ONLINE ISSN: 3007-3197 | PRINT ISSN: 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 5 (2025)

Deep Learning Enabled Data Protection and Security (DPS) Techniques for Intrusion Mitigation, and Network Vulnerabilities Detection in the Internet of Things (IoTs)

[1*]Iftikhar Ali, [2]Meesam Raza, [3]Salheen Bakhet, [4]Muhammad Usman Saleem, [5]Syed Muhammad Rizwan

Article Details

Keywords: Machine Learning, Deep Neural Network, CNN, Prediction Models, Routing Attacks Detection, Deep Learning, Internet Of Things, Threat Detection, Deep Neural Network, Internet Of Things Networks, Wi-Fi security, wireless protocols, WEP, Encryption

Iftikhar Ali
Department of Software Engineering, National University of Modern Languages, Islamabad, Pakistan. Corresponding Author Email: iftikhar.ali@numl.edu.pk
Meesam Raza
Department of Computer Science, National University of Modern Languages, Islamabad, Pakistan. meesum.raza@numl.edu.pk
Salheen Bakhet
Department of Computer Science, University of Engineering and Technology, Lahore. salheen@ieee.org
Muhammad Usman Saleem
Department of Computer Science, Government College Women University Sialkot
usman.saleem@gcwus.edu.pk / usman.saleem@live.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan. rizwan.naqvi@ieee.org

ABSTRACT

Deep learning operates as the main technology pillar of the present Industry 4.0. Various applications in healthcare along with visual recognition and text analytics besides cybersecurity functions have adopted Deep Learning implementation. Developing suitable DL models remains complicated because of real-world problems and data show constant changes and diverse patterns. A structured Deep Learning approach is proposed and discussed in this article that includes a DL taxonomy system. The DL-IDS framework examines different types of practical operations that include supervised or unsupervised protocols. This work proposes a novel deep learning technique for threat mitigation and a l73 accuracy rate stands at 71.73 listing real-life applications in which deep learning techniques serve practical purposes. This article works toward compiling IoT (Internet of Things) connected systems, applications, data storage, and services that may be a new gateway for cyberattacks as they continuously offer services in the organization. Currently, software piracy and malware attacks are high risks to compromise the security of IoT. The proposed DL-IDS system uses acquired information to determine if data needs to be transferred to the fog layer. The proposed approach demonstrates better functionality than available DL-IDS solutions operating on the RT-IoT2022 dataset. The accuracy rate stands at 71.73 when measuring the detection performance of Intrusion using the proposed IPS-DL system. Through an integration of Deep Learning DL-IDS based the Proposed IPS system achieves an anomaly identification with a precision of 70.63%, together with a recall of 96.30% and an F1-score at 92% for intrusion prevention tasks. 85% detection ratio coupled with a 0.99% ideal throughput and a 0.23% packet delivery ratio at a minimum energy usage of 0.11 joules with a bandwidth of 0.84 bps and the delay was measured at 0.21 ms using 100 nodes with 0.66% improved probability. Security issues within IoT networks is also addressed through quick response systems for intrusion detection in IoT networks.

INTRODUCTION

Internet of Things (IoT) refers to the inter-connectivity of physical objects incorporating sensors and/or activators embedded in them and which are either connected through cable or wireless networks. It brings about a change, especially in the manner in which people adopt technology

in their day-to-day activities. IoT deals largely with domains such as smart cities, houses and health-oriented industries. However, security and privacy issues emerge due to the increase in the usage of smart devices and IoT applications [1]. Security threats such as node spoofing, unauthorized access of data, and cyber threats such as DoS, eavesdropping, and intrusion have become very relevant issues. Over the years, the methods based on Machine learning (ML) and deep learning (DL) have been enhanced and these are found to solve such security issues in IoT devices effectively. It is noteworthy that the main focus of the currently active Fourth Industrial Revolution, also known as Industry 4.0, is generally considered to be technology-intensive automation and intelligent systems and/or applications in diverse fields [2, 3]. They include smart health care, smart city, smart business intelligence, as well as Cyber Intelligence [4]. Deep learning methods have experienced rapid expansion in themselves to tackle various real-world problems. Determining performance on various application forms is the core of its capabilities. Security technologies are particularly effective as an excellent solution for uncovering complex architecture in high-dimensional data [5]. DL techniques maintain a crucial position in development. These systems function based on data intelligence requirements of the present day because of their excellent learning capabilities from historical data. The implementation of Deep Learning provides the possibility to transform both society and humans [6]. Figure 1 represents the Generalized Security Framework based on Layers of Advanced analytics [8, 9].

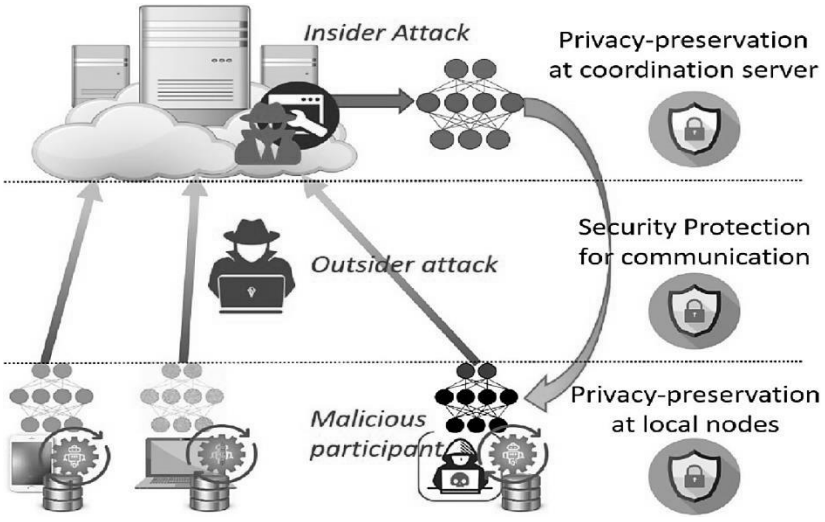

FIGURE 1: GENERALIZED SECURITY FRAMEWORK BASED ON LAYERS [9]

EXPLAINABLE DEEP LEARNING AND NEURAL NETWORK ARCHITECTURES

Deep Learning as a modern computer science, features intelligent computing as its main area with vital techniques. The following part introduces the position of explainable deep learning in AI. DL functions as one of the fundamental technology implementations [10]. AI presents a

frontier for artificial intelligence alongside other features that belong to its domain. The technology implements intelligent systems automation through its application. More Smarter AI represents the advanced state that this technology achieves. Deep learning has data-learning capabilities that provide a strong connection with intelligence systems. Typical data science work consists of the complete procedure that starts with finding meaning or insights in data in a particular problem advanced decision-making in this domain depends largely on DL technologies. Analytics and intelligent decision-making [11, 12]. Overall, DL technology possesses capabilities that enable it to transform current systems. The current world, particularly, is a powerful computational. The advanced computational power enables machine automation with technological solutions. Data-driven systems change their operation according to smart and intelligent systems and achieve their goals [13, 14]. A deep neural network from TensorFlow is suggested to be used in the identification of pirated software based on source code plagiarism. The tokenization and weighting feature methods are applied to pre-process the noisy data and to highlight the relevance of each token to specifically detect the source code plagiarism. After that, the deep learning method is applied to identify source code plagiarism [15]. It uses a deep convolutional neural network for detecting the presence of infections in an IoT network through color mapping. The malware samples are collected from the used malware dataset for testing and evaluation. Based on the experimental evaluation results, we note that the classification results of the proposed solution for measuring cybersecurity threats in IoT are comparatively better than the existing methods [16, 17]. A function f (x) is called μ strongly convex whenever μ> 0 exists, where x1, x2 belong to Rd, f (x1) > f (x2) + (x1 - x2)T∇ f (x2) + μ as shown in Eq. 1.

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^{k}$$

Eq (1)

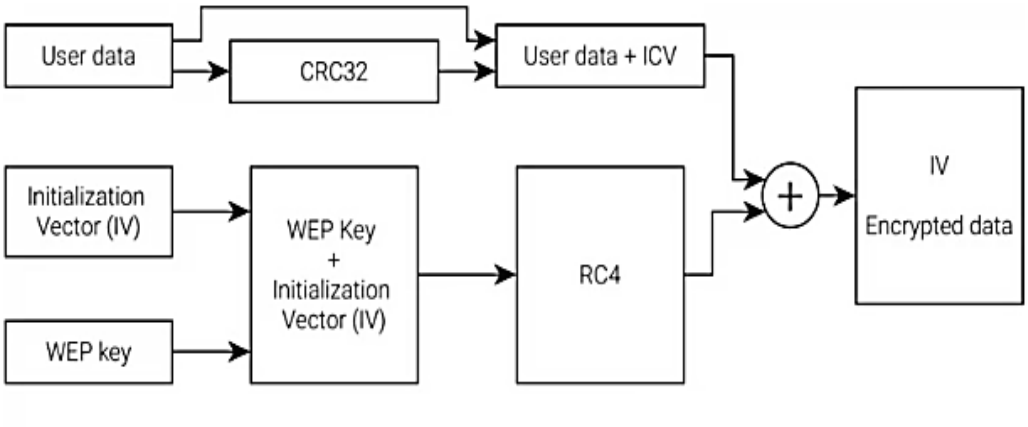

FIGURE 2: MACHINE LEARNING BASED ENCRYPTION USING CRC32 [19]

Wired Equivalent Privacy (WEP) was the original WiFi security protocol, introduced way back in 1997. The idea was simple: to use a shared key to encrypt data so that only devices with that key could access the network. The lack of key management made it easy for attackers to recover the key. Figure 2 represents a Machine Learning based Security Encryption based on CRC32 [19]. WEP was deprecated in 2004, but you will be shocked to know that some routers still support it up to date. Security through obscurity doesn't work. It was imperative to come up with a protocol based on reliable, open-source cryptographic algorithms [20].

$$\mu_i = \frac{1}{n_i}\sum_{j=1}^{n_i} x_j, \quad \sigma_i^2 = \frac{1}{n_i - 1}\sum_{j=1}^{n_i}(x_j - \mu_i)^2 \qquad \text{Eq (2)}$$

$$\mu_g = \frac{\sum_{i=1}^{k} n_i \mu_i}{\sum_{i=1}^{k} n_i}, \quad \sigma_g^2 = \frac{\sum_{i=1}^{k}(n_i - 1)\sigma_i^2}{\sum_{i=1}^{k} n_i - k} \qquad \text{Eq (3)}$$

Packet transmittance ratio is the total number of packets acquired divided by the total number of packets transmitted shows the Performance of Packet Delivery Ratio as shown in Eq 4.

$$PDR = \frac{Total\ no.of\ packets\ received\ (x_i)}{Total\ no\ of\ packets\ sent\ (y_i)} \qquad \text{Eq (4)}$$

PDR = Total no. of packets received/total number of packets sent. Similar to the point-to-point link described in headers, enclose the data that travels between shared and public internetworks towards its destination point. The goal of encryption becomes security as the system operates to duplicate private link operations. The captured packets on shared or public networks become unreadable until the encryption keys are provided for decryption. An IOT connection contains private data that has been either encoded or secured. A user can establish a secure corporate

Internet server connection through the Internet routing structures using an SDN connection from home or any other location [21, 22]. The data transmission method between shared and public internetworks uses headers to contain data as described in [23]. The main purpose of encryption is protection because the system duplicates private connection functionality. The encryption keys serve as the only means to decode captured packets that reside on shared or public networks until the keys are furnished for decryption. The private information of IOT connections remains secure through either encoding or security protocols. A user can create secure corporate Internet server connections through Internet routing structures by establishing an SDN link at home or any other location [24]. Through the following ML algorithms, the Network achieves the ability to process vast amounts of data after learning from it to determine its course of action. The process requires algorithms to learn by processing labeled information, which enables them to forecast upcoming data or classify incoming data. Machine Learning operates through object recognition and speech analysis through techniques that include neural networks and decision trees [25, 26].

$$B = \{B_1, B_2, \ldots, B_k, \ldots, B_l\} \quad \text{Eq (5)}$$

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v \quad \text{Eq (6)}$$

RELATED WORK ON DEEP LEARNING-BASED IDS FOR IOT

They provide the Network with the capacity to take in large amounts of information and learn from it to then decide what to do with that data using the following ML algorithms. This involves training algorithms on labeled data to make predictions or classify new data. Machine Learning used for tasks such as object recognition and speech analysis typically includes techniques like neural networks or decision trees. For example, convolutional neural networks (CNNs) have achieved well over 90% accuracy on benchmark tasks like object recognition [27]. Figure 3 shows the Performance Analysis of DL and other ML techniques for IDs in IoTs. This method can be thought of as a Network looking for patterns of unlabeled data, for example, clustering and dimensionality reduction for anomaly detection and feature extraction are implemented using these methods. For example, k-means clustering has been successfully used for Network vision data segmentation. This method requires the training of Networks by rewarding them whenever they take a good course of action. But, more interestingly, it is well suited for discovering complex behaviors and adaptive control [28. 29].

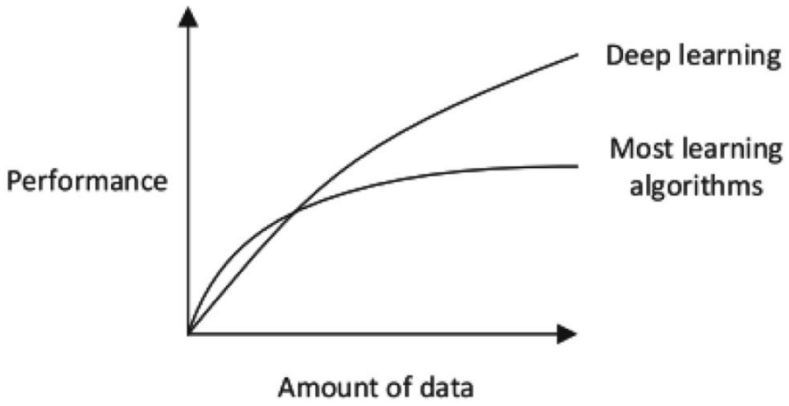

FIGURE 3: PERFORMANCE ANALYSIS OF DL AND OTHER ML TECHNIQUES FOR IDS IN IOTS [30]

DEEP LEARNING AND DEEP NETWORKS TECHNIQUES

Traditional Q-learning and deep Q-networks (DQN) algorithms are capable of achieving state-of-the-art Network navigation and manipulation performance improvements on a subset of benchmark tasks [31]. The Internet of Things (IoT) stands as the prevalent notion concerning Internet expansion during the third wave. The Medical Internet of Things exists as a group of Internet-connected medical equipment that helps health processes through procedure execution and service delivery [32]. With the use of tiny wearable devices or implanted sensors. MIOT represents a new healthcare technology that collects vital patient data while monitoring pathological conditions through its system. MIOT applications that use wireless body area networks (WBAN) to implantable medical devices have proven their ability to enhance healthcare for people. IOMT operates as a worldwide system that links medical devices into a single network available for universal access at any point in time [33, 34]. Figure 4 below represents the Taxonomy of Deep Learning Techniques.

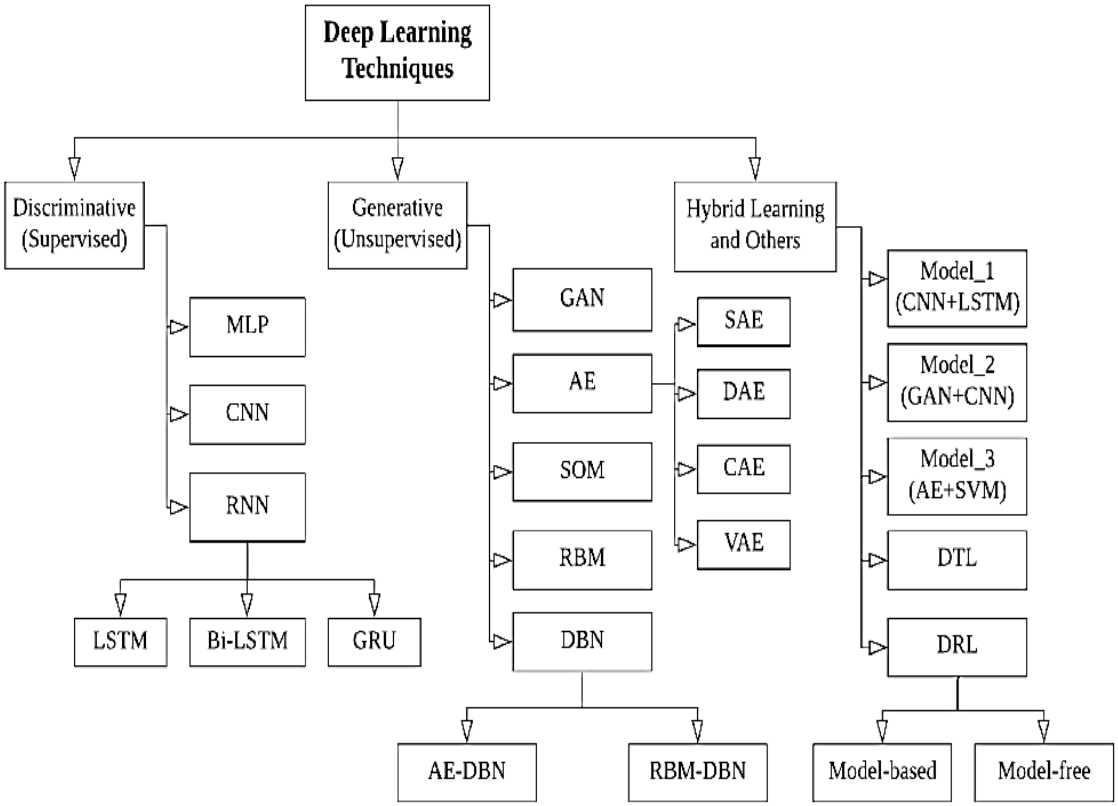

FIGURE 4: TAXONOMY OF DEEP LEARNING TECHNIQUES [35]

STATIC MALWARE DETECTION TECHNIQUES BASED ON DL

The extraction of structural elements from binary files along with function calls and other features constitutes static detection. The main employment of this technique occurs while developing and testing software. Static detection approaches currently use the procedures demonstrated in Fig. 5.

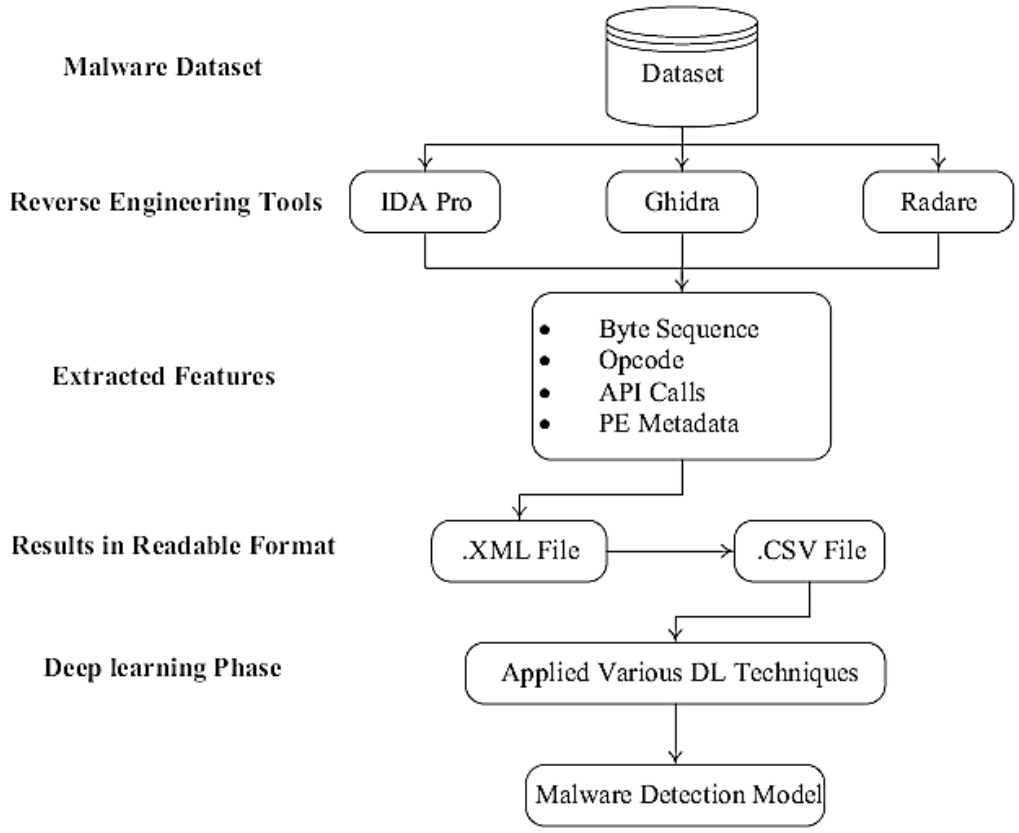

FIGURE 5: MACHINE LEARNING BASED EXISTING STATIC INTRUSION DETECTION FOR IOTS [36]

DYNAMIC MALWARE DETECTION TECHNIQUES BASED ON DL

Through dynamic detection, analysts execute possibly malicious software files inside environments that remain confined to virtual machine emulators or sandboxes. This process monitors. Analysis of the sample's resource usage enables detection of behavioral characteristics characteristic of malware. During software operation and maintenance, the detection technique finds its main application. The current dynamic detection methodology includes its fundamental operational flow illustrated in Figure 6

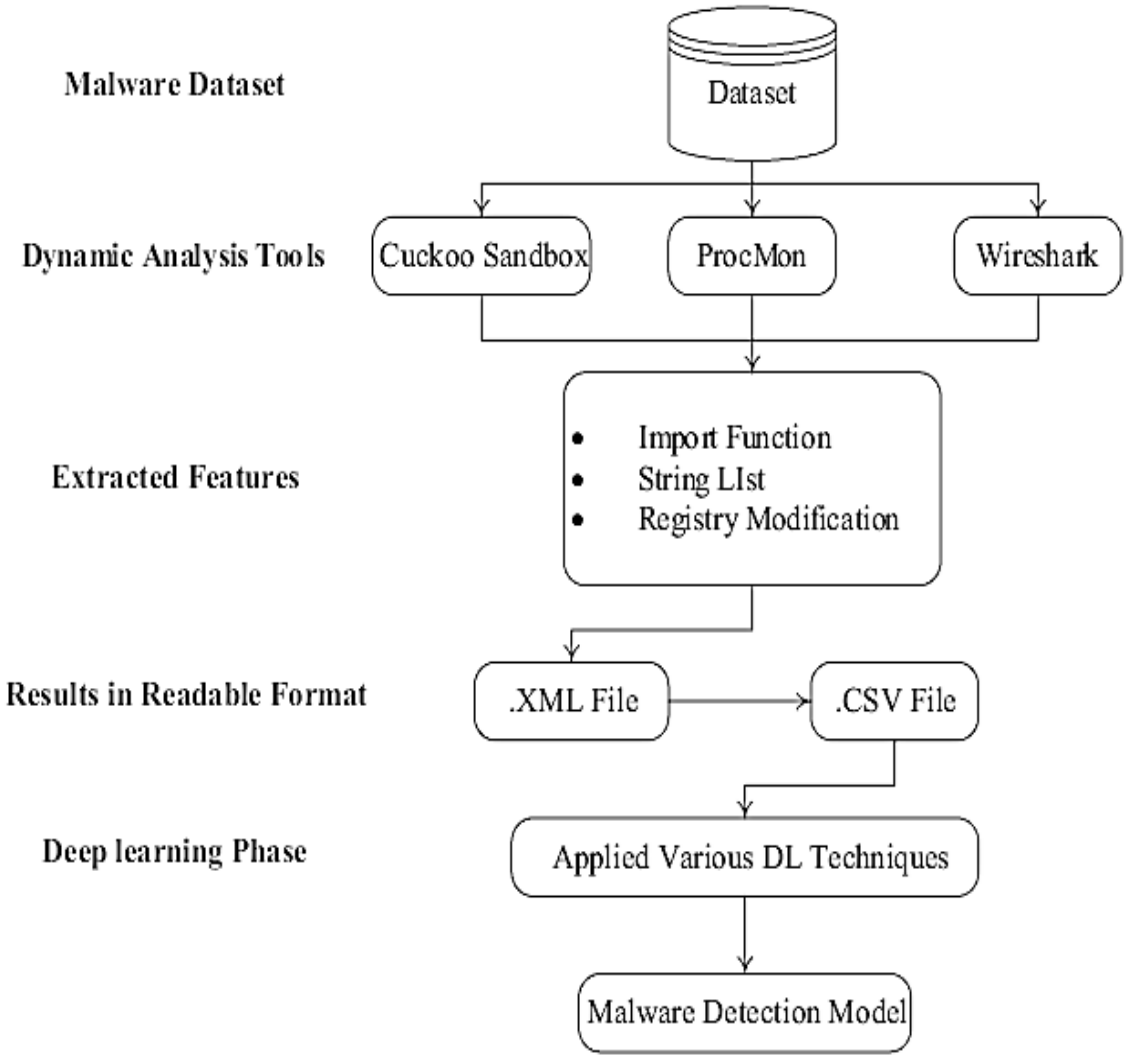

FIGURE 6: MACHINE LEARNING BASED EXISTING DYNAMIC INTRUSION DETECTION FOR IOTS [37]

HYBRID MALWARE DEEP LEARNING TECHNIQUES BASED ON DL

Detecting shell malware becomes particularly hard during static analysis processes. The techniques used for dynamic analysis provide researchers with valuable information about hidden functionalities of code operating in an emulated environment. The method brings future potential, but it simultaneously presents security vulnerabilities, together with functional and size limitations. Researchers developed a hybrid detection system to correct its former limitations [38, 39]. The analytic method follows steps to run dynamic analysis on shell malware for shell process execution, followed by static code analysis of the shelled programs. The dynamic-static method combination benefits from the key features of each technique to identify malware characteristics effectively.

TKIP was developed to work on the existing WEP hardware with the help of a simple firmware

tweak. It was not a perfect solution, but it gave us time to come up with a better approach to the problem. You input a passphrase, and from this passphrase you get your encryption keys. That is as long as one uses a strong passphrase to check his/her email or establish a connection to another system.

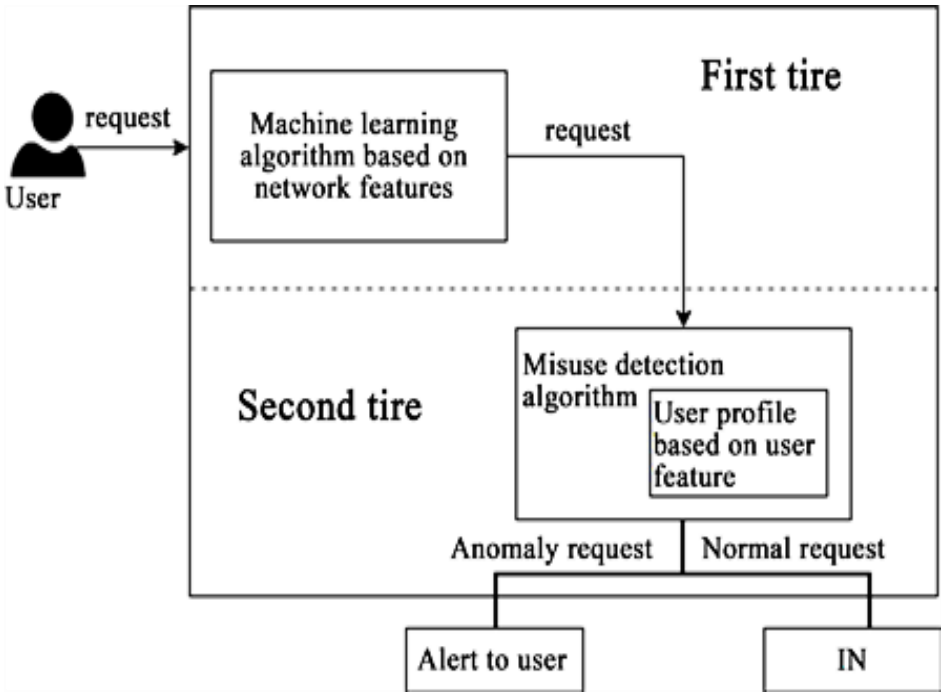

FIGURE 7: MACHINE LEARNING BASED EXISTING HYBRID INTRUSION DETECTION FOR IOTS [40]

ROLE OF DEEP LEARNING IN HEALTHCARE NETWORKS

The health industry has transformed because of its advancing development patterns. The IOMT-based e-health application landscape dominates wellness services, which motivate millions of global human beings to choose healthier lifestyles according to research findings in [41]. Healthcare services have developed into user-directed and accurate, comprehensive, customized, and pervasive healthcare solutions, which include 24-hour private healthcare services. These are responsible for image classification and object detection tasks to help Networks see, interpret, and understand the visual world. CNNs have been extremely successful, with architectures like AlexNet getting a top-5 error rate of 15.3% on the ImageNet dataset. Research about mammalian visual cortex mechanisms formed the basis of Convolutional Neural Networks (CNNs) [42]. Each new protocol has had to balance increased security with ease of use. WPA3's Enhanced Open is a great example of improving security without sacrificing convenience. Figure 8 shows different Attacks in IoT Network dataset used in IoTs.

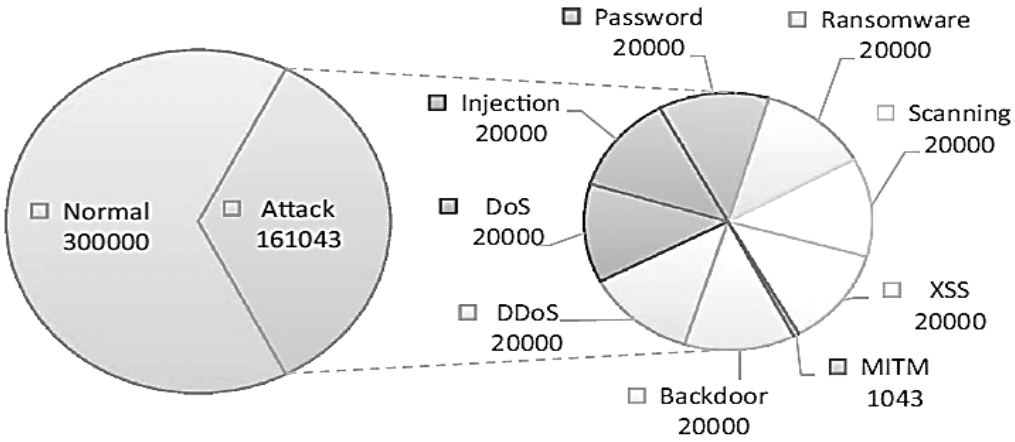

FIGURE 8: DIFFERENT ATTACKS IN IOT NETWORK DATASET USED IN IOTS [45]

METHOD & MATERIALS

This research considers how deep learning-based security protocols have developed and how effective they have become. The research methodology uses qualitative methodology through comparative analysis and case studies, together with literature reviews as research instruments. The research draws its primary information from IEEE 802.11 specifications and white papers together with secondary information obtained from peer-reviewed journals and industry reports and practical field studies. Secure access strategies depend on the performance level of employed authentication systems. The framework analyzes known weaknesses that expose systems to attacks as well as vulnerability factors within their structure.

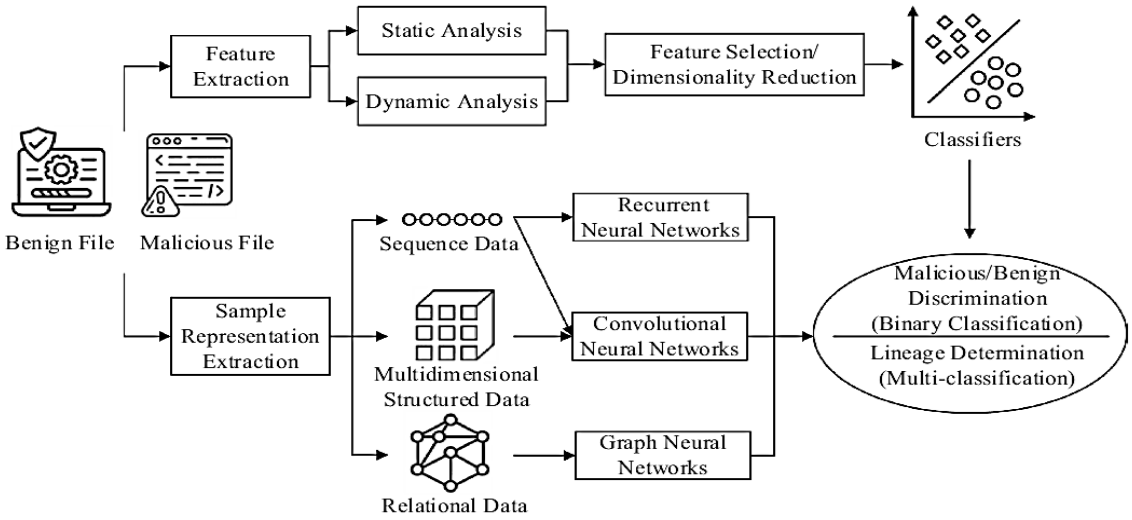

FIGURE 9: PROPOSED MALWARE AUTHENTICATION AND IDENTIFICATION FRAMEWORK BASED ON DL

Figure 9 above represents the Proposed Malware Authentication and Identification Framework based on DL. Utility in both personal and enterprise settings. Actual field deployments and real-

attack cases were chosen to support analytical findings as verification evidence. The wireless security protocol WPA2 experienced KRACK attacks, while WPA3 implemented smart city deployments. The first wireless communication security protocol, named Wired Equivalent Privacy (WEP) appeared on the market. The design sought to create wired network-level security however, development problems led to its ineffectiveness as a solution. RC4 stream cipher with 24-bit initialization vectors (IVs). CRC-32 checksum for error detection. The identity of IVs served as a setback because attackers could use brute-force decryption methods against the data packets. Weak Encryption: Susceptible to statistical attacks. Research findings confirmed that WEP remained in use by various legacy network systems.

DEEP LEARNING-BASED SECURE INTRUSION DETECTION SYSTEM FOR IOTS

In today's interconnected world, network security and privacy are more crucial than ever. As we rely more on digital platforms for both personal and business activities, the threats to our online security have grown significantly. Rapid technological advancements have brought greater convenience, but they've also introduced new vulnerabilities in how we communicate and share data. This helps ensure secure and private communication, especially over potentially unsafe networks like the public internet. However, cyber threats are constantly evolving. Sophisticated hacking techniques, data interception, and identity theft create significant challenges for network security. Additionally, the increasing rise of surveillance by governments, data collection by corporations, and even censorship complicate the ability to maintain personal privacy online.

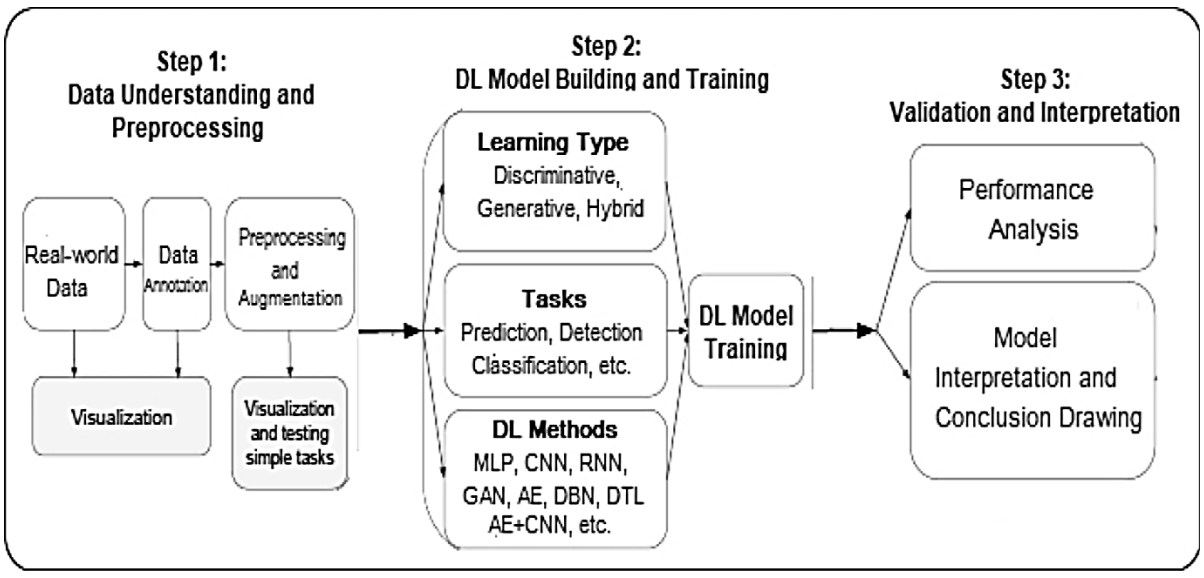

FIGURE 10: DEMONSTRATION OF PROPOSED DEEP LEARNING MODEL FOR IDS USING RT-IOT2022 UCI MACHINE LEARNING DATASET

Figure 10 shows the Demonstration of the Proposed Deep Learning model for IDS using the RT-IoT2022 UCI Machine Learning dataset. The research problem centers on understanding

and addressing these growing challenges to network security and privacy. Protocols that not only ensure secure communication but also protect against emerging threats while maintaining privacy in the increasingly complex online world. Older devices require firmware upgrades. Dictionary attacks cracked some systems using SAE during specific deployments. WPA3-secured networks enabled safe IoT device protection without sacrificing high-speed data speeds. The development sequence from WEP to WPA3 represents the ongoing transformation of security technology throughout history. WPA started to resolve WEP's encryption weaknesses, though it maintained support for obsolete cryptographic methods.

$$f(x) = w^T a + \quad b \qquad \text{Eq (7)}$$

The proposed classifier contains i to represent random units of b-layer units and y to represent the total b-layer units, as shown below in Eq (8) (9) and 10.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)} \qquad \text{Eq (8)}$$

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)}) \qquad \text{Eq (9)}$$

$$P(w) = \sqrt{\frac{t}{f(w)}} + \frac{t}{f(w)}, \qquad \text{Eq (10)}$$

The introduction of AES encryption into WPA2 created the modern standard but it still had to overcome new preliminary vulnerabilities discovered in its system. The future wireless network security solution WPA3, was designed to protect the networks of the forthcoming years against current real-world cyber threats. Each protocol has successfully improved wireless network security over time however, each stage has demonstrated its connection weaknesses. The defense mechanism that endured as robust against attackers shows insufficient strength against current rapid cyber threats. WPA3 presents itself as the advancement in wireless security that will establish future-proof defenses for interconnected digital systems. The practice of wireless security requires ongoing transformation efforts because it is an endless evolutionary process. The security improvement through WPA3 represents a breakthrough but ongoing technological advances and changing attack methods will make wireless security maintenance an ongoing

challenge. This research adopts a qualitative approach, focusing on the conceptual analysis of Routing protocols through an extensive ML-based approach. The goal is to gain insights into the operational mechanics, security features, and performance aspects of various Network protocols. By leveraging academic papers, industry reports, and technical documentation, this approach aims to build a well-rounded protocol function in modern network environments.

$$f(w) = \frac{count_w}{totalno.oftokens},$$

Eq (11)

As shown below in Eq. (12) attacks cracked some systems using SAE during specific deployments. WPA3-secured networks enabled safe IoT device protection without sacrificing high-speed data speeds.

$$f_t = \sigma(W_f.[h_{(t-1)}, x_t] + b_f)$$

Eq (12)

The development sequence from WEP to WPA3 is represented in Eq (13) and Eq (14) and Eq (15) as the ongoing transformation of security technology throughout history. WPA started to resolve WEP's encryption weaknesses, though it maintained support for obsolete cryptographic methods.

$$i_t = \sigma(W_i.[h_{(t-1)}, x_t] + b_i),$$

Eq (13)

The introduction of AES encryption into WPA2 created the modern standard but it still had to overcome new preliminary vulnerabilities discovered in its system. The future wireless network security solution WPA3 was designed to protect the networks of the forthcoming years against current real-world cyber threats.

$$\tilde{C}_t = tanh(W_c.[h_{(t-1)}, x_t] + b_c),$$

Eq (14)

$$C_t = f_t * C_{(t-1)} + i_t * \tilde{C}_t,$$

Eq (15)

$$O_t = \sigma(W_O.[h_{(t-1)}, x_t] + b_o), \quad \text{Eq (16)}$$

RESULTS AND CLASSIFICATION OF PERFORMANCE

This section elaborates on the results as each protocol has successfully improved wireless network security over time however, each stage has demonstrated its connection weaknesses. Figure 11 represents the (TPR-FPR) Receiver Operating Characteristic Curve as the defense mechanism that endured as robust against attackers shows insufficient strength against current rapid cyber threats.

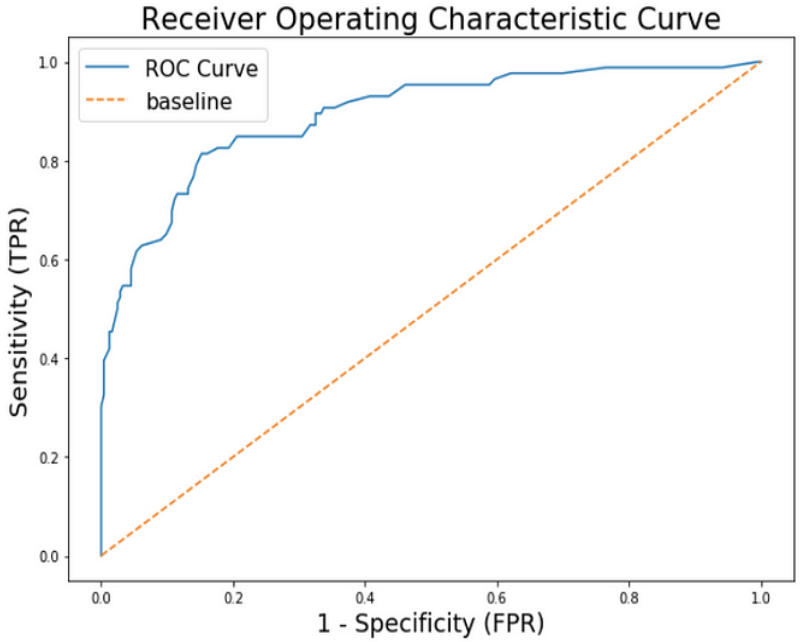

FIGURE 11: (TPR-FPR) RECEIVER OPERATING CHARACTERISTIC CURVE

Below mentioned Table 1 below represents the Comparative Analysis of Intrusion Detection based on the Proposed Deep Learning IDS Model using RT-IoT2022 UCI Machine Learning Dataset using WPA3. The practice of wireless security requires ongoing transformation efforts because it is an endless evolutionary process. The security improvement through WPA3 represents a breakthrough but ongoing technological advances and changing attack methods will make wireless security maintenance an ongoing challenge. Table 2 shows the Proposed Deep Learning IDS Model using the RT-IoT2022 UCI Machine Learning dataset

TABLE 1 COMPARATIVE ANALYSIS OF INTRUSION DETECTION BASED ON PROPOSED DEEP LEARNING IDS MODEL USING RT-IOT2022 UCI MACHINE LEARNING DATASET

Classifier	Data Set	F-T1	F-T2	F-T3	F-T4	F-T5	F-T6	F-T7	F-T8	F-T9	F-T10

RNN	RT-IoT2022 UCI	Machine Learning	59.89	59.89	62.19	91.34	90.62	62.19	91.34	90.62	63.23	59.89
DT			54.32	54.32	57.34	91.30	90.18	57.34	91.30	90.18	56.71	54.32
NBB			57.92	57.92	57.78	90.77	89.65	57.78	90.77	89.65	59.89	57.92
RF			90.62	63.23	59.89	90.62	63.23	59.89	90.62	63.23	91.34	60.21
SVM			90.18	56.71	54.32	90.18	56.71	54.32	90.18	56.71	57.92	53.68
CNN			89.65	59.89	57.92	89.65	59.89	57.92	89.65	59.89	60.21	57.97

Dataset

$$\ln fl_{it}^{+} = \sum_{j=0}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=0}^{t} \max(\Delta w^{T}{}_{ij,0}) + \in_{it} \qquad \textbf{Eq (17)}$$

$$\ln fl_{it}^{+} = \sum_{j=1}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=1}^{t} \max(\Delta w^{T}{}_{ij,1}) + \in_{it} \qquad \textbf{Eq (18)}$$

$$B_{m,n}(q+1)\left(1 - \frac{1 - X(0,1) - X(-1,1)}{1 - c_{m,n} \times f_{mn}(q)}\right) = X(0,1) \times R_{s,n} \qquad \text{Eq (19)}$$

TABLE 2: PROPOSED DEEP LEARNING IDS MODEL USING RT-IOT2022 UCI MACHINE LEARNING DATASET

Classifier	Data Set	F-T11	F-T12	F-T13	F-T14	F-T15	F-T16	F-T17	F-T18	F-T19	F-T20
RNN	RT-IoT2022 UCI	59.89	52.34	91.07	57.97	55.79	61.28	62.19	90.18	56.71	57.92
DT		54.32	54.32	57.34	52.34	62.19	52.34	57.34	62.19	59.89	60.21
NBB		57.92	53.37	57.78	54.32	57.34	54.32	57.78	57.34	54.32	53.68
RF		59.89	55.79	61.28	53.37	57.78	53.37	62.19	90.18	56.71	57.92
SVM		54.32	54.32	54.72	56.84	53.68	57.78	57.34	62.19	59.89	60.21
CNN		89.65	54.32	54.72	56.84	53.68	57.92	57.78	57.34	54.32	53.68

Machine Learning

$$\ln fl_{it}^{+} = \sum_{j=2}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=2}^{t} \max(\Delta w^{T}{}_{ij,2}) + \in_{it} \qquad \textbf{Eq (20)}$$

TABLE 3: ANALYSIS OF BASED ON ACTIVE ATTACK IDS USING RT-IOT2022 UCI

Attack	Method	No of Nodes	PDR (bytes)	SVM	DT	RF	Proposed DL-IDS
	Accuracy	100	2000	0.144	0.5431	0.411	0.9642
	R^2 Score	100	2000	0.285	0.3985	0.343	0.331
	Loss	100	2000	0.344	0.2644	0.132	0.3411
	F-1 Score	100	2000	0.485	0.1785	0.453	0.531
	Specificity	100	2000	0.51	0.4321	0.541	0.121

Active	Sensitivity	100	2000	0.631	0.7531	0.455	0.531
Attack	Delay	100	2000	1.22ms	2.34ms	1.1ms	0.21ms
	Detection	100	2000	50.13%	55.2%	68.56%	70.63%

CONCLUSION AND RECOMMENDATIONS

In this article, the technical field of malware detection through deep learning technology is presented using a proposed DL based IDS model. The technology demonstrates improvements in accuracy as well as other features. The high computational demands of these models work as a significant limitation for their broader Application. Deep learning technology shows continuous improvement, which leads researchers to predict that malware detection based on deep learning will achieve superior outcomes. Permanent vigilance against emerging malware detection trends and challenges must be maintained as we actively seek new approaches to handle advanced cyber threats. Improving systems that detect malicious code through effective resolution of the mentioned problems will produce better cyber defense systems by enhancing model accuracy alongside practical usage and general application. The Proposed approach outperforms existing Deep Learning and Machine Learning based Intrusion Detection Systems that run on RT-IoT2022 when evaluating functionality. The detection system's accuracy reaches 96.42 % through the proposed detection model. An integrated DL approach in the Proposed IPS delivers an anomaly detection performance of 70.63% precision and 96.30% recall and 92% F1-score in intrusion prevention operations. The system provides an 85% detection rate using 0.11 m joules of power expenditure, 0.84 bps top speed, 0.21 ms delay, 0.23% packet delivery ratio, and 0.99% ideal throughput using 100 nodes. The system achieved 4% better F1-score results while decreasing latency to 10 ms and decreasing energy consumption to 0.02W with 0.66% better probability. The proposed models make it possible to develop fast-response intrusion detection systems for resolving security problems in IoT networks.

FUNDING STATEMENT: The authors received no specific funding for this study.

CONFLICTS OF INTEREST: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] Islam, M. K., Rahman, M. M., Ali, M. S., Mahim, S. & Miah, M. S. Enhancing lung abnormalities diagnosis using hybrid dcnnvit- gru model with explainable ai: A deep learning approach. Image Vis. Comput. 142, 104918 (2024).

[2] Tariq U, Ahmed I, Bashir AK, et al. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023;23(8):4117.

[3] Kaspersky. IT threat evolution Q3 2023[R/OL]. (2023–12–01)[2024–05–11]. https:// secur elist. com/ ksb-2023-stati stics/ 111156/.

[4] Ma B, Zhang Z, Chen Y, Wu JX. The defense method for code-injection attacks based on instruction set randomization. J Cyber secur. 2020;5(4):30–43.

[5] Sihao SHAO, Qing GAO, Sen MA, et al. Progress in research on buffer overflow vulnerability analysis technologies. J Softw. 2018;29(5):1179–98.

[6] Qiang LIU, Yapin DENG, Zheng XU, et al. Research on hidden trojan horse detection technology. Comput Eng. 2006;32(1):180–2.

[7] Xiao-Meng F, Qiu-Ye S, Bing-Yu W, Jia-Wen G. The coordinated cyber physical power attack strategy based on worm propagation and false data injection. Acta Automatica Sinica. 2022;48(10):2429–41.

[8] Yadav B, Tokekar S. Recent innovations and comparison of deep learning techniques in malware classification: a review. Int J Inf Secur Sci. 2021;9(4):230–47.

[9] Shaukat K, Alam T M, Luo S, et al. 2021 A review of time-series anomaly detection techniques: a step to future perspectives//Advances in Information and Communication: proceedings of the 2021 future of information and communication conference (FICC), Volume 1. Springer International Publishing, 865–77.

[10] Sung A H, Xu J, Chavez P, et al. 2004 Static analyzer of vicious executables (save)[C]//20th annual computer security applications conference. IEEE, 326–34.

[11] Nataraj L, Karthikeyan S, Jacob G, et al. 2011 Malware images: visualization and automatic classification[C]//Proceedings of the 8th international symposium on visualization for cyber security. 1–7.

[12] Smmarwar SK, Gupta GP, Kumar S. Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: a comprehensive review. Telemat Inf Rep. 2024;12:100130

[13] Gao, J., Wang, H., & Shen, H. (2020). Task failure prediction in cloud data centers using deep learning. IEEE Transactions on Services Computing, 1111–1116. https:// doi.org/10.1109/BigData47090.2019.9006011 ...

[14] Guo, X., Aviles, G., Liu, Y., Tian, R., Unger, B. A., Lin, Y. H. T., & Kampmann, M. (2020). Mitochondrial stress is relayed to the cytosol by an OMA1–DELE1–HRI pathway. Nature, 579(7799), 427–432.

[15] Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Computer Networks, 153, 36–48. Khoramshahi, M., & Billard, A. (2019). A dynamical system

approach to task adaptation in physical human-Network interaction. Autonomous Networks, 43(4), 927–946.

[16] Lin, K., Li, Y., Sun, J., Zhou, D., & Zhang, Q. (2020). Multi-sensor fusion for a body sensor network in a medical human-Network interaction scenario. Information Fusion, 57, 15–26. Manogaran, G., Baskar, S., Hsu, C. H., Kadry, S. N., Sundarasekar, R., Kumar, P. M., & Muthu, B. A. (2021).

[17] FDM: Fuzzy-optimized Data Management Technique for Improving Big Data Analytics. IEEE Transactions on Fuzzy Systems, 29(1), 177–185. Manogaran, G., Shakeel, P. M., Priyan, R. V., Chilamkurti, N., & Srivastava, A. (2019). Ant colony optimization-induced route optimization for enhancing the driving range of electric vehicles. International Journal of Communication Systems, e3964. https://doi.org/10.1002/dac.3964

[18] Gesture-based human-Network interaction for human assistance in manufacturing. The International Journal of Advanced Manufacturing Technology, 101(1), 119–135. Nguyen, N. T., Liu, B. H., Pham, V. T., & Huang, C. Y. (2016). Network under limited mobile devices: A new technique for mobile charging scheduling with multiple sinks. IEEE Systems Journal, 12(3), 2186–2196.

[19] Preeth, S. S. L., Dhanalakshmi, R., & Shakeel, P. M. (2020). An intelligent approach for energy efficient trajectory design for mobile sink based IoT supported wireless sensor networks. Peer-to-Peer Networking and Applications, 13(6), 2011–2022.

[20] Priyan, M. K., & Devi, G. U. (2018). Energy-efficient node selection algorithm based on node performance index and random waypoint mobility model on the Internet of vehicles. Cluster Computing, 21(1), 213–227.

[21] Ramprasad, L., & Amudha, G. (2014, February). Spammer detection and tagging based user generated video search system—A survey. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1–5).

[22] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[23] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[24] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core

Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[25] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[26] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[27] Khan, A. Ali, S. Alshmrany, "Enery-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[28] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

[29] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[30] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[31] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[32] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[33] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering siences, 2(3), 528-586.

[34] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 201

[35] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[36] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Networkic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[37] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[38] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[39] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[40] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[41] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[42] SU J W, VASCONCELLOS D V, PRASAD S, et al. 2018 Lightweight classification of IoT malware based on image recognition[C]//HIRONORI K. 2018 IEEE 42nd annual computer software and applications conference(COMPSAC). Piscataway: IEEE, 664–9.

[43] Mohurle S, Patil M. A brief study of wannacry threat: ransomware attack 2017. Int J Adv Res Comput Sci. 2017;8(5):1938–40.

[44] Shaukat K, Rubab A, Shehzadi I, et al. A socio-technological analysis of cyber crime and cyber security in Pakistan. Transylv Rev. 2017;1:84.

[45] Shaukat K, Alam T M, Hameed I A, et al. A review on security challenges in internet of things (IoT)[C]//2021 26th international conference on automation and computing (ICAC). IEEE, 2021: 1–6.