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)

Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network

[1*]Nasir Ayub, [2]Abdul Waheed, [3]Sameer Ahmad, [4]Muhammad Hamza Ali Akbar, [5]Muhammad Zubair Fuzail, [6]Abdul-Hadi Hashmi, [7]Ali Waris, [8]Hamayun Khan

Article Details

Keywords: Deep Neural Network, Internet of Things Networks, Intrusion detection; CNN; BiLSTM; BiGRU

Nasir Ayub
Deputy Head of Engineering Calrom Limited, M1 6EG, United Kingdom. Corresponding Author Email: nasir.ayyub@hotmail.com
Abdul Waheed
Kips Education System Department of Computer Science, Lahore, Pakistan
aw030140@gmail.com
Sameer Ahmad
HITS META, Software Company, Bahria Orchard, Lahore, 54000, Pakistan
sameer@hitsmeta.com
Muhammad Hamza Ali Akbar
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, Pakistan
muhammadhamzaaliakbar@gmail.com
Muhammad Zubair Fuzail
Assistant Professor/ HoD CS&IT Lahore College of Pharmaceutical Sciences
hod.cs@lcps.edu.pk / mzubair1725@gmail.com
Abdul-Hadi Hashmi
HITS META, Software Company, Bahria Orchard, Lahore, 54000, Pakistan
ceo@hitsmeta.com
Ali Waris
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, Pakistan. aliwariskhan512@gmail.com
Hamayun Khan
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, Pakistan. hamayun.khan@superior.edu.pk

ABSTRACT

These days, the Internet of Things (IoT) makes it possible for millions of smart devices and sensors from everywhere to be interconnected and for distributed applications and services to touch all aspects of our lives. IoT has a strong impact on our economy and daily lives, attracting cyber criminals which is why cybersecurity is so important to its ecosystem. Research in cybersecurity has gone on for decades, but because of large-scale IoT devices and new challenges, those old methods are often ineffective. Advances in deep learning can help address IoT intrusions by spotting out of the ordinary behaviors and detecting attacks that have never been seen before. The adoption of the Internet of Things (IoT) in smart manufacturing has recently seen a boost in economic and technological Advancement. As many network attacks have revealed how much detection matters for secure cyberspace. A data preprocessing step and a deep learning model are included in our novel system for identifying network attacks. We have developed a deep learning model, whose structures are based on CNN mechanisms. An evaluation of the model was done to see how they performed in detecting threats on the NSL-KDD dataset. Finding out about cyber security weaknesses within IoT devices before cybercriminals take advantage of them is increasingly difficult, but it is the main technology to secure these devices from attacks. The purpose of the research is to review the tools used for recognizing IoT vulnerabilities, using machine learning techniques with the datasets IoT. During the study, possible flaws in IoT architectures are highlighted on every layer, along with a description of how machine learning helps detect such flaws. An approach for finding and handling vulnerabilities in IoT using machine learning was first proposed and then a recap of recent studies is presented. The approach performs better than other DL- systems that use the NSL-KDD dataset. The accuracy was 81.2%, Recall was 96.30% and the system earned a Precision of 88%. It successfully counters all types of Active, passive, DoS, and DDoS attacks.
.

INTRODUCTION

Due to quick progress in Internet technology, the frequency of network attacks has gone up, leading people to pay more attention to network security [1]. Most cyber attacks aim to interfere with or take valuable data. Network attacks are further grouped as active attacks and passive attacks. In active attacks, the system may be compromised or unavailable, but in passive attacks, details about its features are retrieved from scanning its open ports and weaknesses [2–4]. They act as a defense by seeing all the events on a network, analyzing traffic and keeping computer systems secure [5]. In [6] initial intrusion detection system has led to many approaches being used in this area. It has recently been found that mainstream IDSs mostly consist of two separate parts. In the beginning, you will process the data by performing feature engineering and mitigating data imbalances. The second section is about constructing classifiers. By comparison, intrusion detection must respond to two specific scenarios. In the first example, network changes can be analyzed with regression-based methods for detecting and preventing intrusions. As an example, both network history and intrusion data can be put to use when training to develop models for anticipating variations in network parameters, for example, the k-barrier value (as in [7-9]). When network data is observed live and compared to what was predicted, any unauthorized actions can be identified promptly and appropriate responses such as cutting off abnormal traffic or notifying system staff can be made. Machine learning is mainly applied for classifying intrusions in the second situation [10]. For intrusion classification, a model is developed by using known intrusion cases, allowing the model to group incoming data into separate categories, etc. Figure 1 represents the Generalized IoT vulnerabilities in Networks.

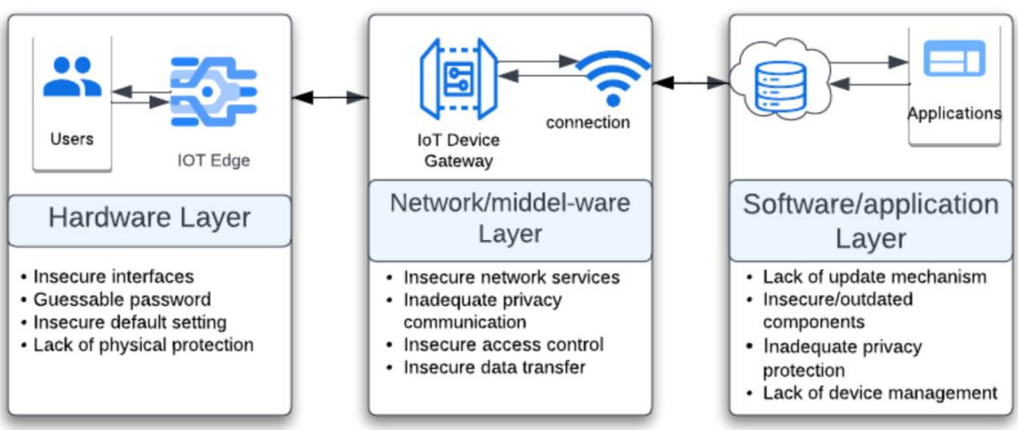


FIGURE 1: GENERALIZED IOT VULNERABILITIES IN NETWORKS [11]

Here you will learn about the components that carry the data over a network. They matter a lot in data collection systems. Most data collection methods in today's networks rely on packets, flows and logs. Also, the controllers in Software Defined Network (SDN) are useful network components that play a role in data collection [12, 13]. Sent test packets are used in active packet testing to actively gather information about a network while its usual traffic is also sent. They offer a way to check the performance of your network. We use the response of the network to these packets to understand how smoothly the network is operating [14-17]. What makes this method useful is that it is simple to control. Simple active probing methods such as "Trace out" and "ping" can be applied without having to work with the target system. However, the most typical active approaches depend on many network management protocols and these are discussed below. Most often, packet-based systems use sniffers under central control to collect data from computer networks. The best-known packet capture tools Wire Shark and TCP Dump work by sniffing packets. Most of the time, a packet will be received only by a Network Interface Card (NIC) if its destination Media Access Control (MAC) address is the same as the MAC address of the host attached to the NIC [18-23].

MACHINE LEARNING TECHNIQUES IN DETECTING ATTACKS IN THE IOT HARDWARE LAYER

In recent days, many researchers have turned their focus to how ML and DL can be applied to detect and prevent intrusions. Several recent papers [24-27] studied agricultural IoT security, proposing a federated-based system for detecting attacks. The potential of discovering vulnerabilities automatically becomes clear when we consider that machine learning and deep learning can recognize patterns, learn from these, and react to new developments [28, 29]. Figure 2 represents the Numerous IoT Themes based on Machine Learning Techniques. Prevention from active threats as well as the identification and management of menaces to IoT devices are made better due to ML and DL techniques. Particularly, DL approaches identify and categorize possible risks present in large data volumes from IoT. Besides, using DL makes it possible to check for threats throughout the entire IoT system early in the process. Many researchers have recently designed DL-based approaches [30, 31]. They built their DL-powered solutions using three types of classifiers: deep neural networks (DNNs), convolutional neural networks (CNNs) and recurrent neural networks (RNNs). These methods were checked against two different datasets, CSE-CIC-IDS2018 and InSDN [32].

fxn

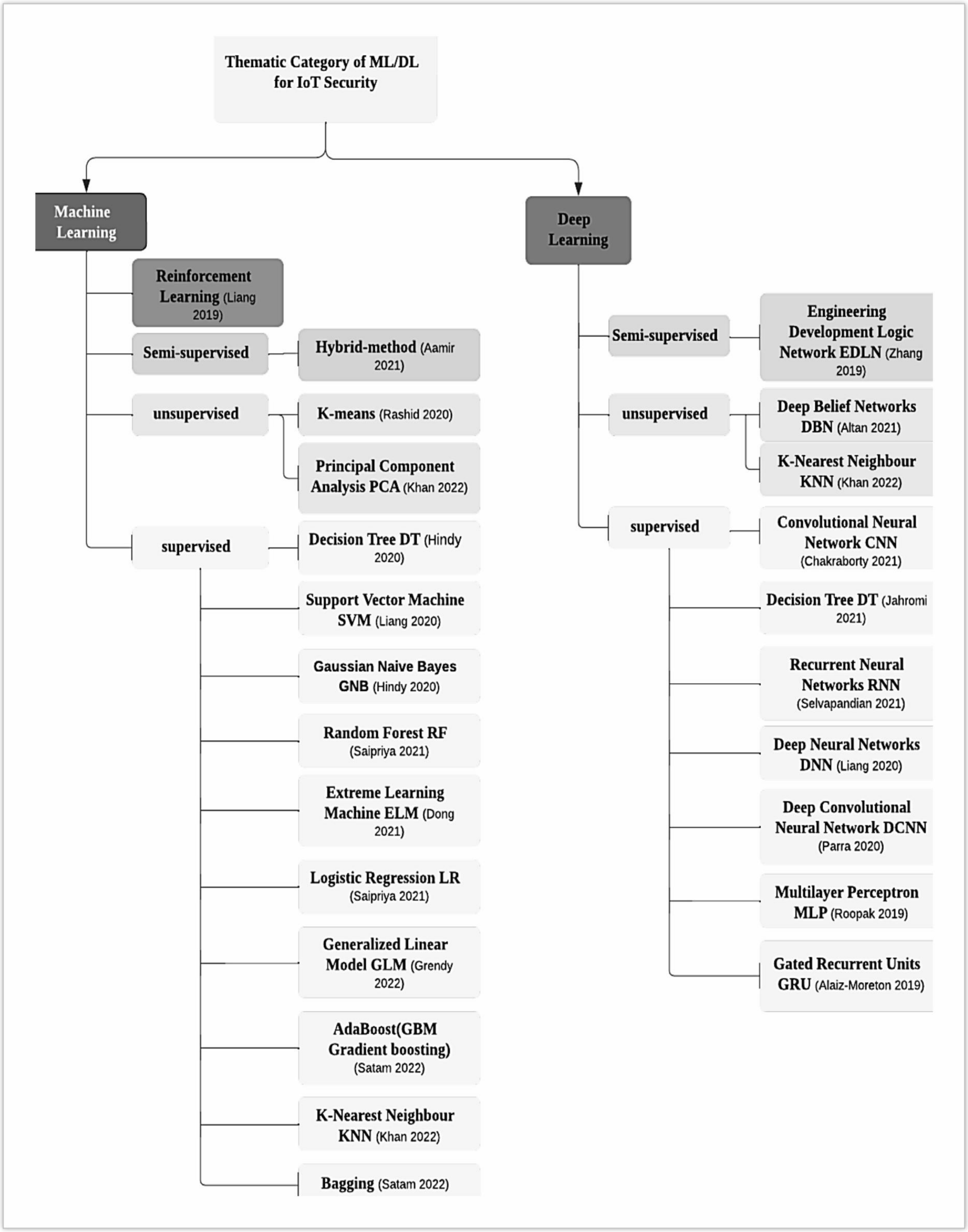


FIGURE 2: NUMEROUS IOT THEMES BASED ON MACHINE LEARNING TECHNIQUES [33]

According to the results, RNN presented the highest accuracy for traffic2018 and CNN was best for the second dataset. Also, Jain et al. applied an intrusion detection system that includes a neural network to detect and stop suspicious devices in IoT healthcare systems. Applying real data allowed the study to achieve an accuracy of 99.4% [34].

RELATED WORK

An NIC also works in a promiscuous mode which means the host will collect any packet, did the packet belongs there or not. This form of data collection seems to work well and is convenient for hosts in many circumstances. A method suggested by the author uses a packet sniffer located on the host NIC to observe and look at incoming packets [23, 24]. DFI technology is another type of flow monitoring approach. It identifies flow based on the behavior characteristics of flow. For example, packet length is an important and effective behavior feature of flow [35, 36]. In a VoIP connection, the packet length of a voice message is usually between 130 and 220 bytes and the active flow often stays for a long time [37]. Thus, a DFI mechanism applies specific features compared to normal flow detection approaches. Afterward, its latter process analyzes the content of data packages and compares them to attack features stored in a presupposed library. As a result, corresponding hardware or software modules control access rules and discard unexpected packets [38-42]. 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.

$$a_{i,j}^{m} = \begin{cases} 1, & rand \leq sigmoid(v_{ij}^{m}) \\ 0, & 1 \end{cases}$$

Eq (1)

$$sigmoid(v_{ij}^{m}) = \frac{1}{1 + e^{-v_{ij}^{m}}}$$

Eq (2)

Lately, feature selection practitioners have turned to metaheuristic algorithms because of their strong global search skills [43, 44]. Examples of widely adopted metaheuristic algorithms are Genetic-Algorithm (GA), Particle Swarm Optimization (PSO), Whale Optimization Algorithm (WOA), Grey Wolf Optimization (GWO), Simulated Annealing and similar. The PSO algorithm developed by Kennedy and his colleagues draws ideas from how flocks of birds respond to each other [45, 46]. Particles model the way birds also hunt and move across a range to find the best solution. A random group of particles is produced in the search space and each particle suggests an answer to the problem. Changing their speed enables particles to choose their path and move a certain distance. When going to a new position, particles use their own best positions and the best place for the group together to head toward the best position [47, 48]. As a result, the population as a whole finds out the best possible outcome.

TABLE 1: ANALYSIS OF ML/DL-BASED IOTS APPROACHES

Technique	Description	Limitations	Ref
ANN-based Security Framework	Adaptability to evolving threats	High computational demands	[49, 50]
RNN-based Security Framework	Automated recovery, cost-effectiveness	Requires SDN integration	[51,52]
LSTM-based Security Framework	Minimized false negatives, scalability	Dataset quality issues	[53]
DT-based Security Framework	Improved trust and interpretability	Complexity in implementation	[54, 55]
ANN-based Security Framework	Adaptability to evolving threats	High computational demands	[56, 57]
Machine Learning	High accuracy, real-time detection	Dataset biases	[58]
Deep Reinforcement Learning	Adaptability to evolving threats	High computational demands	[59,60]
Explainable AI	Improved trust and interpretability	Complexity in Implementation	[61, 62]
DBAR Mechanism	Automated recovery, cost-effectiveness	Requires SDN integration	[63]
API Security Framework	Minimized false negatives, scalability	Dataset quality issues	[64]
Autoencoder Models	High accuracy, feature extraction	Real-time adaptability	[65]

Both traditional Q-learning and DQN algorithms can improve performance on Network navigation and manipulation when tested on a selected set of benchmark problems [66]. As the third iteration of the Internet grew, the main idea discussed became the Internet of Things (IoT). The Medical Internet of Things refers to a set of connected medical tools that support healthcare by running procedures and providing services [67]. The network recording system often uses log files for documenting events. An event log and a message log may both be part of the log. It captures information about users' activities, and the state of different events and fails during diagnosis if needed. When you switch on a service, its log file is automatically created. Since users are concerned about their privacy, these message logs such as those for IRC and chat, are commonly encrypted by providers. It is traditional to gather information by looking at event logs.

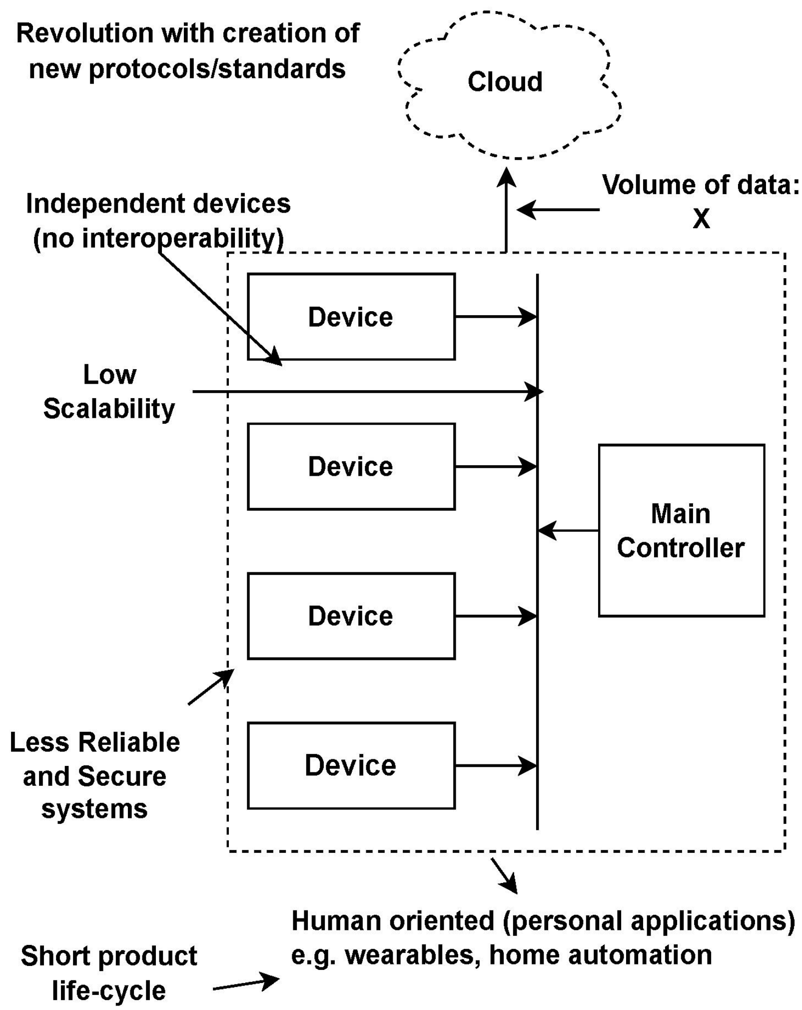


FIGURE 3: GENERAL FRAMEWORK FOR ML-BASED SECURE IOTS [68]

The logs are made up of operating system logs, Web logs and equipment logs, according to the sources. There is no fixed way to format log files. Determining how many log files there are in every class is more difficult than we can handle. Nevertheless, logs generally have certain typical features. As an illustration, while a routine is in progress, every line of log information is written down along with the date, exact time, operator and actions [69]. Log detection provides another solution for collecting data. The distinction is that, unlike many collection techniques, log files are usually written to persistent storage. However, log data fills up much of the system's memory, has very little information per unit and the file format is often complex. Existing approaches suggest that automatic and adaptive methods can answer these types of problems [70].

VULNERABILITY DETECTION AND CLASSIFICATION SYSTEM

Detecting IoT vulnerabilities is made possible by using models that spot the usual appearance of these vulnerabilities, in a manner familiar to instance-based models based on CVEs and CWEs. Still, the model could be developed to spot unknown threats in IoT ecosystems by examining the details and features of packets moving within such systems and then identifying the vulnerabilities they might bring. The model suggested in [71] might be improved to fit the IoT ecosystem better. Figure 4 demonstrates that the approach used to spot vulnerabilities in IoT devices is consistent with that followed in some past studies. Essentially, ML should take three main actions: prepare the data, make a model and implement the model so that it can detect and classify different vulnerabilities and attacks.

DATA COLLECTION

Collected data by from NSL-KDD dataset networks that share IOT data with mobiles and computers; the traffic used in this experiment includes regular use and suspicious traffic used in potential attacks. Types of data include network traffic, logs, or similar kinds of info. Training a model means it can learn (define) the best values for all weights and biases by using data that has been trained before. The strategy depends on the algorithms chosen; for supervised learning, costs are minimized by ordering many examples and using methods to build a useful model [72]. Typically, part of the main dataset is used by dividing it into training data and excused (tested) data for training the predictive model.

DATA PREPROCESSING

The use of ML methods, particularly with heterogeneous data, depends on giving the data a thorough clean before analysis. It seeks to find errors and correct them using different machine-learning algorithms. In specific situations, the data have to be cleaned and reformatted.

What you do at this stage can change the outcome of the whole procedure. Accuracy, balance and completeness are the elements by which data quality can be judged [73]. Mistakes in this stage may create major problems for the predictive models. Some of the problems with the data are simple, including empty columns, duplicated rows and, at times, various types of data. You should start with screening the data which focuses on correcting every mistake within the dataset. After that, we need to choose features that will identify the most important inputs. After that, you transform your data which involves either resizing or grouping your variables. After that, techniques are put in place to produce new elements using the existing data. The final stage, less dimensional, is designed to give shorter predictions of the data.

FEATURE EXTRACTION

The goal is to figure out which features from the data are the most valuable for the model which might be achieved using DL and preparing some useful characteristics for decision making. In some situations, this part is taken care of by the DL model because it learns to perform it by itself during training, making DL much simpler to work with than other types of ML. 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. The Conv1d sections of the four suggested models are shown in Fig. 5a and an explanation of their architecture is provided in Fig. 5b. The Multi-Conv1d is a neural network that applies multi-scale 1D convolution. Every network layer uses three convolution kernels, each having a different size. With Conv1d, you can process sequences because the convolution kernels are moved over the sequence, so it can detect features that vary from small scale to broad scale. Smaller values in the kernel find more details in the neighborhood, but bigger values find longer patterns. After pooling operations are used, the data is made less complex by a fully connected layer meant for classification.

Figure 4 shows the Proposed Framework for ML-based Vulnerability Detection and Classification System.

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

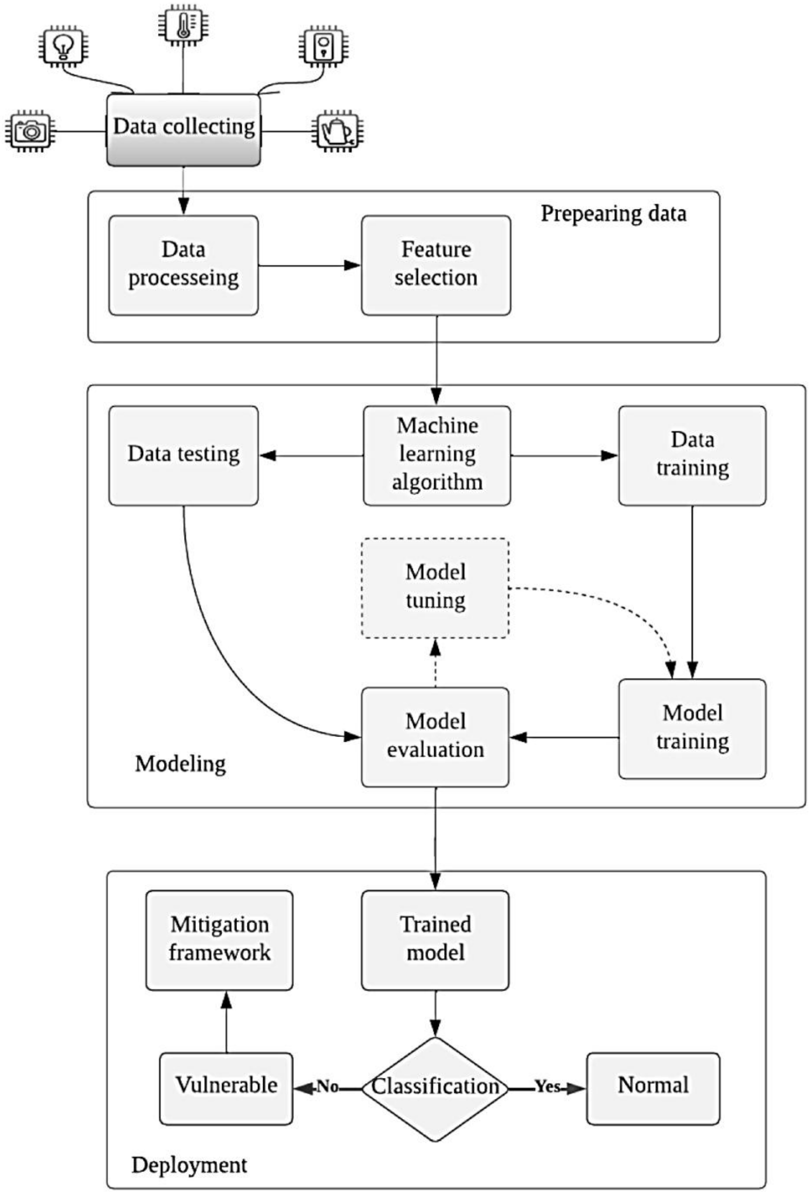


FIGURE 4: PROPOSED FRAMEWORK FOR ML-BASED VULNERABILITY DETECTION AND CLASSIFICATION SYSTEM

MODEL EVALUATION

This aims to evaluate the trained model using various metrics with predicted models to assess the quality of the ML model, such as calculating the accuracy, precision, recall, and F1 in these algorithms to ensure effectiveness.

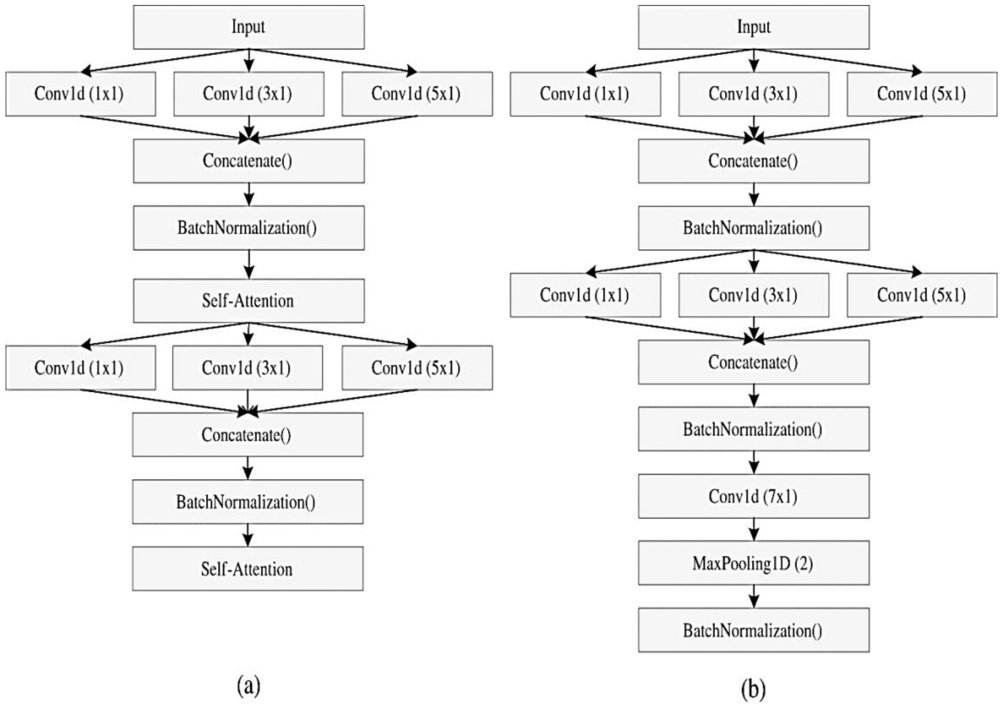


FIGURE 5: DEMONSTRATION OF (A) MULTI-CONV1D-SELF-ATTENTION-HEAD (B) MULTI-CONV1D-HEAD FOR SECURE DATA TRANSFER

Figure 5 shows the Demonstration of (a) Multi-Conv1d-Self-Attention-Head (b) Multi-Conv1d-Head for Secure data transfer. 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.

$$f_t = \sigma(W_f x_t + W_f h_{t-1} + b_f) \quad \text{Eq (3)}$$

$$i_t = \sigma(W_i x_t + W_i h_{t-1} + b_i) \quad \text{Eq (4)}$$

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 (5) (6) and 7.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)}$$ Eq (5)

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)})$$ Eq (6)

$$o_t = \sigma(W_o x_t + W_o h_{t-1} + b_o)$$ Eq (7)

$$\tilde{c}_t = tanh(W_c x_t + W_c h_{t-1} + b_c)$$ Eq (8)

As shown below in Eq. (9) 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 (9)

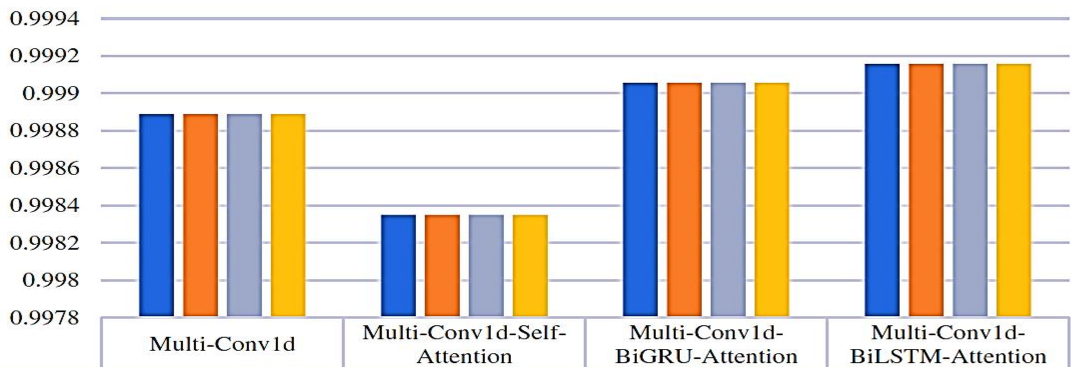
RESULTS AND CLASSIFICATION OF PERFORMANCE

Research has shown us several opportunities for immediate further investigation using network measurements. To start, focusing on data reduction in data collection means less accurate and quality data is collected. With big data now the standard, handling vast amounts of data is where we should start. The majority of current systems have the collectors gather all incoming network data. Yet, not all of these attributes are necessary for working with or studying the corresponding data. Because of the limited resources of wireless sensors and the lack of benefit from data, storing a lot of information is not necessary. We looked into traffic forecasting and data sampling as part of some schemes we considered. As seen in Table 1 experiments reveal a study of network faults in a multiple node scenario. Moreover, an effective, accurate and flexible scheme for selecting samples in the literature is still missing. For this reason, how data is collected and used is still an open question for ongoing study.

The development sequence from WEP to WPA3 is represented in Eq (10) and Eq (11) and Eq (12) 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.

$$i_t = \sigma(W_i.[h_{(t-1)}, x_t] + b_i), \quad \text{Eq (10)}$$

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.



	Multi-Conv1d	Multi-Conv1d-Self-Attention	Multi-Conv1d-BiGRU-Attention	Multi-Conv1d-BiLSTM-Attention
Accuracy	0.998889	0.99835	0.999057	0.999158
Precision	0.998889	0.99835	0.999057	0.999159
Recall	0.998889	0.99835	0.999057	0.999158
F1-score	0.998889	0.99835	0.999057	0.999158

FIGURE 6: COMPARATIVE ANALYSIS OF RENOWNED MODELS WITH THE PROPOSED MODEL USING NSL-KDD DATA SET

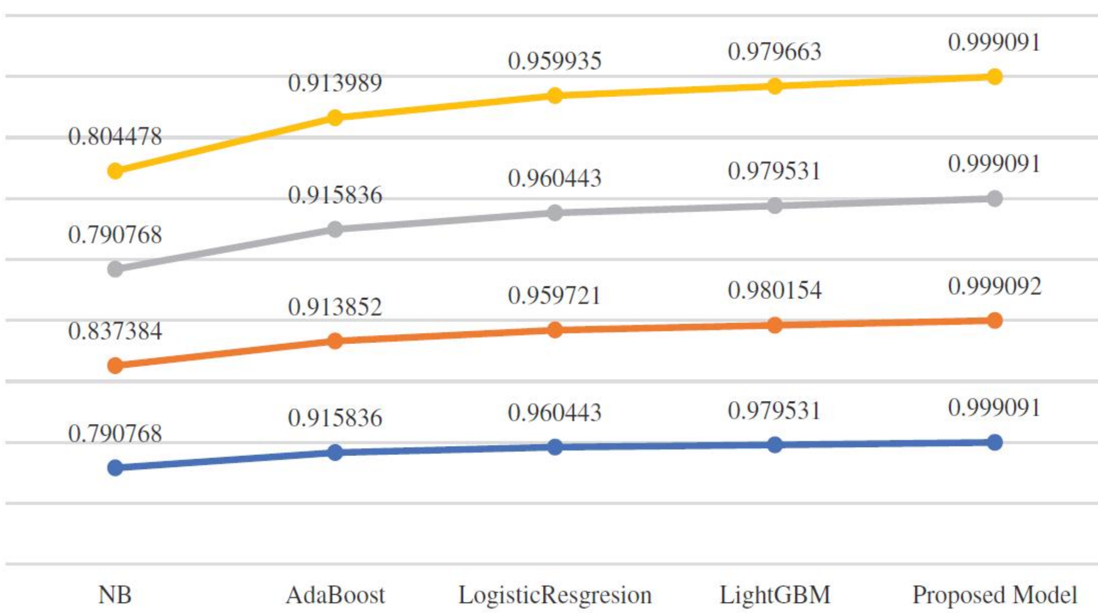


FIGURE 7: COMPARATIVE ANALYSIS OF THE PROPOSED MODEL WITH CURRENT ML MODELS

TABLE 1: ANALYSIS OF ML MODEL WITH PROPOSED USING NSL-KDD DATASET

Parameter	CNN	LSTM	SVM	DT	RF	Proposed Model
Accuracy	0.3985	0.243	0.144	0.5431	0.1785	0.1785
R^2 Score	0.3785	0.2785	0.1785	0.3985	0.4321	0.4321
Loss	0.3321	0.2321	0.4321	0.2644	0.1785	0.1785
F-1 Score	0.4785	0.2785	0.485	0.1785	0.4785	0.2785
Specificity	0.6985	0.343	0.51	0.4321	0.6985	0.343
Sensitivity	0.7531	0.255	0.631	0.7531	0.7531	0.255
Delay (ms)	2.340	1.101	1.221	2.341	1.123	0.2112
Detection %	55.2	68.56	50.13	55.2	68.56	70.63

TABLE 2: COMPARATIVE ANALYSIS OF PROPOSED MODEL WITH STANDARD RESULTS

Reference	Normal	DOS %	Probe %	R2L %	U2R%	Data Rate
[74]	3.198	2.581	3.581	0.3411	3.916	0.64 bps
[75]	2.118	3.1	3.198	0.5431	1.5	0.61 bps
[76]	3.4	2.581	1.41	0.6321	1.1	0.72 bps
[77]	3.198	3.5	3.198	0.7531	1.51	0.83 bps
[78]	1.41	5.1	2.1	0.8451	3.1	0.97 bps
[79]	1.51	1.21	3.1	0.6751	2.51	0.86 bps
[80]	2.41	5.1	3.581	0.3411	3.916	0.64 bps
[81]	6.55	4.21	4.3	0.5431	5.5	0.61 bps
[82]	7.11	5.1	3.581	0.6321	5.1	0.72 bps
[83]	3.8	3.198	2.581	0.7531	1.51	0.83 bps
[84]	4.1	2.118	3.1	0.8451	3.1	0.97 bps
[85]	4.128	3.4	2.581	0.6751	1.51	0.86 bps
[86]	5.7	5.1	3.1	0.3411	7.11	0.64 bps
[87]	6.55	4.21	4.3	0.5431	3.8	0.61 bps
Proposed	7.11	5.1	3.581	0.6321	4.1	0.72 bps

CONCLUSION AND RECOMMENDATIONS

We offer an approach to intrusion detection that relies on deep neural networks in this paper. In this article, we have worked with the NSL-KDD dataset which holds information on malware and five types of network traffic. Better technology is helping things run smoother and making them simpler to use. Because these models have high energy requirements, applying them is not easy. Experts think that, as deep learning progresses, it will provide better malware detection results than using traditional methods. Watching out for certain trends in malware detection is important as we search for ways to tackle strong cyber hazards. Handling the problems brought by malicious code will make cyber defense systems better and easier to use. The Proposed System achieves better results using the NSL-KDD dataset system than it does with Deep Learning and Machine Learning systems. The approach performs better than other DL- systems that use the NSL-KDD dataset. The accuracy was 81.2%, Recall was 96.30% and the system earned a Precision of 88%. It successfully counters all types of Active, passive, DoS, and DDoS attacks. Multi-Conv1d-Self-Attention is the least effective of all the models studied. Because it has the fewest parameters, running it is possible in places where system resources are not plentiful. In terms of practical use, the model chosen ought to be influenced by what resources are available including the performance needs. On the other hand, it likewise indicates that down the road, we will need to experiment with advanced models that do more work and need less computing power to make the being able to use intrusion detection methods.

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

REFERENCES

[1] Bertino, E., Kantarcioglu, M., Akcora, C. G., Samtani, S., Mittal, S., & Gupta, M. (2021, April). AI for Security and Security for AI. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (pp. 333-334).

[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] 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.

[4] Mohurle S, Patil M. A brief study of wannacry threat: ransomware attack 2017. Int J

Adv Res Comput Sci. 2017;8(5):1938–40.

[5] 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.

[6] 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.

[7] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in 2015 National Aerospace and Electronics Conference (NAECON). IEEE, 2015, pp. 339–344. [42] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," Ieee Access, vol. 5, pp. 21 954– 21 961, 2017.

[8] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2016, pp. 258–263.

[9] Saiyed, A. (2025). AI-Driven Innovations in Fintech: Applications, Challenges, and Future Trends. International Journal of Electrical and Computer Engineering Research, 5(1), 8-15.

[10] 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.

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

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

[13] 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.

[14] 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.

[15] 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

[16] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on

Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[17] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[18] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[19] 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

[20] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[21] 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.

[22] 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

[23] 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, Oct. 2018

[24] 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 sciences, 2(3), 528-586.

[25] 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

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

[27] 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

[28] 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.

[29] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[30] 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. 2018

[31] 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.

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

[33] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[34] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[35] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic 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

[36] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[37] 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

[38] 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.

[39] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[40] 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

[41] 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

[42] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[43] Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. ENHANCING THE RESILIENCE OF IOT NETWORKS: STRATEGIES AND MEASURES FOR MITIGATING DDOS ATTACKS. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

[44] 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.

[45] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[46] Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

[47] Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

[48] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[49] 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

[50] 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

[51] Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

[52] Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

[53] Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

[54] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance

Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[55] Khan, H., Ali, A., & Alshmrany, S. (2023). Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs. Computers, Materials & Continua, 75(1).

[56] Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

[57] Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

[58] Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

[59] Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

[60] Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). 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, 14(4), 442-452.

[61] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[62] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[63] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[64] Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

[65] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

[66] Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

[67] Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

[68] Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

[69] Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

[70] Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

[71] Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

[72] Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

[73] Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

[74] Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

[75] Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

[76] Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

[77] Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

[78] Hashmi, U., & ZeeshanNajam, S. A. (2023). 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, 14(4), 442-452.

[79] S. A. Ludwig, “Intrusion detection of multiple attack classes using a deep neural net ensemble,” in 2017 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, 2017, pp. 1–7.

[80] A.-H. Muna, N. Moustafa, and E. Sitnikova, “Identification of malicious activities in industrial internet of things based on deep learning models,” Journal of Information Security and Applications, vol. 41, pp. 1–11, 2018.

[81] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. A. Calero, “Virtual iot honeynets to mitigate cyberattacks in sdn/nfv-enabled iot networks,” IEEE Journal on Selected Areas in Communications, pp. 1–1, 2020.

[82] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM computing surveys (CSUR), vol. 41, no. 3, p. 15, 2009.

[83] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," Journal of Network and Computer Applications, vol. 84, pp. 25–37, 2017.

[84] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, "Enhancing iot security through network softwarization and virtual security appliances," International Journal of Network Management, vol. 28, no. 5, p. e2038, 2018.

[85] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

[86] B. Subba, S. Biswas, and S. Karmakar, "Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis," in 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, 2016, pp. 1–6.

[87] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Managing aaa in nfv/sdn-enabled iot scenarios," in 2018 Global Internet of Things Summit (GIoTS). IEEE, 2018, pp. 1– 7.