Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

AN EFFICIENT MACHINE LEARNING AND DEEP LEARNING BASED DEEP PACKET SECURITY FRAMEWORK FOR DETECTION OF COMPUTING NETWORK FAULTS IN THE IOTS

Nasir Ayub[*1], Akif Ejaz[2], Bilal Hassan[3], Muhammad Zunnurain Hussain[4], Maseerah Nadeem[5], Laiba Sabir[6], Seerat Fatima[7], Hamayun Khan[8]

[*1]*Deputy Head of Engineering, Calrom Limited, M1 6EG, United Kingdom*
[2]*Department of Computer Engineering, Information Technology University, Lahore, Pakistan*
[3,5,6,7,8]*Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, Pakistan*
[4]*Department of Computer Science, Bahria University Lahore Campus*

[*1]nasir.ayyub@hotmail.com, [2]akifejaz40@gmail.com, [3]bilal707355@gmail.com, [4]zunnurain.bulc@bahria.edu.pk, [5]maseerahnadeem14@gmail.com, [6]laibasabir81@gmail.com, [7]seeratfatima5688@gmail.com, [8]hamayun.khan@superior.edu.pk

DOI: https://doi.org/10.5281/zenodo.15487598

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

Article History
Received on 14 April 2025
Accepted on 14 May 2025
Published on 22 May 2025

Copyright @Author
Corresponding Author: * Nasir Ayub

Abstract
In Industry 4.0 deep learning plays vital role as Deep Learning for cybersecurity is applied in healthcare, the software industry and IoTs. Developing deep learning models is difficult, as both the world and the data are always changing. This article proposed an approach based on Deep Learning using an intrusion detection system. It also scrutinizes operations such as supervised operations and unsupervised ones. It introduces a new method for dealing with threats and achieves an accuracy rate of 71.73% in the l73 faulty packets. The article tries to find IoT systems, applications, data and services in the organization that might be vulnerable to cyber attacks due to their persistent connections. Software piracy and increased malware attacks are currently putting IoT security at risk. Once the information has been gathered, DL-IDS decides whether to send data to the fog layer. It demonstrates better results than other DL-IDS systems that were evaluated using the RT-IoT2022 dataset. The Intrusion Detection System with IPS-DL was found to be 71.73 percent accurate. When practicing intrusion prevention, the system's accuracy was 70.63%, recall was at 96.30% and it achieved an F1-score of 92%. It can stop 85% of attacks and holds just 0.23% of the data lost from the sensors, with only 0.11 joules of power needed, as it keeps throughput high at 0.99% and its delivery ratio is ideal at 0.99%.

INTRODUCTION

Networks are now a big part of our daily lives, but they also face many security problems, like cyber attacks and violations. To protect networks, collecting data from them is very important. It helps with monitoring, checking performance, managing traffic, and stopping attacks. However, current data collection methods are not always flexible or suitable for all types of networks, and there is little research that compares how well these methods work [1, 2]. Different network data collection methods and systems, compare their performance, and explain their main features. We also point out some

problems that still exist and suggest ideas for future research to improve data collection in network security [3]. The term Internet of Things (IoTs) describes physical devices that are fitted with sensors or activators and are either connected through wires or wirelessly. It causes people to use technology differently in their daily lives. Smart cities, homes and health sectors are important areas for IoTs. Still, problems relating to security and privacy arise as more people start using smart devices and IoT [4]. Security challenges like node spoofing, unauthorized access and cyber attacks like DoS, eavesdropping and intrusion have become extremely significant. With time, methods based on ML and DL have improved and have helped address security problems in IoT devices. Industry 4.0, or the Fourth Industrial Revolution, is mainly concerned with applying automation and intelligent technologies in various fields [5, 6]. Networks have changed our daily lives in a big way and have become a part of everything we do. Every day, we use many network services and apps that create a large amount of data. While most of this data isn't useful to us, some of it contains important or sensitive information that needs to be collected, protected, and properly managed. However, while we enjoy the benefits of networks, we also face many smart and harmful cyber attacks [7, 8]. These attacks can be of many types, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), viruses, wormholes, or password stealing. To detect and prevent these attacks, we need to collect network data to find out where the network is weak. By knowing these weak points, network administrators can fix problems, prevent future attacks, and improve the overall safety and strength of the network [9]. Figure 1 represents the Generalized Packet Transmission Framework in Networks.

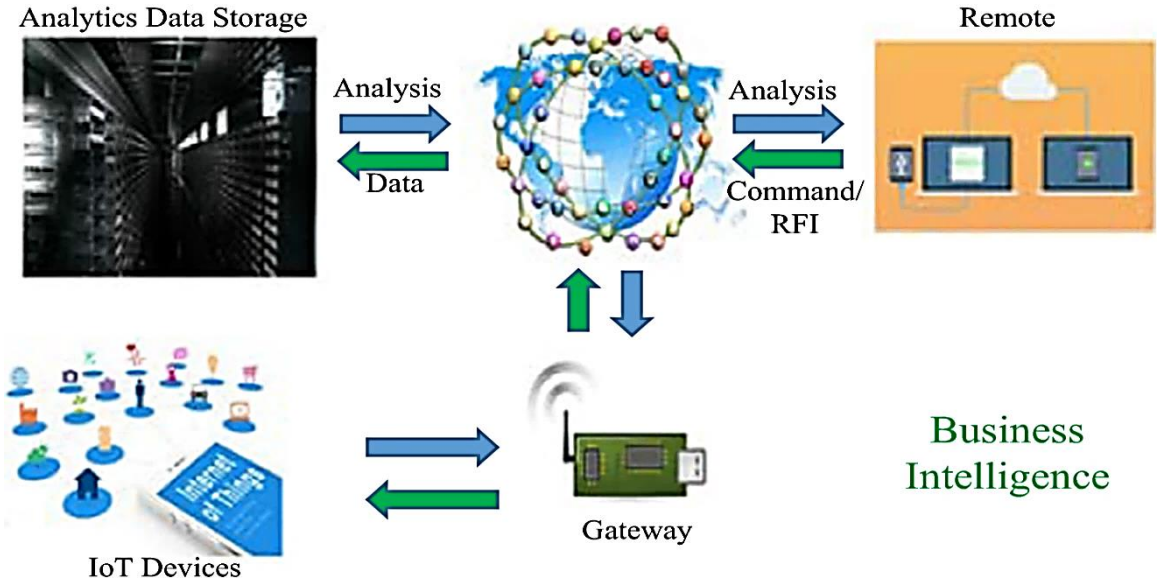

Figure 1: Generalized Packet Transmission Framework in Networks [10]

Collecting network data helps in spotting attacks and also supports network management. With real-time monitoring, testing, and controlling based on data, administrators can understand how well the network is performing, find errors, and make improvements [11]. Figure 2 shows the Standard Neural network extract Intrusion Packet image on ML techniques [12]. These retransmissions do not raise the MAX_RETRANSMIT setting because it generally uses the value 4. The representation of examples using CON and NON messages can be observed

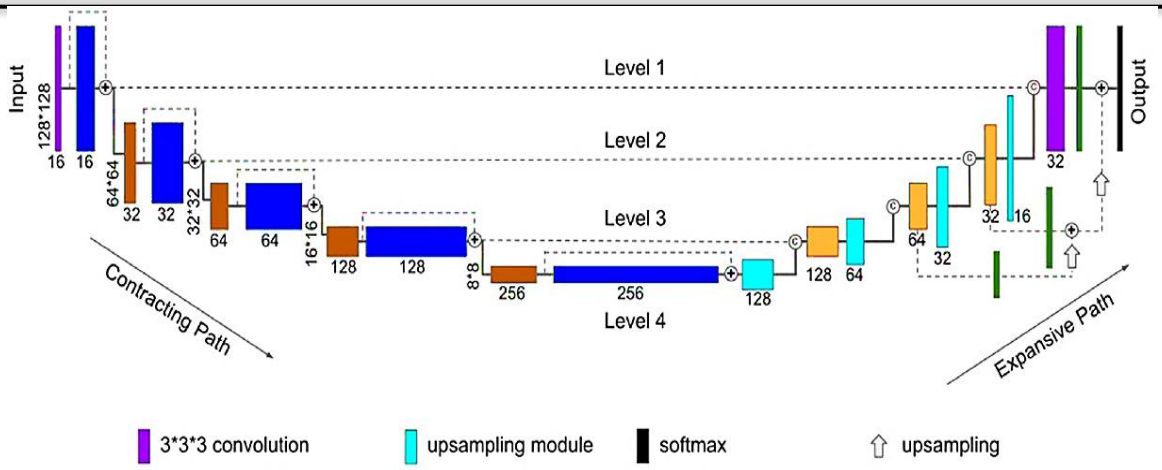

Figure 2: Standard Neural Network extracts Intrusion Packet image on ML techniques

This section briefly introduces the carriers of network data. They are significant for data collection mechanisms. Packets, flows, and logs are widely used in mainstream data collection mechanisms. Besides, some network components, such as the controllers of Software Defined Network (SDN) implement and assist data collection [13, 14]. The data collection mechanisms monitor data flow locally and record available information for network quality measurement, traffic estimation and attack prevention. In what follows, we will briefly introduce three basic types of network data collection methods:

2. ML-based Network Faults and Testing Mechanisms

Machine learning (ML) models can effectively predict and detect network faults, offering proactive solutions for maintaining network stability and performance. These models can analyze network data, identify patterns indicative of potential failures, and even predict future outages, allowing network administrators to take preventative actions [15, 16].

2.1 Active packet testing

Active packet testing is a way to actively collect data from a network by sending special test packets along with the normal network traffic. These test packets help measure the quality of the network. Based on how the network responds to these packets, we can judge how well the network is working [17, 18]. This method is useful because it is easy to control and manage. Common tools like "Trace out" and "ping" are examples of simple active probing methods that do not require cooperation from the target system. However, the most commonly used active methods rely on special network management protocols, which are explained below.

2. 2 Passive Packet Testing

Most of the time, packet-based approaches rely on sniffers and are centrally managed to collect network data. Well-known packet capture tools Wire Shark and TCP dump are both packet sniffers. Most of the time, a packet can only be received by a NIC if the media access card (MAC) of the receiver matches the address in the packet [19-22]. But, when an NIC is set for promiscuous mode, it gathers all the packets that arrive, even if the packets aren't directed at the host. Sometimes, these types of data collection methods work well and are easy to use for single hosts. The author suggested a way to monitor and analyze network traffic by placing a packet sniffer in the computer's network card, using that card as a passive device [23, 24]. Thus, the attacker is able to circumvent LAN rules and capture data from the Internet. Using this approach is simple for deployment directly on a host computer [25, 26].

2.3 Deep Flow Inspection (DFI) mechanisms

DFI technology is a different sort of flow monitoring method. Flow is identified by looking at how someone behaves when in it. One clear behavior of flow is the length of packets it sends and this makes a significant difference [27, 28]. Usually, a message sent over VoIP has a packet length of between 130 and 220 bytes and stays active for quite some time.

So, a DFI mechanism is designed differently than traditional flow detection methods. Subsequently, its later process studies the data packages' contents and checks whether they match the patterns found in the attack features library supplied beforehand. As a consequence, appropriate hardware or software controls access rules and dumps all unexpected packets [29, 30].

2.4 Deep Packet Inspection (DPI)

The internet is used to connect smartphones with medical professionals by acting as a communication proxy. It allows for using both HTTP and CoAP on the doctor's smartphone, improving how the device can access server functions [31, 32]. With CoAP technology, devices can exchange data efficiently, with fewer constant data transfers between the server and the client. Both the server and the client work together to retrieve information from the medical sensors. It works by responding to the system at intervals, rather than constantly [33, 34]. Using CoAP as the IoT protocol is beneficial because it is lightweight and relaxing for all devices [35]. It runs efficiently, keeping CPU workload low, consuming little memory and making power efficient. The research team in [36] constructed and carried out an IoT messaging system for use in healthcare settings. It functions efficiently with a range of IoT devices by providing dedicated communication routes. Because the devices spend more time waiting for requests, they have less time for other activities [37, 38].

How information is shared between Smart Grid devices depends on the communication protocol, as OSGP cannot be used with IoT devices that use CoAP. IoT devices generally use CoAP for communication, but they do not integrate CoAP into their design. CoAP and OSGP Integration ensures that data packets are correctly converted from CoAP to OSGP, following the descriptions from [39, 40]. Each request-response interaction goes through the mapping function. First, the GET method is handled by the MicroCoAP library and then the mapping takes place. When an IoT device gets a data packet through CoAP, it uses the OSGP partial read request to process it. The program obtains the type of request, the message ID and the packet size from the CoAP messages received. Their content is checked to ensure it is the same as the content delivered by OSGP requests [41, 42]. 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 1.

$$PDR = \frac{Total\ no.of\ packets\ received\ (x_i)}{Total\ no\ of\ packets\ sent\ (y_i)} \quad \text{Eq (1)}$$

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 [43, 44]. 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 [45, 46]. The data transmission method between shared and public internetworks uses headers to contain data as described in [47]. 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 [48, 49]. 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 [50]. 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 [51, 52]. Figure 3 represents the Working Framework for ML based Secure IoTs [53]

$$B = \{B_1, B_2, \ldots, B_k, \ldots, B_l\} \quad \text{Eq (2)}$$

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v \quad \text{Eq (3)}$$

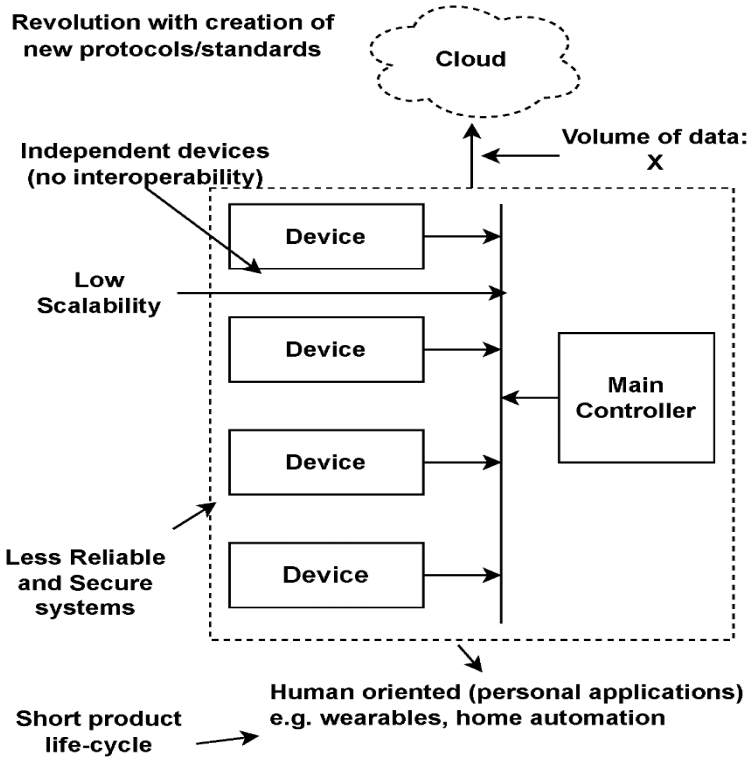

Figure 3: Working Framework for ML-based Secure IoTs [53]

2.1 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 [54]. 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 [55-58]. 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 [59, 60]. Figure 4 below represents the SDN Model used for Secure Network.

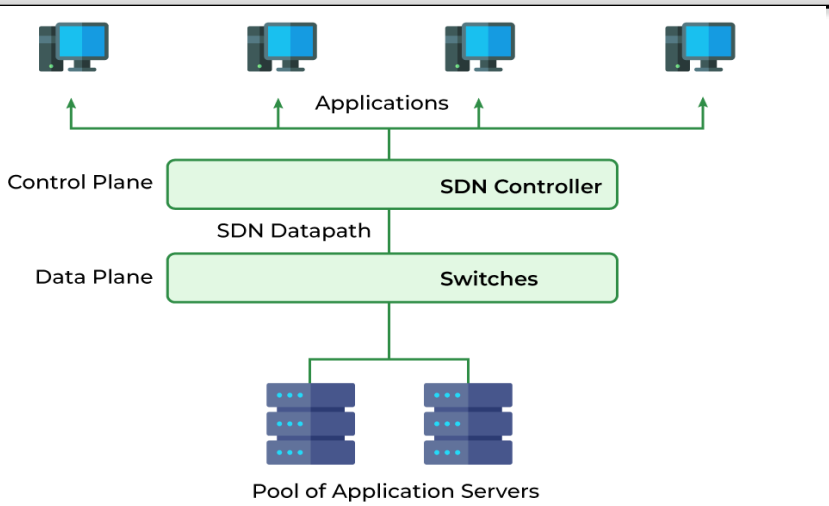

Figure 4: Generalized SDN Model used for Secure Network [61]

Table 1: Comparative Analysis of Numerous Approaches for IOTs stable performance

Approach	Strengths	Limitations	Ref
Machine Learning	High accuracy, real-time detection	Dataset biases	[62, 63]
Deep Reinforcement Learning	Adaptability to evolving threats	High computational demands	[64,65]
Explainable AI	Improved trust and interpretability	Complexity in implementation	[66, 67]
DBAR Mechanism	Automated recovery, cost-effectiveness	Requires SDN integration	[68, 69]
API Security Framework	Minimized false negatives, scalability	Dataset quality issues	[70]
Autoencoder Models	High accuracy, feature extraction	Limited real-time adaptability	[71]
CNN-based Security Framework	High accuracy, real-time detection	Dataset biases	[72]
ANN-based Security Framework	Adaptability to evolving threats	High computational demands	[73]
RNN-based Security Framework	Automated recovery, cost-effectiveness	Requires SDN integration	[74]
LSTM-based Security Framework	Minimized false negatives, scalability	Dataset quality issues	[75]
DT-based Security Framework	Improved trust and interpretability	Complexity in implementation	[76]

3. 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.

3.1 Packet-based data Collection

In the TCP/IP world, packet serves as a vital way to transport information. In a packet-exchanging network, useful information is split into packets. The packets sent from the source node by the source node to the host include the source and destination addresses. As soon as packets are delivered to the

destination, the data is decoded and brought together to be useful. Different networking protocols use different formats for packing data. The packet consists of both a packet header and its payload. The header guides a packet through a network and shows where the packet is from. In several data collection techniques, it is the header that makes it possible to identify and filter data packets. In this case, some header-based methods divide packets into various flows by looking at their IP addresses, ports and protocols found in the header. All the information being exchanged between parties is called the payload, but some data might be encrypted

3.2 Flow-based data collection

It is also important to use network flow collection for network data collection. In flow, certain packets with identical characteristics pass through a specific point during a particular period. You can carry out network flow monitoring at all points on your network. Therefore, monitoring and controlling network core devices on the network is most helpful, as they have access to considerable information about intrusions. Consequently, flow collection at network core devices is used the most by data collection applications today. Flow collection is found at both network edge devices and hosts. Unlike core devices, hosts only watch for data transferring through them and keep flow records accordingly. The inside switches and hosts in edge nodes and gateways have their network activity observed. Using monitoring and collection, there are three layers in the inbound and outbound flow structure: data plane, control plane and application plane. Network architecture is applied by dividing functions into control and forwarding. Negotiated networking strategies are enforced by the control plane and implemented by the data plane which forwards or discards the network traffic correctively. OpenFlow is widely recognized as the main protocol and API for uniting the control plane and data plane in SDN. Flow in an Open Flow architecture acts as a way to store flow tables. All the information in a flow table determines how packets will be handled. All packet-related operations, for example packet forwarding, dropping, matching and classification, happen directly in the data plane.

3.3 Log based data collection

These days, log file is a popular data format in recording systems for network actions. An event log and a message log can make up the log. All user steps, status of events and cases of system failure during diagnosis are logged in the event log. When any service is started, its log file is generated. Because people worry about privacy, service providers usually encrypt message logs like IRC and IM. Event logs are commonly utilized when collecting data. Sources say that log data includes operating system logs, Web logs and logs from different equipment. There is no set way logs are organized into files. Calculating the number of log files in each type of class is very difficult. Still, logs have certain features that are the same across them. For example, while a routine is running, each line of the log writes down the information to record, the date, the exact time, the operator and the action in appropriate places. Log detection is another mechanism applicable for data collection. Contrary to other collection mechanisms, the log files are mostly stored in persistent storage. However, the log files usually occupy a large memory, have low information density and apply complex file formats. To solve these tricky problems, automatic and adaptive solutions are proposed in previous work.

3.4 Machine Learning based Secure Network Fault Detection System

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 5 below shows how Proposed Secure communication

and data transfer in IoT is done system using RT-IoT2022 UCI Machine Learning dataset

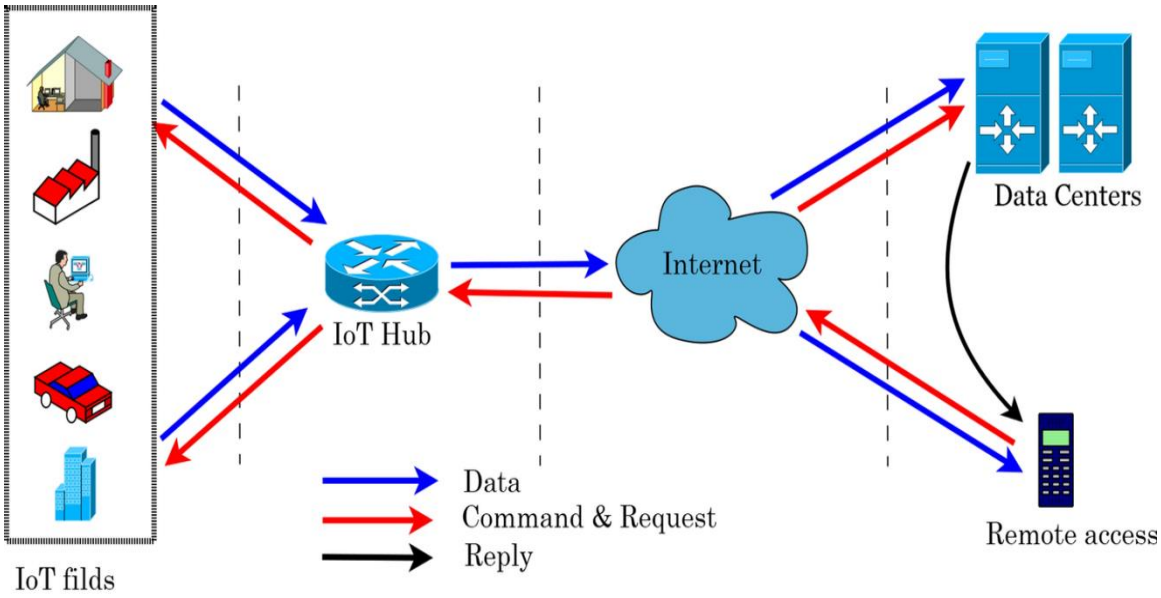

Figure 5: Demonstration of Proposed Secure communication and data transfer in IoT system using RT-IoT2022 UCI Machine Learning dataset

Figure 5 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.

$$f(x) = w^T a + \quad b$$

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)

$$P(w) = \sqrt{\frac{t}{f(w)}} + \frac{t}{f(w)},$$

Eq (7)

Even after AES encryption was added to WPA2, the system faced new early flaws that had to be resolved. WPA3 was built to defend wireless networks from the cyber threats of the present age that will affect the forthcoming years. While every protocol has made wireless networks more secure, each state has also

highlighted weaknesses in the wireless link. The old defense system cannot hold back the swift cyber attacks being experienced at present. WPA3 is designed to offer better security for wireless networks used by interconnected systems in the future. Wireless security needs continual updates since it is always changing. WPA3 brings a great improvement, though, since technology is always developing and criminals keep inventing new tactics, managing wireless security will always be a challenge. There was a qualitative approach taken in this research, with the main focus being on explaining Routing protocols by using many different ML tools. The aim is to discover how different Network protocols are designed, stay secure and function. With the help of these resources, this approach strives to design a complete method for modern network functionality.

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

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)

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.

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

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.

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

Eq (11)

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

Eq (12)

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

Eq (13)

4. Results and Classification of Performance

Through our studies, we find that some areas in network data collection require immediate further attention. First, managers aim to cut down data collection by skipping accurate and effective data collection. Now that big data is here, the first focus has become how much data is available. In the majority of existing systems, the collectors are those responsible for gathering network data. Not every needed data can be processed or analyzed using all the tools. Since devices in IoT (such as sensors) have limited capability, we should try to use only the important data needed to reduce the use of resources and memory space at the device side. Some of the schemes we looked at included traffic forecasting and gathering data. The tables below demonstrate the analysis of network faults processed using the RT-IoT2022 files, for several nodes. Furthermore, many literature offerings still lack a technique for collecting data that is highly reliable, precise and flexible. Hence, further studies will need to deal with how much data is needed to properly model a process. Table 2 represents the Analysis of Network Faults using RT-IoT2022 Dataset Multiple Nodes while Table 3 shows the Analysis DOS Attack based on RT-IoT2022 as shown in below section.

Table 2: Analysis of Network Faults using RT-IoT2022 Dataset Multiple Nodes

Data Set	Faulty Node 1	Faulty Node 2	Faulty Node 3	Packet Loss N4	Packet Loss N5	Packet Loss N6	Packet Loss N6	Packet Loss N7	Packet Loss N8	Packet Loss N8
RT-IoT2022	0.011	62.19	3211	56.71	62.19	181,33	211,01	200,25	196,23	202,21
	0.041	57.34	3244	59.89	57.34	211,01	196,23	181,33	196,23	214.11
	0.121	57.78	3364	54.32	57.78	211,01	196,23	211,01	156,13	217.92
	0.034	62.19	3057	52.34	57.34	211,01	181,33	300,12	196,23	60.21
	0.025	62.19	3158	54.32	57.78	196,23	181,33	196,23	217.11	213.68
	0.011	62.19	3211	56.71	62.19	196,23	211,01	156,13	220,3	202,21
	0.041	211,01	200,25	196,23	911.34	211,01	200,25	196,23	911.34	211,01
	0.121	196,23	181,33	196,23	217.11	196,23	181,33	196,23	217.11	196,23
	0.034	196,23	211,01	156,13	220,3	196,23	211,01	156,13	220,3	196,23
	0.025	181,33	300,12	196,23	216.71	181,33	300,12	196,23	216.71	181,33
	156,13	196,23	181,33	196,23	156,13	211,01	200,25	196,23	519.89	211,01
	196,23	181,33	300,12	156,13	196,23	211,01	200,25	196,23	911.34	211,01

Table 3: Analysis based on DOS Attack Using RT-IoT2022

Attack	Method	CNN	LSTM	SVM	DT	RF	Proposed DL-IDS
DOS Attack	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

5. Conclusion and Recommendations

Here, you will learn how to use deep learning technology to identify malware. Technology is making everything more efficient and easier to use. Since they use a lot of energy, it is difficult for these models to be widely applied. Researchers believe that as deep learning improves, its use in malware detection will lead to better results than relying on conventional methods. As we seek solutions for tough cyber threats, we need to watch for trends in malware detection. Addressing the mentioned problems with malicious code will ensure cyber defense systems are more reliable and practical. Using the RT-IoT2022 system, the Proposed System works better than Deep Learning and Machine Learning systems. The detection accuracy of the method is 96.42%. On our proposed IPS that uses DL, our model's anomaly detection can be measured with 70.63% precision, 96.30% recall and a F1-score of 92%. The system can detect 85% of threats by using 0.11 m joules, sending 0.1 packets each second, with 0.21 ms of delay, featuring an efficiency of 0.23% and achieving a throughput of 0.99% at maximum speed. After making the adjustments, the F1 score went up by 4%, the latency fell to 10 ms, energy was reduced to 0.02 W and probability improved by 0.66%. As a result of these models, developers can develop fast-acting intrusion detection systems for IoT networks.

5.1 Future research directions:

Based on what we have outlined above, we suggest a number of future research directions that should receive extra attention. First, data collection approaches are a valuable area for feature investigators to explore. The new mechanisms ought to work well at collecting data in a wide and mixed network of devices. Up to now, most small-scale enterprise architectures and prototypes from researchers have been tested in actual networks. It

remains difficult for today's network operators to securely control and manage different parts of the network.

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

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).

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.

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.

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.

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

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

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.

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.

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

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

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

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.

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

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

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.

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

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

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.

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

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.

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

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.

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

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

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

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

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.

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

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

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

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

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.

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

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

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

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

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

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.

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

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.

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.

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.

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

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

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.

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.

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.

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.

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

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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

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.

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.