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)

REVIEW ARTICLE

A Survey on Deep Learning-Based Ransomware Detection and Prevention in IoT Devices

Sandeep Gupta*
SATI, Vidisha
Email-Sandeepguptabashu@gmail.com

Received: 16-10-2025; Revised: 23-11-2025; Accepted: 14-12-2025

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 methods such as SVMs, decision trees, random forests, CNNs, RNNs, autoencoders, and hybrid networks could be used in ransomware detection and prevention. The prevention methods focused on by the paper include deep learning-powered prevention systems, including behavioral anomaly detection, deep learning-enhanced intrusion detection system (DL-IDS), 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 deep learning is superior to traditional means of attaining superior accuracy, less false alarms and in time, avert threats before they occur. The results emphasize the value of privacy-preserving, adaptive, and scalable deep learning systems to develop robust ransomware prevention systems in resource-limited IoT systems.

Keywords— Deep Learning, Ransomware Detection, Internet of Things (IoT), Cybersecurity, Machine learning.

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 depends 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 zero-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 of smart, flexible, and scalable defense mechanisms, which has fueled the desire to integrate Artificial Intelligence (AI) and, more precisely, deep learning into IoT security systems. AI presents the potential to process vast volumes of heterogeneous IoT data with the capability to identify discrete attack patterns, anticipate malicious actions, and counterattack threats without having to create rules manually[4][5]. The potential of deep learning, 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 have been shown to be more effective in detecting subtle behavioral anomalies that could represent ransomware running[6][7]. The deep learning-based solutions can reveal malicious patterns by analyzing network traffic abnormalities, device activity patterns, API call patterns, and system logs associations, which the traditional methods cannot identify.

However, deep learning 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]. In order to address these limitations, modern studies have considered lightweight deep learning 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.

A. Structure of the paper

This review systematically examines deep learning-driven ransomware threat prevention in IoT devices. Section II outlines the ransomware threat landscape in IOT. Section III discusses machine and deep learning in cybersecurity. Section IV focuses on deep learning-driven ransomware prevention techniques in IOT. Section V summarizes key literature

ISSN 2581 – 3781

findings, highlighting model performance, accuracy, and existing research gaps. Section VI presents conclusion and future work.

RANSOMWARE THREAT LANDSCAPE IN IOT

Ransomware detection methods have relied on several key strategies. Signature-based detection 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.

A. 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, artificial intelligence (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.

B. 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 like KDD Cup 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).

1. **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 DoS, U2R, R2L, and Probing.
2. **NSL-KDD:** the NSL-KDD dataset, which 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.
3. **UNSW-NB15:** The UNSW-NB15 dataset was the production of 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.
4. **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, 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.

C. Common IoT threats

This section highlights the most popular threats found in most IoT environments. Threats 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 to break security or get sensitive data[17]. IoT devices are important for social engineers because it gives them a brief about someone’s behavior which is one of the main steps for success to 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.

D. Feature Extraction and Data Representation in IoT Security

The Internet of Things (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 exponential 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 models within IoT networks rely directly on well-founded feature extraction and data representation.

MACHINE AND DEEP LEARNING IN CYBERSECURITY

Machine and Deep Learning Models Applied to IoT Ransomware Manufacturers and services rely on numerous communication protocols to provide effective information exchange via the Internet of Things (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 machine learning (ML) like Support vector machines, decision trees, random forests, and logistic regression and deep learning (DL) for intelligent threat detention systems. Traditional deep learning 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:

1. Support vector machines (SVM)

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

2. Decision trees (DT)

Decision trees are a simple and intuitive machine learning algorithm that can be used for classification tasks, including ransomware detection. Decision trees 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.

3. Random forests (RF)

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

4. Logistic regression (LR)

Logistic regression 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

5. Deep Neural Networks (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 computation power, which can be managed using techniques like regularization, weight decay, and GPU acceleration.

6. Convolutional neural network (CNN)

CNN is a type of deep learning 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.

7. Deep Belief Networks (DBN)

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.

8. Recurrent Neural Networks (RNN)

RNNs are designed to handle sequential data like 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 (Long Short-Term Memory) can remember information for longer periods useful for tasks like weather prediction or speech recognition[24].

9. Autoencoder

AE are unsupervised deep learning 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.

A) Role of Machine Learning in Threat Detection

Machine Learning (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 machine learning techniques include supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, deep learning, neural networks, decision trees, random forest, support vector machines (SVM) and K-Nearest neighbors (KNN), which can be appropriately applied based on their used cases, either as classification, clustering, regression or otherwise. Machine learning (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.

B) Advantages over Traditional Machine Learning 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 Deep Neural Network (DNN) model for precise DDoS detection[27][28]. Results indicate the effectiveness of the proposed Fund model, demonstrating superior accuracy compared to conventional machine learning 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 (AUC), and Receiver Operating Characteristic (ROC) used for evolution.

DEEP LEARNING-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 via 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. Deep learning (DL) and machine learning (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 NN-related structures, to classify the security level for the prevention and detection of ransomware. The authors implement many ML techniques, namely, LR, DT, NB, NN-related classifiers, and RF, on a selected number of features for classifying ransomware.

1. **Deep Learning based behavioral anomaly detection**

   This involves the use of deep learning models like Autoencoders, Variational Autoencoders and LSTM networks to model 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 the potential ransomware threat[30]. Preventive measures involve an early warning, and shutting down of processes and isolation of the devices prior to encryption.

2. **Deep Learning-Improved Intrusion Detection Systems (DL-IDS)**

The IDS based on deep learning involves the use of CNNs, LSTMs, and hybrid CNN-LSTMs to process the real-time traffic on the internet of things network and system logs. The models identify patterns of ransomware communications like 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.

3. **Ransomware Early Prevention Temporal Prediction Models**

The attack of ransomware is time-related and thus well represented by LSTM, GRU, and Temporal Convolutional Networks. These models use time-series data like CPU load, file access and memory traffic to forecast ransomware behavioral patterns before the encryption stage. Prediction in the early stage facilitates prevention of blocking and data preservation.

4. **Lightweight Deep Learning Models on Edge-Based Prevention**

Lightweight deep learning models are executed on the devices or edge nodes to overcome the constraints of the IoT resources[31]. Pruning of models, quantization and TinyML 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.

5. **Federated and Collaborative Deep Learning 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 adding 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. Deep learning has emerged as a powerful tool to detect and mitigate these threats by analyzing massive IoT-generated data.

Ibraheem and Hassan, (2025) Introduction a hybrid classification approach aimed at improving ransomware detection accuracy and reducing 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 seconds. 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.*, (2025) exploration 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 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, (2025) 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 examines 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, (2024) first analyzes the current market demand and technology trends in the mobile application development industry, and points out the great potential of deep learning and neural network technology in enhancing application intelligence and personalization. It describes how to introduce deep learning framework and neural network model in JAVA mobile application development course, and analyzes how to realize deep learning applications such as image recognition, emotion analysis and speech recognition in mobile applications[36].

Çalışkan *et al.*, (2024) Provide a comprehensive analysis of recent advancements in ransomware detection and behavior analysis, focusing on trends from the last two 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 and proprietary datasets reveals the challenges in training robust machine learning models. By analyzing 12 state-of-the-art detection methodologies, this research highlights the superiority of Random Forest-based models and the critical role of dynamic analysis techniques like API calls in early-stage detection[37].

Imamguluyev, (2024) 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, (2023) Proposes a novel approach for 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 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, (2023) Presents a comprehensive approach for Ransomware Threat Detection and Mitigation using Machine Learning Models. Feature engineering techniques extract relevant behavioral attributes. A trio of machine learning algorithms, including Self-Organizing Maps (SOM), Random Forest Classifier, and Long Short-Term Memory (LSTM) networks, is deployed for behavioral analysis. These algorithms excel in identifying intricate patterns and temporal dependencies within the data[40].

TABLE I. SUMMARY OF RECENT STUDIES ON RANSOMWARE DETECTION IN IOT

Reference	Study On	Approach	Key Findings	Challenges / Limitations	Future Directions
Ibraheem & Hassan (2025)	Hybrid ransomware detection for CPS	Hybrid: signature + anomaly-based classifiers	FAR < 0.020%; detection time < 5s; 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)	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 & 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, compute 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 & 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 & detection trends across ransomware families	Comparative empirical study; behavioral & 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 & Chen (2023)	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 & 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

C) 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 features extraction. The overview of machine learning and deep learning models revealed that deep learning algorithms are more accurate at detection, at early threat detection, and less false alarms than traditional methods. Behavioral anomaly detection, DL-enhanced intrusion detection systems, 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 deep learning approach.

A. Future Work

Future studies must be aimed at creating lightweight and energy efficient deep learning models that can be deployed on carelessly tight IoT and edge devices. The generation of massive, current, and ransomware-specific IoT data that represent occurrences of real-world attacks is an urgent requirement. Also, explainable AI (XAI)-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] J. Kizza, “Internet of Things (IoT): Growth, Challenges, and Security,” 2017, pp. 277–291. doi: 10.1007/978-3-319-70712-9_14.

[2] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, “Internet of things and ransomware : Evolution , mitigation and prevention,” *Egypt. Informatics J.*, vol. 22, no. 1, pp. 105–117, 2021, doi: 10.1016/j.eij.2020.05.003.

[3] S. Chatterjee, “Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry,” *Int. J. Multidiscip. Res.*, vol. 3, no. 4, pp. 1–10, Aug. 2021, doi: 10.36948/ijfmr.2021.v03i04.34396.

[4] A. H. Abdi *et al.*, “Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions,” *IEEE Access*, vol. 12, pp. 69941–69980, 2024, doi: 10.1109/ACCESS.2024.3393548.

[5] P. Chandrashekar and M. Kari, “Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System,” *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, pp. 901–907, 2024.

[6] I. Sarker, “Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective,” *SN Comput. Sci.*, vol. 2, 2021, doi: 10.1007/s42979-021-00535-6.

[7] S. Thangavel, “AI Enhanced Image Processing System For Cyber Security Threat Analysis,” 202411074557, 2024

[8] M. Mizuno, Y. Sugahara, D. Iwayama, N. Miyashita, H. Katano, and I. Sekiya, “Stress and motivation of cell processing operators: A pilot study of an online questionnaire survey,” *Regen. Ther.*, vol. 21, pp. 547–552, 2022, doi: https://doi.org/10.1016/j.reth.2022.10.004.

[9] Gaurav Sarraf, “Autonomous Ransomware Forensics: Advanced ML Techniques for Attack Attribution and Recovery,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1377–1390, Jul. 2023, doi: 10.48175/IJARSCT-11978W.

[10] S. BuchiReddy Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, “Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration,” *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 4, no. 1, pp. 1–12, Apr. 2025, doi: 10.62760/iteecs.4.1.2025.127.

[11] M. Davidian, M. Kiperberg, and N. Vanetik, “Early Ransomware Detection with Deep Learning Models,” *Futur. Internet*, vol. 16, no. 8, 2024, doi: 10.3390/fi16080291.

[12] A. S. Adebayo, N. Chukwurah, and O. O. Ajayi, “Proactive Ransomware Defense Frameworks Using Predictive Analytics and Early Detection Systems for Modern Enterprises,” *J. Inf. Secur. Appl.*, vol. 18, no. 2, pp. 45–58, 2022.

[13] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, “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, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[14] Siddhesh Amrale, “A Novel Generative AI-Based Approach for Robust Anomaly Identification in High-Dimensional Dataset,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, pp. 709–721, Oct. 2024, doi: 10.48175/IJARSCT-19900D.

[15] B. R. Ande, “Enhancing Cloud-Native AEM Deployments Using Kubernetes and Azure DevOps,” *Int. J. Commun. Networks Inf. Secur.*, vol. 15, no. 8, pp. 33–41, 2023.

[16] K. M. Harahsheh and C.-H. Chen, “A Survey of Using Machine Learning in IoT Security and the Challenges Faced by Researchers,” *Informatica*, vol. 47, no. 6, pp. 1–54, May 2023, doi: 10.31449/inf.v47i6.4635.

[17] Vilas Shewale, “Demystifying the MITRE ATT&CK Framework: A Practical Guide to Threat Modeling,” *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 3, pp. 182–186, May 2025, doi: 10.32996/jcsts.2025.7.3.20.

[18] S. Garg, “Next-Gen Smart City Operations with AIOps & IoT: A Comprehensive Look at Optimizing Urban Infrastructure,” *SSRN Electron. J.*, vol. 12, no. 1, 2021, doi: 10.2139/ssrn.5271046.

[19] D. Sh, S. Pal, and C. Hegde, “Ransomware Auto-Detection in IoT Devices using Machine Learning,” *Int. J. Eng. Sci. Comput.*, vol. 8, no. December, pp. 0–10, 2018.

[20] A. R. Bilipelli, “AI-Driven Intrusion Detection Systems for

Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," *Tijer – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[21] H. Kali, "The Future of Hr Cybersecurity: Ai-Enabled Anomaly Detection in Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023, [Online]. Available: https://scholar.archive.org/work/2jwzgzcz5nh3bpfbvx7t2d55aq/access/wayback/https://lamintang.org/journal/index.php/ijortas/article/download/128/108

[22] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.

[23] D. Irankunda, K. El Fazazy, T. Hamid, and J. Riffi, "A comparative study of deep learning-based ransomware detection for industrial IoT," *Int. J. Adv. Technol. Eng. Explor.*, vol. 12, no. 124, pp. 450–466, 2025, doi: 10.19101/IJATEE.2024.111101413.

[24] M. Dixit, A. Tiwari, H. Pathak, and R. Astya, "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, pp. 293–297. doi: 10.1109/ICACCCN.2018.8748442.

[25] K. Seetharaman, "Incorporating the Internet of Things (IoT) for Smart Cities: Applications, Challenges, and Emerging Trends," *Asian J. Comput. Sci. Eng.*, vol. 08, no. 01, pp. 8–14, Mar. 2023, doi: 10.22377/ajcse.v8i01.199.

[26] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[27] A. M. Abdallah, A. Saif Rashed Obaid Alkaabi, G. Bark Nasser Douman Alameri, S. H. Rafique, N. S. Musa, and T. Murugan, "Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques— Recent Research Advancements," *IEEE Access*, vol. 12, pp. 56749–56773, 2024, doi: 10.1109/ACCESS.2024.3390844.

[28] Nirav Kumar Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[29] V. Varma, "Secure Cloud Computing with Machine Learning and Data Analytics for Business Optimization," *J. Eng. Technol. Adv.*, vol. 4, no. 3, pp. 181–188, 2024, doi: 10.56472/25832646/JETA-V4I3P119.

[30] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[31] V. Shah, "TRAFFIC INTELLIGENCE IN IOT AND CLOUD NETWORKS: TOOLS FOR MONITORING, SECURITY, AND OPTIMIZATION," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024.

[32] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[33] A. Ibraheem and R. Hassan, "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, pp. 74–79. doi: 10.1109/CCNCPS66785.2025.11135708.

[34] M. R. Karim, S. Kabir, C. Lei, and R. Lefticaru, "Safety-Security Interaction in IoT," in *2025 15th International Conference on Advanced Computer Information Technologies (ACIT)*, 2025, pp. 669–672. doi: 10.1109/ACIT65614.2025.11185898.

[35] K. Wanjari and P. Verma, "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, pp. 1707–1711. doi: 10.1109/ICSADL65848.2025.10933346.

[36] H. Guo, "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, pp. 65–70. doi: 10.1109/AIDLNN65358.2024.00018.

[37] B. Çalışkan, İ. Gülataş, H. H. Kilinc, and A. H. Zaim, "The Recent Trends in Ransomware Detection and Behaviour Analysis," in *2024 17th International Conference on Security of Information and Networks (SIN)*, 2024, pp. 1–8. doi: 10.1109/SIN63213.2024.10871663.

[38] R. Imamguluyev, "Fuzzy Logic-Driven Approaches to Enhancing Hardware Security in IoT Devices," in *2024 9th International Conference on Communication and Electronics Systems (ICCES)*, 2024, pp. 568–573. doi: 10.1109/ICCES63552.2024.10859589.

[39] X.-L. Ren and A.-X. Chen, "Solving the VRP Using Transformer-Based Deep Reinforcement Learning," in *2023 International Conference on Machine Learning and Cybernetics (ICMLC)*, 2023, pp. 365–369. doi: 10.1109/ICMLC58545.2023.10327956.

[40] S. Khurana, "Ransomware Threat Detection and Mitigation using Machine Learning Models," in *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*, 2023, pp. 1–6. doi: 10.1109/ICTBIG59752.2023.10456343.