Effective against unknown or polymorphic ransomware; capable of early detection.
- Limitations: Requires continuous monitoring and can generate false alarms; may impact system performance.

Machine Learning-Based Detection

Machine learning (ML)-based detection employs algorithms that learn from labeled or unlabeled data to distinguish between normal and malicious behavior. ML models can be trained on various system-level features such as file access patterns, process behavior, and network traffic.

- Advantages: Adaptive, scalable, and effective against zero-day ransomware; improves over time with more data.
- Limitations: Requires large datasets for training; performance depends on feature selection and model tuning.

II. STATIC ANALYSIS

Static analysis examines files without executing them. It involves analyzing code structure, embedded resources, and metadata to identify malicious intent.

- Advantages: Fast, low resource usage, and safe (no execution required).
- Limitations: Can be bypassed through obfuscation and packing techniques.

Dynamic Analysis

Dynamic analysis involves executing a suspicious file in a controlled environment (sandbox) to observe its behavior. This method detects ransomware based on real-time actions such as file encryption or registry modification.

- Advantages: Effective at detecting complex, obfuscated ransomware.
- Limitations: Time-consuming, resource-intensive, and susceptible to sandbox evasion tactics.

Hybrid Detection Techniques

Hybrid techniques combine two or more detection methods (e.g., static + dynamic, heuristic + ML) to leverage the strengths of each while minimizing individual weaknesses.

- Advantages: Provides balanced accuracy and coverage; enhances detection robustness.
- Limitations: Higher computational cost and complexity in integration and management.

These detection techniques form the foundation of modern anti-ransomware solutions. In recent years, machine learning-based and hybrid detection approaches have shown superior performance, especially in handling sophisticated and unknown ransomware variants. This research focuses on analyzing and designing an optimized ML-based detection framework to address the limitations of existing methods and provide a more effective ransomware defense mechanism.

Types of Machine Learning Model used Ransomware Detection

Various machine learning (ML) models have been utilized for ransomware detection, each with unique capabilities to analyze, classify, and predict malicious behavior. The effectiveness of these models largely depends on the nature of the dataset, feature selection, and the complexity of the ransomware variant. Below are the most commonly used ML models for ransomware detection:

Decision Tree (DT)

A Decision Tree is a simple yet powerful model that uses a tree-like structure to make decisions based on feature values. It works by splitting the data into subsets based on the value of input features.

- Advantages: Easy to interpret, fast training, handles both numerical and categorical data.
- Limitations: Prone to overfitting; may not generalize well without pruning.
- Use Case: Ideal for early-stage detection using process behavior logs or file access patterns.

Random Forest (RF)

Random Forest is an ensemble method based on multiple decision trees. It combines the results of many trees to improve accuracy and robustness.

- Advantages: High accuracy, resistant to overfitting, handles large datasets.

- Limitations: Slower training; less interpretable than a single tree.
- Use Case: Suitable for behavioral analysis of ransomware across multiple features.

Support Vector Machine (SVM)
SVM is a supervised learning algorithm used for binary classification. It finds the hyperplane that best separates the data into ransomware and non-ransomware classes.

- Advantages: Effective in high-dimensional spaces, robust to outliers.
- Limitations: Requires careful parameter tuning; slow for large datasets.
- Use Case: Efficient for detecting ransomware based on system call sequences.

K-Nearest Neighbors (KNN)
KNN classifies a sample based on the majority vote of its 'k' nearest neighbors in the feature space.

- Advantages: Simple, effective with small datasets.
- Limitations: Computationally expensive; sensitive to noisy data.
- Use Case: Used in lightweight detection systems where rapid deployment is needed.

Naïve Bayes (NB)
Naïve Bayes is a probabilistic classifier based on Bayes' theorem with the assumption of feature independence.

- Advantages: Fast training and prediction, performs well with limited data.
- Limitations: Assumes feature independence, which may not hold in real-world data.
- Use Case: Useful in classifying ransomware emails or social engineering attack vectors.

Artificial Neural Networks (ANN)
ANNs are inspired by the structure of the human brain and can model complex non-linear relationships in data.

- Advantages: Capable of learning intricate patterns, scalable to large data.
- Limitations: Requires large training datasets, less interpretable.
- Use Case: Effective for detecting advanced and polymorphic ransomware through behavioral analysis.

Convolutional Neural Networks (CNN)
Though originally used for image data, CNNs can also be adapted to detect ransomware by analyzing system activity graphs or encoded binary sequences.

- Advantages: Excellent at recognizing patterns in structured inputs.
- Limitations: Requires pre-processed input formats.
- Use Case: Suitable for detecting fileless ransomware from memory images.

Recurrent Neural Networks (RNN) and LSTM
RNNs, particularly LSTM networks, are ideal for analyzing sequential data like system logs, API call sequences, or user activity patterns.

- Advantages: Can learn temporal dependencies; suitable for time-series data.
- Limitations: Complex architecture; slow training.
- Use Case: Highly effective for real-time ransomware detection based on behavior over time.

III. ROLE OF MACHINE LEARNING IN RANSOMWARE DETECTION

The rapid growth of digital technologies and interconnected computing environments has significantly increased the prevalence of ransomware attacks. Modern ransomware has evolved beyond conventional malware by employing advanced techniques such as encryption, code obfuscation, polymorphism, and fileless execution, making it increasingly difficult for traditional signature-based and rule-based security solutions to provide effective protection. Since conventional antivirus systems rely primarily on known malware signatures, they often fail to identify newly emerging or modified ransomware variants. Consequently, there is a growing need for intelligent detection mechanisms capable of recognizing previously unseen attacks through behavioural analysis rather than static signatures.

Machine Learning (ML) has emerged as a powerful technology for addressing these challenges by enabling automated, adaptive, and data-driven ransomware detection. Instead of relying solely on predefined rules, ML algorithms learn from historical system data to identify complex relationships and behavioral patterns associated with malicious activities. This capability allows ML-based systems to detect both known and unknown ransomware variants with improved accuracy, making them highly suitable for modern cyber security applications.

Behavioral Analysis of Ransomware
One of the most significant advantages of Machine Learning is its ability to perform behavioral analysis. Rather than examining only the static characteristics of executable files, ML algorithms monitor how applications interact with the operating

system during execution. Ransomware typically exhibits distinctive behavioral characteristics that differentiate it from legitimate software. These behaviors include rapid encryption of multiple files, abnormal file access sequences, unauthorized registry modifications, suspicious process creation, unusual memory utilization, and unexpected network communications. Machine learning models are trained using datasets containing both benign and malicious system activities. During training, the algorithms learn normal operating behavior and identify deviations that may indicate ransomware activity. Features commonly analyzed include:

- File creation, deletion, and modification patterns
- Registry modifications and persistence mechanisms
- Process execution behavior and parent-child process relationships
- Memory allocation and consumption patterns
- Network traffic characteristics and communication with remote servers
- System call sequences generated during program execution

By analyzing these behavioral attributes, ML models can accurately distinguish malicious activities from legitimate system operations even when ransomware employs sophisticated evasion techniques.

IV. REAL-TIME DETECTION AND EARLY RESPONSE

Traditional security solutions often detect ransomware only after file encryption has already commenced, resulting in irreversible data loss. In contrast, Machine Learning enables continuous monitoring of system activities, allowing suspicious behavior to be identified during the early stages of an attack.

Real-time detection systems continuously evaluate incoming system events and compare them with learned behavioral models. When suspicious activities exceed predefined confidence thresholds, immediate defensive actions can be initiated. These actions may include:

- Early identification of ransomware behavior before widespread encryption
- Immediate termination of malicious processes
- Isolation or quarantine of infected files and applications
- Automatic blocking of unauthorized network communications
- Alert generation for system administrators
- Preservation of forensic evidence for incident investigation

Such proactive response mechanisms significantly reduce the impact of ransomware attacks and minimize organizational downtime.

Adaptive Learning and Continuous Improvement

The dynamic nature of ransomware presents a major challenge for conventional cybersecurity systems. Cybercriminals continuously modify malware code, employ obfuscation techniques, and develop new attack strategies to evade detection. Machine Learning addresses this challenge through its ability to adapt and improve over time.ML models can be periodically retrained using newly collected ransomware samples and updated benign datasets. This continuous learning process enables the detection system to recognize evolving attack patterns and maintain high detection performance against emerging threats.

Adaptive learning is particularly valuable for identifying advanced ransomware variants, including:

- Polymorphic ransomware that modifies its code structure while maintaining the same functionality
- Metamorphic ransomware capable of completely rewriting its internal code
- Fileless ransomware that executes directly in system memory without creating executable files on disk
- Obfuscated malware specifically designed to bypass traditional antivirus signatures
- Zero-day ransomware exploiting previously unknown software vulnerabilities

By continuously learning from new attack patterns, ML-based systems remain effective even as ransomware techniques evolve.

Feature Extraction and Intelligent Pattern Recognition

Feature extraction represents one of the most critical stages in Machine Learning-based ransomware detection. The effectiveness of an ML model depends largely on the quality and relevance of the features used during training.

Modern ransomware detection systems analyze a wide variety of static and dynamic features, including:

- File entropy indicating encryption activity
- File size and extension modifications
- Frequency of file access operations
- CPU, memory, and disk utilization
- System call sequences
- Process execution timelines
- Registry modification events
- Network packet statistics

- User privilege escalation attempts
- Command execution behavior

Machine Learning algorithms identify complex correlations among these features that are often difficult for human analysts or rule-based systems to recognize. This multidimensional analysis substantially improves detection accuracy while reducing the likelihood of false alarms.

V. MACHINE LEARNING ALGORITHMS FOR RANSOMWARE DETECTION

Several Machine Learning algorithms have demonstrated strong performance in ransomware detection, each offering unique advantages depending on the nature of the available data.

Supervised learning algorithms, including Decision Trees, Random Forests, Support Vector Machines (SVM), Logistic Regression, Naïve Bayes, and Artificial Neural Networks, are trained using labeled datasets containing both ransomware and benign samples. These algorithms classify unknown applications based on previously learned patterns.

Unsupervised learning techniques, such as K-Means Clustering, DBSCAN, and Hierarchical Clustering, identify abnormal behaviors without requiring labeled training data. These methods are particularly useful for detecting novel ransomware variants that have not previously been encountered.

Deep Learning approaches, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders, automatically learn complex feature representations from large datasets. These models are especially effective in recognizing sophisticated ransomware behaviours involving sequential system events. Ensemble learning methods combine multiple algorithms to improve prediction accuracy, robustness, and generalization capability.

Integration with Modern Cyber security Infrastructure
Machine Learning-based ransomware detection systems can be seamlessly integrated into existing cybersecurity infrastructures to provide comprehensive protection across enterprise environments. Such integration enhances threat visibility, automates response mechanisms, and supports centralized security management.

These systems can operate alongside:

- Host-based Intrusion Detection Systems (HIDS)
- Network Intrusion Detection Systems (NIDS)
- Endpoint Detection and Response (EDR) platforms
- Security Information and Event Management (SIEM) systems
- Extended Detection and Response (XDR) solutions
- Cloud security platforms
- Security Orchestration, Automation, and Response (SOAR) frameworks

The combination of ML with these technologies enables continuous monitoring, rapid threat intelligence sharing, automated incident response, and improved organizational resilience against ransomware attacks.

Improved Detection Accuracy and Reduced False Alarms
An important objective of ransomware detection systems is to maximize detection accuracy while minimizing false positive and false negative rates. Excessive false positives may interrupt legitimate user activities, whereas false negatives allow malicious software to evade detection.Properly trained Machine Learning models effectively balance sensitivity and specificity by learning the distinguishing characteristics of both malicious and benign behaviours. Performance is commonly evaluated using metrics such as:

- Accuracy
- Precision
- Recall (Detection Rate)
- F1-Score
- Receiver Operating Characteristic (ROC) Curve
- Area Under the Curve (AUC)
- False Positive Rate
- False Negative Rate

High-performing models ensure reliable ransomware detection while maintaining an acceptable user experience and minimizing unnecessary security alerts.

Challenges and Future Directions
Despite its numerous advantages, Machine Learning-based ransomware detection also faces several challenges. High-quality labeled datasets are often limited, and class imbalance can adversely affect model performance. Adversarial attacks may manipulate input features to deceive ML models, while computational overhead may hinder deployment in resource-constrained environments. Furthermore, ensuring explainability and transparency remains an important consideration, particularly for critical security applications.

Future research is expected to focus on Explainable Artificial Intelligence (XAI), Federated Learning, Online Learning, Transfer Learning, Reinforcement Learning, and Hybrid Deep Learning models capable of providing more accurate, interpretable, and scalable ransomware detection in dynamic computing environments.

VI. CONCLUSION

Machine Learning has fundamentally transformed the field of ransomware detection by introducing intelligent, adaptive, and behaviour based security mechanisms capable of identifying both known and previously unseen ransomware variants. Through behavioral analysis, real-time monitoring, intelligent feature extraction, continuous learning, and seamless integration with modern cyber security frameworks, ML significantly enhances an organization's ability to detect and mitigate ransomware attacks at an early stage.The proposed research seeks to leverage these capabilities to design a robust, scalable, and real-time Machine Learning-based ransomware detection framework that achieves high detection accuracy, minimizes false positives, and provides effective protection against the continuously evolving landscape of ransomware threats.

REFERENCES

1. Madani, H. Ouerdi, N.,Boumesaoud. A.et al. Classification of ransomware using different types of neural networks.Sci Rep 12, 4770 (2022).https//doi.org/10.1038/s41598-022-08504-6
2. Sharmeen. S: Ahmed. Y.A.; Huda, S.; Kocer, B. S Hassan, M.M. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access 2020,8, 24522-24534.
3. Abukar Ahmed Yahye, Shamsul Huda , Bander Ali Saleh Al-rimy , Nouf Alharbi , Faisal Saeed , Fuad A. Ghaleb and Ismail Mohamed Ali “A Weighted Minimum Redundancy Maximum Relevance Technique for Ransomware Early Detection in Industrial IoT” 2022, pp 3-5.
4. Ahmed, Y.A.; Koçer, B.; Huda, S., Al-rimy, B.A.S.; Hassan, M.M. A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection.J. Netw.Comput. Appl. 2020, 167, 102753.
5. Ali, Azad. "Ransomware: a research and a personal case study of dealing with this nasty malware." Issues in Informing Science & Information Technology, vol. 14, annual 2017, pp.
6. Almomani, L.; Qaddoura, R.; Habib, M.; Alsoghyer, S., Al Khayer, A.; Aljarah, I. Faris, H. Android Ransomware Detection Based on a Hybrid Evolutionary Approach in the Context of Highly Imbalanced Data IEEE Access 2021, 9, 57674-57691.
7. Al-Rimy, B.A.S., Maarof. M.A., Alazab, M., Shahid, S.Z.M., Ghaleb, FA Al Alawi, A. AL, AM, A Hadhrami, T. Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection. Future Gener. Comput. Syst. 2021, 115, 641-658.
8. Alzahrani, N.; Alghazzawi, D. A Review on Android Ransomware Detection Using Deep Learning Techniques. In Proceedings of the 11th International Conference on Management of Digital EcoSystems, Limassol, Cyprus, 12-14 November 2019, pp. 330-335.
9. Anand, P., Singh, Y., Singh, H. et al. SALT: transfer learning-based threat model for attack detection in smart home. Sci Rep 12, 12247 (2022).
10. Andronio, Nicoló, Stefano Zanero, and Federico Maggi. "Heldroid: Dissecting and detecting mobile ransomware." international symposium on recent advances in intrusion detection. Springer, Cham, 2015.
11. Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A. Automated ransomware behavior analysis: Pattern extraction and early detection. In Proceedings of the International Conference on Science of Cyber Security, Nanjing, China, 9-11 August 2019, pp. 199-214.
12. Oz, H. Aris A. Levi, A., Uluagac, A.S. A Survey on Ransomware: Evolution. Taxonomy, and Defense Solutions. arXiv 2021, arXiv:2102.06249.
13. 14.David Akande, Saqib Hakak, Muhammad Khurram Khan. Ransomware: Recent advances, analysis, challenges and future research directions, Computers & Security, Volume 111, December 2021, 102490 pp 2-5.
14. Damien Warren Fernando, Nikos Komninos and Thomas Chen. A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques, 2020, pp 2-5.
15. Firoz Khan; Cornelius Ncube; Lakshmana Kumar Ramasamy; Seifedine Kadry; Yunyoung Nam “A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning” IEEE Access (Volume: 8) June 2020.
16. Hasan, M.; Rahman, M. RansHunt: A Support Vector Machines Based Ransomware Analysis Model(s) with Integrated Feature Set. In 20th International Conference of Computer and Information Technology (ICCTT), Dhaka, Bangladesh, 22-24 December 2017: pp. 1-7.

17. Homayoun, Ali Dehghantanha, Marzieh Ahmadzadeh, Sattar Hashem. Raouf Khayami, Kim-Kwang Raymond Choo. David Deep ransomware threat hunting and intelligence system at the fog layer. Future Generation Computer Systems,Volume 90, January 2019, pp 95-104.
18. Khan, F.; McNube, C.; Lakshmana, R.; Kadry, S.; Nam, Y A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning, IEEE Access 2020, 8, 119710-119719.
19. KoK, Abdullahi A, Jhanjhi, N, Mahadevan Supramaniam, Ransomware, threat and detection techniques: A review. International Journal of Computer Science and Network Security, Vol.19 No.2, February 2019, pp 4-5.
20. Lallie, Harjinder Singh, et al. "Cyber Security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." Computers & Security 105(2021): 102248.
21. Md Jobair Hossain Faruk , Hossain Shahriar , Maria Valero , Farhat Lamia Barsha , Shahriar Sobhan, Md Abdullah Khan, Michael Whitman, Alfredo Cuzzocreak , Dan Lo, Akond Rahman and Fan WU. "Malware Detection and Prevention using Artificial Intelligence Techniques". 2021. pp 2-4.