ISSN 2581 – 3781

AJCSE ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info

Asian Journal of Computer Science Engineering 2025;10(4):1-10

REVIEW ARTICLE

A Survey on Deep Learning-based Ransomware Detection and Prevention in Internet of Things Devices

Sandeep Gupta*

Department of Computer Science, Samrat Ashok Technological Institute, Vidisha, Madhya Pradesh, India

Received on: 12-11-2025; Revised on: 10-04-2026; Accepted on: 02-05-2026

ABSTRACT

The growth of the Internet of Things (IoT) has greatly broadened the scope of connectivity of the system, concurrently expanding the attack surface, and thus, the IoT environments are extremely susceptible to ransomware attacks. Ransomware is life-threatening, with a significant likelihood of causing permanent and catastrophic operational and financial losses by encrypting user data, paralyzing the work of devices, and requiring payment of ransom. The existing security measures, including signature-based and heuristic detection, do not work amicably with modern ransomware because of its polymorphic, adaptive, and insidious nature. In this research, the ransomware threat environment specific to the IoT context is surveyed with detection challenges, publicly available datasets, threats peculiar to the IoT, and the application of feature extraction to intelligent security systems. Moreover, it examines how machine learning and deep learning (DL) methods, such as support vector machines, decision trees, random forests, convolutional neural networks, recurrent neural networks, autoencoders, and hybrid networks, could be used in ransomware detection and prevention. The prevention methods focused on by the paper include DL-powered prevention systems, including behavioral anomaly detection, DL-enhanced intrusion detection systems, temporal prediction models to prevent ransomware in its early stages, lightweight edge-based models, and federated learning systems. Through examining available frameworks, datasets, and model architectures, this survey demonstrates that DL is superior to traditional means of attaining superior accuracy, fewer false alarms, and, in time, avert threats before they occur. The results emphasize the value of privacy-preserving, adaptive, and scalable DL systems to develop robust ransomware prevention systems in resource-limited IoT systems.

Key words: Cybersecurity, deep learning, internet of things, machine learning, ransomware detection

INTRODUCTION

The hyper-connectivity provided by the exponential growth of the Internet of Things (IoT) has brought in a new age of hyper-connectivity where billions of smart devices work together in a home, industrial, healthcare, and critical infrastructure environment. Automation and intelligent decision-making in any contemporary cyber-physical system (CPS) depend on IoT devices, which are constantly gathering, processing, and transferring sensitive data. Nonetheless, this impressive growth has at the same time increased the cyberattack surface, which puts IoT networks under the threat of more advanced attacks.[1] Of these threats, one of the most disruptive and financially destructive forms of cybercrime has become ransomware. Ransomware has the potential to stagnate whole IoT ecosystems by encrypting device data, changing system settings, or stopping the processes of the system, with serious economic, privacy, and safety impacts.

Conventional signature-based and rule-based detectives find it very difficult to cope with the fast-developing ransomware, polymorphic malwares, and 0-day exploits, which are specifically coded to take advantage of the limited security services offered by the IoT devices.[2,3] This is a widening gap in the demand for smart, flexible, and scalable defense mechanisms, which has fueled the desire to integrate artificial intelligence (AI) and, more precisely, deep learning (DL) into IoT security systems. AI presents the potential to process vast volumes of heterogeneous IoT data with

Address for correspondence:
Sandeep Gupta
E-mail: sandeepguptabashu@gmail.com

the capability to identify discrete attack patterns, anticipate malicious actions, and counterattack threats without having to create rules manually.[4,5] The potential of DL, an advanced field of AI, ransomware detection and prevention is especially promising as it can learn feature representations that are high-dimensional and hierarchical directly at the data level. Convolutional neural networks (CNNs), long short-term memory (LSTM) networks, autoencoders, generative adversarial networks (GANs), and Transformer architectures are more effective in detecting subtle behavioral anomalies that could represent ransomware running.[6,7] The DL-based solutions can reveal malicious patterns by analyzing network traffic abnormalities, device activity patterns, application programming interface (API) call patterns, and system logs associations, which the traditional methods cannot identify.

However, DL as a component of the IoT is more of a challenge. The IoT devices are usually limited in terms of computing power, memory, and energy, such that implementing large neural networks is not feasible.[8] To address these limitations, modern studies have considered lightweight DL networks, edge-level AI processing, federated learning, and energy-efficient architectures.[9] The innovations will support decentralized privacy-preserving real-time ransomware defense mechanisms that can perform efficiently in resource-limited IoT settings.

Structure of the Paper

This review systematically examines DL-driven ransomware threat prevention in IoT devices. Section II outlines the ransomware threat landscape in IOT. Section III discusses machine learning and DL in cybersecurity. Section IV focuses on DL-driven ransomware prevention techniques in IOT. Section V summarizes key literature findings, highlighting model performance, accuracy, and existing research gaps. Section VI presents the conclusion and future work.

RANSOMWARE THREAT LANDSCAPE IN IOT

Ransomware detection methods have relied on several key strategies. Signature-based detection is the most common method used in traditional antivirus software. It matches known malware signatures, unique strings of data, or characteristics of known malware against files. While effective against known threats, this method struggles to detect new, unknown ransomware variants. Heuristic analysis uses algorithms to examine software or file behavior for suspicious characteristics.[10] The public release of this dataset will make it a useful tool for researchers, enabling them to make even more progress in ransomware detection and stronger protection system development. Second, we have conducted a detailed comparative analysis of various neural network configurations and dataset features.[11] This analysis aims to determine the most effective neural network model and feature set for ransomware detection. Third, we detect ransomware processes using initial API call sequences of a process and obtain an efficient method of early ransomware detection.

Frameworks and Architectures for Ransomware Prevention

The rapid evolution of ransomware necessitates continuous advancements in cybersecurity defense mechanisms. Emerging trends in ransomware prevention focus on predictive analytics, AI-driven threat detection, and enhanced cybersecurity frameworks to mitigate attacks before they cause irreparable damage.[12,13] Network segmentation and zero-trust security architecture have also proven to be effective in minimizing the impact of ransomware attacks. Organizations that implement zero-trust models operate on the principle of least privilege, restricting access to critical systems and requiring continuous authentication for users and devices.

Available Datasets

The IoT ecosystem has experienced the emergence of a variety of datasets tailored for security practices, with each one presenting its own strengths and weaknesses. Because of the increasing number of unreported vulnerabilities and threats, the researchers have decided to concentrate their attention on IoT datasets. The quality of the dataset is the main component for a practical model of detecting real-world intrusions.[14] Even if many studies rely on datasets such as KDDCup 1999, NSL-KDD, and UNSW-NB15, there are still other datasets that can be considered for cybersecurity intrusion detection. The current part sheds light on the datasets that are made public for use in intrusion detection systems (IDS).

KDDCUP99

The KDDCup99 dataset, used in the Third International Knowledge Discovery and Data Mining Tools Competition, identifies "malicious" and "benign" network connections, allowing the development of effective NIDS. KDDCup99, derived from the DARPA dataset, contains 4.9 million connection records with 41 features apiece. Every link is classified as either an attack or normal. The dataset covers different security attacks, including denial of service (DoS), U2R, R2L, and probing.

NSL-KDD

The NSL-KDD dataset is an improved version of the KDDCup99 dataset. While retaining the same features as KDDCup99, NSL-KDD was curated to remove duplicate and repetitive data records and minimize the dataset size. This dataset has 41 attributes along with a class label. The class label is divided into 21 categories, with four main assault types: probe, U2R, R2L, and DoS.

UNSW-NB15

The UNSW-NB15 dataset was produced by the Australian Centre for Cyber Security through their Cyber-Range Lab with the help of IXIA PerfectStorm, generating the expected consumption of both the real and synthetic cyber-attack behaviors. This dataset includes a total of 2,540,044 transactions, which can be divided into 2,218,761 legitimate and 321,283 harmful. The dataset has a variety of nine attack types, including backdoors, fuzzers, analysis, shellcode, DoS, exploits, reconnaissance, worms, and generic.

ToN-IoT

The ToN-IoT dataset, produced in collaboration between the Cyber Range and the IoT Labs at UNSW Canberra, is the result of the integration of data from several sources within a complete IIoT system. Network traffic, OS logs from Linux and Windows, and telemetry from devices that are connected are just a few examples of what is included in the dataset.[15] It also recognizes a wide variety of attacks, which include ransomware, password attacks, scans, DoS, distributed DoS (DDoS), XSS, data injection, backdoors, and MITM attacks, among others. The dataset contains 22,339,021 records and has 44 attributes that are divided into four service-profile-based categories representing connection, user activities (such as DNS, HTTP, SSL), statistics, and breach characteristics.

Common IoT Threats

This section highlights the most popular threats found in most IoT environments. Threat lists are daily updated and add new dangers to the systems. Several approaches are currently in use: traffic analysis, content analysis, application, and user behavior analysis.

- Dental of service DoS/DDoS: DDoS attacks are one of the most severe and frequent attacks in IoT networks.[16] This attack can occur at multiple tiers of the architecture, which makes its detection and resolution increasingly complex.
- Hardware and software vulnerability: not all threats are in cyberspace, as physical threats in the device itself are also very important to consider. Sometimes an open port in the device is used remotely by attackers. Universal passwords and weak embedded codes are examples of this kind of threat.
- Social engineering: it is when malicious activities are done through human interaction. Social engineers trick organizations and individuals into breaking security or getting sensitive data.[17] IoT devices are important for social engineers because they give them a brief into someone's behavior, which is one of the main steps for success for social engineers.
- User weakness: many studies show that most companies' attacks were because of employees. Social engineering, mail phishing, and other security problems are caused by the lack of security knowledge and training.

Feature Extraction and Data Representation in IoT Security

The IoT comprises an immense amount of connected devices that constantly communicate and exchange information as part of modern life. The increase in connectivity has grown exponentially in device connectivity and has drastically increased the attack surface, thus rendering IoT ecosystems easily susceptible to hostile activities. Devices with malware targeting IoT devices are rapidly rising, and pose a significant threat to the integrity, confidentiality, and availability of systems connected to IoT. Traditional security mechanisms, characterized by signature-based detection, are inadequate to combat sophisticated and adaptive threats. IoT malware embodies polymorphic and metamorphic properties, allowing it to effectively slip past traditional defenses.[18] Consequently, there is now an urgency to develop intelligent and adaptive security systems that can detect adversarial traffic within rapidly changing and complex IoT ecosystems. Within this frame, the identification of relevant patterns, anomaly detection, and the identification of malware by machine learning (ML) models within IoT networks rely directly on well-founded feature extraction and data representation.

ML AND DL IN CYBERSECURITY

ML and DL models applied to IoT Ransomware Manufacturers, and services rely on numerous communication protocols to provide effective information exchange through the IoT-connected devices. An increased number of protocols allows for increased connectivity, also increasing the risk attack surface for IoT systems from various attackers.[19] Since ransomware threats dramatically increase this liability, researchers are working on ML like support vector machines (SVM), decision trees (DT), random forests (RFs), and logistic regression (LR), and DL for intelligent threat detection systems. Traditional DL models (such as deep neural networks [DNN], deep belief networks [DBN], and recurrent neural networks [RNN]) to more accurately detect patterns and improve the accuracy of detections of different types of ransomware. The main ones are:

SVM

SVMs are reliable ML techniques that can be utilized for ransomware detection and classification, and regression applications. SVM operate by identifying the hyperplane that divides the data into distinct classes according to the values of the features as thoroughly as possible.[20] SVM can effectively handle high-dimensional data.

DT

DTs are a simple and intuitive ML algorithm that can be used for classification tasks, including ransomware detection. DTs work by recursively partitioning the data into subsets based on the values of the features and creating a tree-like structure representing the decision-making process.

RFs

RFs are an extension of DTs that improve performance and reduce overfitting. By randomly selecting features and data, RFs create multiple DTs and combine their predictions.[21] They are better-equipped to handle high-dimensional data and are less likely to overfit.

LR

LR is a parametric algorithm used for binary classification tasks (i.e., where the output is one of two possible classes). It works by modeling the probability of the output class as a function of the input features. The algorithm is trained to find the optimal parameters that maximize the likelihood of the training data and can be regularized to prevent overfitting.

DNN

A DNN is an artificial neural network with multiple hidden layers between the input and output. These layers help the model learn complex, non-linear relationships in data.[22] However, DNNs can face overfitting and require high computational power, which can be managed using techniques like regularization, weight decay, and graphics processing unit acceleration.

CNN

CNN is a type of DL used in various tasks like image recognition and classification, a powerful tool of cybersecurity used to learn features and detect malware and other anomalies. They are also robust for data variability, which makes them suitable for analyzing complex and evolving structures of ransomware.[23] CNN architectures comprise five layers: Convolutional layer, pooling layer, fully connected layer, and fully connected input and output layer, where each layer has its specific functions.

DBNs

A DBN is a layered probabilistic model made up of multiple hidden layers. Each layer learns to represent data features at different levels of abstraction. Training happens layer by layer, making it efficient for learning hierarchical patterns in data.

RNN

RNNs are designed to handle sequential data such as time series or text. They have loops that allow information to pass from one step to the next, helping the model remember previous inputs. A special type called LSTM can remember information for longer periods, useful for tasks such as weather prediction or speech recognition.[24]

Autoencoder

AE are unsupervised DL models that encode input data into a compressed, meaningful representation and then decode it to reconstruct the original data with minimal loss.[25] These neural networks are highly effective due to their ability to capture complex nonlinear correlations. Autoencoder models have played a significant role in various domains, including cybersecurity.

Role of ML in threat detection

ML encompasses a diverse set of techniques and algorithms that enable systems to learn patterns, make predictions, and improve performance over time without being explicitly programmed. Some of the fundamental ML techniques include supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, DL, neural networks, DTs, RF, SVM, and K-Nearest neighbors, which can be appropriately applied based on their use cases, either as classification, clustering, regression, or otherwise. ML has proved to be a powerful tool for threat detection in cybersecurity.[26] It enables the development of robust and adaptive systems that can analyze vast amounts of data, identify patterns, and detect anomalies that may indicate potential security threats.

Advantages over traditional ML techniques

The study focused on detecting DDoS attacks within cloud environments using an AI-based IDS framework, with a primary goal of improving accuracy while minimizing false alarms. Proposed solutions involve employing ensemble feature selection to identify key features and constructing a DNN model for precise DDoS detection.[27,28] Results indicate the effectiveness of the proposed Fund model, demonstrating superior accuracy compared to conventional ML techniques and surpassing existing methods in various performance metrics. The research highlighted the efficiency of the AI-based IDS framework with performance evaluation metrics such as accuracy, precision, recall, F1 score, area under the curve, and receiver operating characteristic used for evolution.

DL-DRIVEN RANSOMWARE PREVENTION TECHNIQUES IN IOT

Ransomware is irreversible and tedious to stop, unlike other security issues. The approach of this malware depends on access limitations to user files through encryption and demands a ransom to attain the decryption key.[29] An invader usually shows a ransom note after encoding the data of the victim, which generally indicates that the attack was executed; then, the invader demands money. Dynamic analysis provides higher accuracy in detection through the execution of the samples. DL and ML have effects on all aspects of life. Such technology has several applications in each domain because of its capability for decision-making. The feature-selection-related structure by adopting various ML methods, which include neural networks (NN)-related structures, to classify the security level for the prevention and detection of ransomware. The authors implement many ML techniques, namely, LR, DT, Naïve Bayes, NN-related classifiers, and RF, on a selected number of features for classifying ransomware.

DL based Behavioral Anomaly Detection

This involves the use of DL models such as Autoencoders, Variational Autoencoders, and LSTM networks to model the normal behavior of IoT devices. Any deviation of the learned behavior, including the situation of an uncharacteristic file access, a high rate of encryption activity, or abnormal consumption of resources, is addressed as a potential ransomware threat.[30] Preventive measures involve an early warning, shutting down processes, and isolation the devices before encryption.

DL-Improved IDS (DL-IDS)

The IDS based on DL involves the use of CNNs, LSTMs, and hybrid CNN-LSTMs to process the real-time traffic on the IoT network and system logs. The models identify patterns of ransomware communications such as connections with command-and-control servers or suspicious flow of packets. When an attack is identified, the system controls it by blocking bad traffic and limiting access by an intruder.

Ransomware Early Prevention Temporal Prediction Models

The attack of ransomware is time-related and thus well represented by LSTM, gated recurrent unit, and temporal convolutional networks. These models use time-series data like central processing unit load, file access, and memory traffic to forecast ransomware behavioral patterns before the encryption stage. Prediction in the early stage facilitates the prevention of blocking and data preservation.

Lightweight DL Models on Edge-based Prevention

Lightweight DL models are executed on the devices or edge nodes to overcome the constraints of the IoT resources.[31] Pruning of models, quantization, and Tiny ML are some of the techniques that decrease computation workloads without compromising the accuracy of the prediction. These models allow real-time ransomware prevention at a low level of latency and power.

Federated and Collaborative DL Distributed Prevention

The concept of federated learning allows several IoT devices to jointly train ransomware prevention models without exchanging raw data.[32] All devices train using local data and add to a global model, increasing flexibility to new ransomware variants. This decentralized strategy enhances the precision of the prevention process and maintains privacy and scalability.

LITERATURE REVIEW

Modern IoT systems differ from traditional computers, making them more susceptible to security attacks. Common threats such as DoS, unauthorized access, and data breaches compromise confidentiality, integrity, and availability. Large-scale IoT setups with identical devices can amplify the impact of a single breach. DL has emerged as a powerful tool to detect and mitigate these threats by analyzing massive IoT-generated data, as summarized in Table 1.

Ibraheem and Hassan, introduction of a hybrid classification approach aimed at improving ransomware detection accuracy and reducing False Alarm Rate (FAR). Specifically, the proposed hybrid approach combines the strengths of both signature-based and anomaly-based detection techniques to enhance ransomware detection. Evaluation results demonstrate an FAR below 0.020% and a detection time under 5 s. Our hybrid detection model is highly relevant to securing CPS, where both cyber and physical damage may result from ransomware attacks. Ransomware's ability to encrypt files and demand ransom poses serious risks to individuals, economies, and state security by endangering critical data.[33]

Karim *et al.* explore the intricate interaction between safety and security in the context of the IoT, emphasizing the need for a comprehensive approach to address these critical aspects and the importance of ongoing research and collaboration to navigate the challenges in this domain. The AQ6 CIAS model extends the traditional CIA triad by incorporating safety as a fourth pillar, thereby acknowledging the essential role of physical safety in IoT applications.[34] Wanjari and Verma demonstrate how the applications of healthcare and security systems and social media analysis influence society. The latest image processing techniques include ViTs alongside GANs and few-shot learning, but developers need to achieve better results in future improvements. The main goal of this research examine present-day advancements in ML and DL with a review of their capabilities as well as constraints before recommending future study paths to overcome problems encountered today. This paper evaluates both the future potential and benefits alongside drawbacks of ML and DL models applied to image recognition.[35]

Guo first analyzes the current market demand and technology trends in the mobile application development industry, and points out the great potential of DL and neural network technology in enhancing application intelligence and personalization. It describes how to introduce the DL framework and neural network model in JAVA mobile application development course, and analyzes how to realize DL applications such as image recognition, emotion analysis, and speech recognition in mobile applications.[36]

Çalışkan *et al.* provide a comprehensive analysis of recent advancements in ransomware detection and behavior analysis, focusing on trends from the last years. Through an in-depth behavioral analysis of 14 ransomware families, the research highlights common infection vectors, encryption strategies, and malicious activities. Moreover, a comparative evaluation of publicly available

Table 1: Summary of recent studies on ransomware detection in IoT

Reference	Study on	Approach	Key findings	Challenges/ limitations	Future directions
Ibraheem and Hassan (2025)	Hybrid ransomware detection for CPS	Hybrid: signature + anomaly-based classifiers	FAR <0.020%; detection time <5 s; effective for CPS scenarios	Potential dataset/ coverage limits; scalability to diverse IoT stacks not fully validated	Real-world deployment studies in heterogeneous CPS; adaptive models for unseen ransomware variants
Karim *et al*. (2025) AQ6 AQ6	Safety–security interplay in IoT	Conceptual framework (CIAS) extending CIA triad	Introduces safety as explicit pillar for IoT security design	Largely conceptual—needs empirical validation; integration complexity with legacy systems	Develop integrated safety-security toolchains and case studies in critical IoT domains
Wanjari and Verma (2025)	ML/DL trends in image processing, healthcare, security	Systematic review of DL techniques (ViTs, GANs, few-shot)	Identifies promise of modern architectures but notes bias, privacy, and computing challenges	Real-time constraints and privacy-preserving deployment in resource-limited devices	Research on lightweight models, privacy-preserving learning, and bias mitigation methods
Guo (2024)	Deep learning in mobile app development and education	Applied survey + curriculum design proposals	DL can boost app intelligence (image/emotion/speech) and industry–edu collaboration aids practical skills	Focused on pedagogy and mobile apps, not IoT-specific security; lacks security evaluation	Curriculum modules bridging DL for secure IoT apps; hands-on projects integrating security use-cases
Çalışkan *et al*. (2024)	Behavioral analysis and detection trends across ransomware families	Comparative empirical study; behavioral and dynamic analysis	Random Forests and API-call-based dynamic features effective; highlights need for real-time detection	Dataset heterogeneity and generalization to new families; limited real-time system prototypes	Build real-time, resilient detection systems and local (edge) solutions with streaming telemetry
Imamguluyev (2024)	Hardware-level IoT security via fuzzy logic	Fuzzy-logic anomaly detection using device telemetry	Improves detection accuracy and lowers false positives with computational efficiency	Simulation-based validation; hardware-in-the-loop/ physical experiments limited	Implement on actual IoT hardware; combine with ML-based anomaly detectors for hybrid defense
Ren and Chen (2023) AQ6	Transformer + RL for VRP (methodological relevance)	Transformer encoder-decoder with RL training	Achieves low GAP and fast solving time vs heuristics; shows Transformer utility on combinatorial tasks	Domain-specific to routing; transferability to security telemetry needs study	Adapt Transformer + RL for sequence/graph security tasks (e.g., attack path prediction)
Khurana (2023)	Ransomware detection using ensemble ML (SOM, RF, LSTM)	Hybrid ensemble combining unsupervised + supervised + temporal models	Captures behavioral and temporal patterns; robust detection across datasets	Potential computational overhead for real-time edge deployment	Model compression, pruning, and edge-friendly implementations; online learning for concept drift

API: Application programming interface, SOM: Self-organizing maps, IoT: Internet of things, ML/DL: Machine learning/deep learning, LSTM: Long short-term memory, RF: Random forest, GANS: Generative adversarial networks, CPS: Cyber-physical system and proprietary datasets reveals the challenges in training robust ML models. By analyzing 12 state-of-the-art detection methodologies, this research highlights the superiority of RF-based models and the critical role of dynamic analysis techniques like API calls in early-stage detection.[37] Imamguluyev proposes a fuzzy logic-driven approach to enhance hardware security in IoT devices by addressing critical challenges such as tampering, side-channel attacks, and unauthorized access. The proposed system offers significant improvements in detection accuracy, reduces false positives, and ensures computational efficiency, making it suitable for resource-constrained IoT environments. Validation through simulations highlights the system's ability to balance security and performance, providing a scalable and reliable solution for safeguarding IoT ecosystems.[38]

Ren and Chen propose a novel approach for AQ6 solving VRP using a Transformer-based deep reinforcement learning framework with an encoder-decoder structure. The encoder utilizes a Transformer model to encode the VRP problem, while the decoder incorporates the positional information of the nodes that have already been visited as input and generates a sequence of nodes to be visited as the output solution. Finally, the entire model is trained using reinforcement learning. Experimental results demonstrate that the GAP value of our model in CRP20 has decreased to 0.705%, which is more stable than other models and has a much faster solving speed than the heuristic model.[39] Khurana presents a comprehensive approach for Ransomware Threat Detection and Mitigation using ML Models. Feature engineering techniques extract relevant behavioral attributes. A trio of ML algorithms, including self-organizing maps, RF classifier, and LSTM networks, is deployed for behavioral analysis. These algorithms excel in identifying intricate patterns and temporal dependencies within the data.[40]

CONCLUSION AND FUTURE WORK

The proliferation of IoT devices across homes, industries, and critical infrastructures has amplified both connectivity and vulnerability, making traditional security methods increasingly inadequate. The survey identified data quality and majority of features as important to proper detection by analyzing publicly available datasets, typical IoT threats, and methodologies of feature extraction. The overview of ML and DL models revealed that DL algorithms are more accurate at detection, at early threat detection, and less false alarms than traditional methods. Behavioral anomaly detection, DL-IDS, temporal prediction models, lightweight edge-based solutions, and federated learning frameworks are particularly promising options when it comes to proactive ransomware mitigation in resource-constrained IoT ecosystems, because of the DL approach.

Future Work

Future studies must be aimed at creating lightweight and energy-efficient DL models that can be deployed on carelessly tight IoT and edge devices. The generation of massive, current, and ransomware-specific IoT data that represents occurrences of real-world attacks is an urgent requirement. Furthermore, explainable AI-based approaches may enhance the transparency of the model and the confidence in automated security choices. Future investigations of federated and collaborative learning models will bolster the privacy protection and scalability, and multi-modal data integration and adaptive learning models may be used to increase resilience to zero-day and continuously changing ransomware attacks.

REFERENCES

1. Kizza J. Internet of things (IoT): Growth, challenges, and security. In: Ethical and Social Issues in the Information Age. Germany: Springer Science and Business Media; 2017. p. 277-91.
2. Humayun M, Jhanjhi NZ, Alsayat A, Ponnusamy V. Internet of things and ransomware : Evolution, mitigation and prevention. Egypt Inform J 2021;22:105-17.
3. Chatterjee S. Risk management in advanced persistent threats (APTs) for critical infrastructure in the utility industry. Int J Multidiscip Res 2021;3:1-10.
4. Abdi AH, Audah L, Salh A, Alhartomi MA, Rasheed H, Ahmed S, *et al*. Security control and data planes of SDN: A comprehensive review of traditional, AI, and MTD approaches to security solutions. IEEE Access 2024;12:69941-80.
5. Chandrashekar P, Kari M. Design machine learning-based zero-trust intrusion identification models for securing cloud computing system. Int J Res Anal Rev 2024;11:901-7.
6. Sarker I. Deep cybersecurity: A comprehensive

overview from neural network and deep learning perspective. SN Comput Sci 2021;2:154.
7. Thangavel S. AI-enhanced image processing system for cyber security threat analysis. Asian J Comput Sci Eng 2024;2024:11074557.
8. Mizuno M, Sugahara Y, Iwayama D, Miyashita N, Katano H, Sekiya I. Stress and motivation of cell processing operators: A pilot study of an online questionnaire survey. Regen Ther 2022;21:547-52.
9. Sarraf G. Autonomous ransomware forensics: Advanced ML techniques for attack attribution and recovery. Int J Adv Res Sci Commun Technol 2023;3:1377-90.
10. Karri SB, Penugonda CM, Karanam S, Tajammul M, Rayankula S, Vankadara P. Enhancing cloud-native applications: A comparative study of java-To-Go micro services migration. Int Trans Electr Eng Comput Sci 2025;4:1-12.
11. Davidian M, Kiperberg M, Vanetik N. Early ransomware detection with deep learning models. Future Internet 2024;16:291.
12. Adebayo AS, Chukwurah N, Ajayi OO. Proactive ransomware defense frameworks using predictive analytics and early detection systems for modern enterprises. J Inf Secur Appl 2022;18:45-58.
13. Nutalapati P, Vummadi JR, Dodda S, Kamuni N. Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data. In: 2025 International Conference on Data Science and Its Applications (ICoDSA), IEEE; 2025. p. 880-5.
14. Amrale S. A novel generative AI-based approach for robust anomaly identification in high-dimensional dataset. Int J Adv Res Sci Commun Technol 2024;4:709-21.
15. Ande BR. Enhancing cloud-native AEM deployments using kubernetes and azure devops. Int J Commun Netw Inf Secur 2023;15:33-41.
16. Harahsheh KM, Chen CH. A survey of using machine learning in iot security and the challenges faced by researchers. Informatica 2023;47:1-54.
17. Shewale V. Demystifying the MITRE ATT and CK framework: A practical guide to threat modeling. J Comput Sci Technol Stud 2025;7:82-6.
18. Garg S. Next-gen smart city operations with AIOps and IoT: A comprehensive look at optimizing urban infrastructure. SSRN Electron J 2021;12:1-14.
19. Sh D, Pal S, Hegde C. Ransomware auto-detection in IoT devices using machine learning. Int J Eng Sci Comput 2018;8:10.
20. Bilipelli AR. AI-driven intrusion detection systems for large- scale cybersecurity networks data analysis : A comparative study. Tijer Int Res J 2024;11:922-8.
21. Kali H. The future of Hr cybersecurity: Ai-enabled anomaly detection in workday security. Int J Recent Technol Sci Manag 2023;8:80-8.
22. Patel R. Automated threat detection and risk mitigation for ICS (industrial control systems) employing deep learning in cybersecurity defence. Int J Curr Eng Technol 2023;13:584-91.
23. Irankunda D, El Fazazy K, Hamid T, Riffi J. A comparative study of deep learning-based ransomware detection for industrial IoT. Int J Adv Technol Eng Explor 2025;12:450-66.
24. Dixit M, Tiwari A, Pathak H, Astya R. An Overview of Deep Learning Architectures, Libraries and its Applications Areas. In: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN); 2018. p. 293-7.
25. Seetharaman K. Incorporating the internet of things (IoT) for smart cities: Applications, challenges, and emerging trends. Asian J Comput Sci Eng 2023;8: 8-14.
26. Prajapati V. Enhancing threat intelligence and cyber defense through big data analytics : A review study. J Glob Res Math Arch 2025;12:1-6.
27. Abdallah AM, Alkaabi AS, Alameri GB, Rafique SH, Musa NS, Murugan T. Cloud network anomaly detection using machine and deep learning techniques- recent research advancements. IEEE Access 2024;12: 56749-73.
28. Prajapati NK. Federated learning for privacy-preserving cybersecurity: A review on secure threat detection. Int J Adv Res Sci Commun Technol 2025;5:520-8.
29. Varma V. Secure cloud computing with machine learning and data analytics for business optimization. J Eng Technol Adv 2024;4:181-8.
30. Narang S, Gogineni A. Zero-trust security in intrusion detection networks: An AI-powered threat detection in cloud environment. Int J Sci Res Mod Technol 2025;4:60-70.
31. Shah V. Traffic intelligence in iot and cloud networks: Tools for monitoring, security, and optimization. Int J Recent Technol Sci Manag 2024;9:138-147.
32. Patel D. Leveraging blockchain and AI framework for enhancing intrusion prevention and detection in cybersecurity. Tech Int J Eng Res 2023;10:853-8.
33. Ibraheem A, Hassan R. A Hybrid Machine Learning Approach for Ransomware Detection: Integrating Signature and Anomaly-Based Techniques. In: 2025 International Conference on Communication, Computing, Networking, and Control in Cyber-Physical Systems (CCNCPS); 2025. p. 74-9.
34. Karim MR, Kabir S, Lei C, Lefticaru R. Safety-Security Interaction in IoT. In: 2025 15th International Conference on Advanced Computer Information Technologies (ACIT); 2025. p. 669-72.
35. Wanjari K, Verma P. A Review on the Applications of Machine Learning and Deep Learning Algorithms for Image Recognition. In: 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL); 2025. p. 1707-11.
36. Guo H. JAVA Mobile Application Development Course Under the Framework of Industry-Education Integration: Practice of Deep Learning and Neural Network Integration. In: 2024 International Conference on Artificial Intelligence, Deep Learning and Neural Networks (AIDLNN); 2024. p. 65-70.
37. Çalışkan B, Gülataş I, Kilinc HH, Zaim AH. The Recent Trends in Ransomware Detection and Behaviour Analysis. In: 2024 17th International Conference on Security of Information and Networks (SIN); 2024. p. 1-8.

38. Imamguluyev R. Fuzzy Logic-Driven Approaches to Enhancing Hardware Security in IoT Devices. In: 2024 9th International Conference on Communication and Electronics Systems (ICCES); 2024. p. 568-73.
39. Ren XL, Chen AX. Solving the VRP Using Transformer-Based Deep Reinforcement Learning. In: 2023 International Conference on Machine Learning and Cybernetics (ICMLC); 2023. p. 365-69.
40. Khurana S. Ransomware Threat Detection and Mitigation using Machine Learning Models. In: 2023 IEEE International Conference on ICT in Business Industry and Government (ICTBIG); 2023. p. 1-6.

Author Query???
AQ6: Kindly provide expansion