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)

Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things

[1*]Nasir Ayub, [2]Muhmmad Abdullah Anwer, [3]Asad Iqbal, [4]Syed Muhammad Rizwan, [5]Amer Shahbaz, [6]Muhammad Haseeb Abid

Article Details

Keywords: Industrial Internet of Things (IIoT); IoT architecture and networks; security, Machine Learning, Deep Neural Network, CNN, Prediction models

Nasir Ayub
Deputy Head of Engineering, Calrom Limited, M1 6EG, United Kingdom. Corresponding Author Email: nasir.ayyub@hotmail.com
Muhmmad Abdullah Anwer
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan. abdullahanwer585@gmail.com
Asad Iqbal
Department of Computer Sciences, National College of Business Administration and Economics (NCBA&E), Lahore, Shark Innovation Labs - Al Sharqi. theasadiqbal.official@gmail.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan. rizwan.naqvi@ieee.org
Amer Shahbaz
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan. akashirshad5@gmail.com
Muhammad Haseeb Abid
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan. haseebch552277@gmail.com
Shoaib Rafi
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan. shoaibnazar7178@gmail.com

ABSTRACT

The Internet of Things (IoT) is rapidly becoming an integral component of the industrial market in areas such as automation and analytics, giving rise to what is termed the Industrial IoTs (IIoTs). The IIoT promises innovative business models in various industrial domains by providing ubiquitous connectivity, efficient data analytics tools. The way an IIoT is designed can become very complex due to its features. The fact that security and privacy are turning out to be very urgent issues. Many models have been released to look into the security challenges of IoT. The studies described, in general, the security issues involved in the IIoTs using ANN based Proposed Model. Included are threats or a determined analysis that highlights specific forms of technology. Even so, studies from recent years fail to compare the security that is demanded by these technologies with the security that is in reality applied. It is unclear if the security issues of IIoT can be properly tackled. The proposed framework covers IIoT security in detail and offers an overview of the defenses used in the industry currently using ANN-based Convolutional Neural Network CNN. The Proposed model outperforms the other renowned RNN, DT and LSTM models and gives significant improvement in results using (CIC APT IIoT) Dataset 2024 with an accuracy of 98.67%, a Recall of 86.1% achieved an F1-score. that measures a model's accuracy by balancing precision and recall with an improvement of 2.3% as compared to RNN, DT and LSTM models. In this article, the Industrial Internet of Things technologies are split into four layers by developing the architecture for defense systems that fulfill the CIA security standards. Identify the weaknesses in today's countermeasures and point out the main issues that are still unresolved challenges. The proposed framework is the solution that covers all issues within the IIoT ecosystem, Security in IIoT systems should be handled using a bottom-up approach it is necessary to reach a higher level of abstraction.

INTRODUCTION

The term "Industrial Internet of Things" refers to the interconnection of intelligent and networked industrial modules or clusters that are strategically deployed to optimize production and decrease operating expenditures through the implementation of continuous monitoring and effective management of industrial assets global economic outlook because of its many positive aspects for factories and production platforms. Besides, the manufacturing industry is clearly showing more IoT usage due to the large influx of IIoT platforms being adopted [1, 2]. The investment is expected to increase from USD 1.67 billion in 2018 to USD 12.44 billion by 2024 [3]. Research performed by ITIF in collaboration with IoT analytics indicates that adopting IoT technology in a plant can boost its performance and productivity by up to 25% [4, 5]. In addition, it is believed that because of these recent advancements, product manufacturing can reach around 1.8 trillion dollars by the year 2025 [6] and will continue to rise by over 24% from the year 2023 to 2030 [7]. They prove that the IIoT greatly improves the manufacturing industry. In the manufacturing industry, many sectors are changing through the use of technologies like big data analytics, AI, digital twins, machine learning, and combined with data to assist in industrial work [8, 9]. Even so, the threat of cyberattacks makes it difficult for companies to take full advantage of IIoT. When IIoT systems are implemented, it becomes easier for security problems to occur. Ensuring data protection at all times and in all places may be an answer to the problems related to putting these vehicles into use in industry. Figure 1 represents the Generalized AI Framework for IIoTs. IIoT is emerging as a new kind of network that has improved the methods of capturing, collecting, exchanging, and processing data. IIoT is different from the usual devices and interactions between people [10, 11].

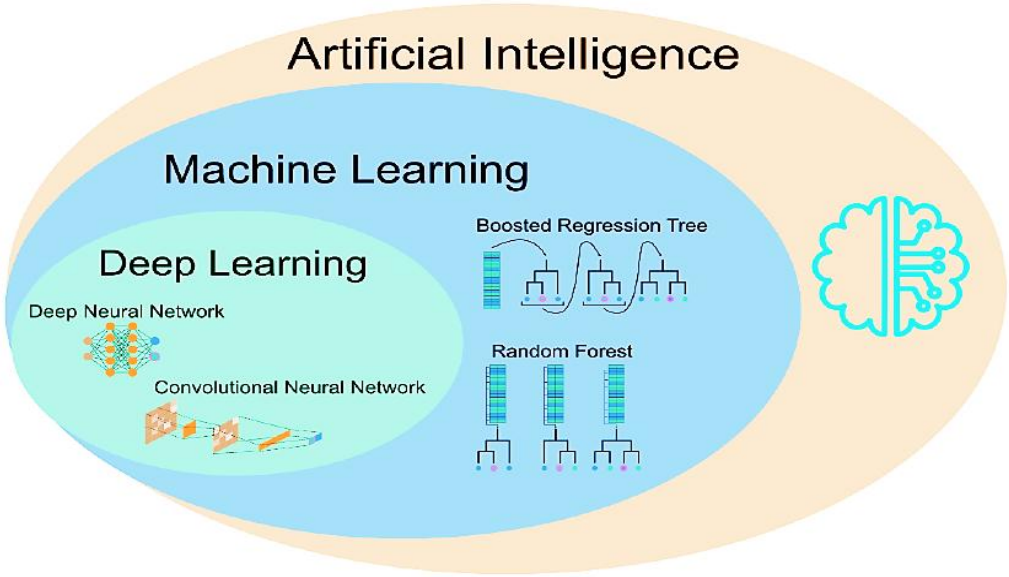

FIGURE 1: GENERALIZED AI FRAMEWORK FOR IIOTS [11]

P2P AND P2M COMMUNICATION NETWORKS

P2P and P2M communication networks are connected to Artificial Intelligence. IIoT. There are billions of devices linked through IoT technology. Systems like M2M communication are part of the networks used in the IoT. These "things". Some examples are ultra-efficient sensors and actuators, automation devices and embedded systems [12]. Machines that do most of the work, as well as gateways with real-time analysis present. Usually, these "things" can be pinpointed with different kinds of addressing. Some schemes involve using electronic product code (EPC) and ubiquitous code (UCode). The sender automatically retransmits the packet through the receiver when the retransmission timeout (RTO) reaches its defined period [13, 14].

END-TO-END LAYERS SECURITY ANALYSIS IIOT

We suggest using a four-layer architecture to protect IIoT security issues with the architecture most IIoT systems adopt at present [15, 16], because they are used in the context of industry. For instance, an IoT architecture that consists of only three layers is not ideal. The IIoT requires the ability to process and manage data. After that, recent storms are further organized into groups. IoT industry technologies and standards should be included in the planned IoT security design [17–18]. The software has been thoroughly checked for security and this analysis is discussed in the section below. Figure 2 elaborates the Layers of IIoTs for a Secure Network. The device layer security analysis concentrates on how to identify physical and

virtual things. Various schemes exist for connecting to IIoT networks. These programs are named EPC and ucode [19, 20]. They use MAC and IP addresses to build the system. Nevertheless, security should be analyzed in the context of transport and network infrastructure. Layers explores the communication and standard technologies of IIoT, especially capillary. Also, there are backhaul and backbone networks to consider. The processing layer covers the entire data processing. How to protect data in an IIoT data processing platform. Also, the application layer is for threats involving applications, communication between hosts and client-server applications protocols [21, 22-25]. As an example, one can use simple object access protocol (SOAP), also known as representational state transfer, and hypertext transfer. Table 1 shows Numerous Approaches for a Secure IIoTs Framework. REST HTTP protocol and the data circulation service used in real-time systems (DDS) [26].

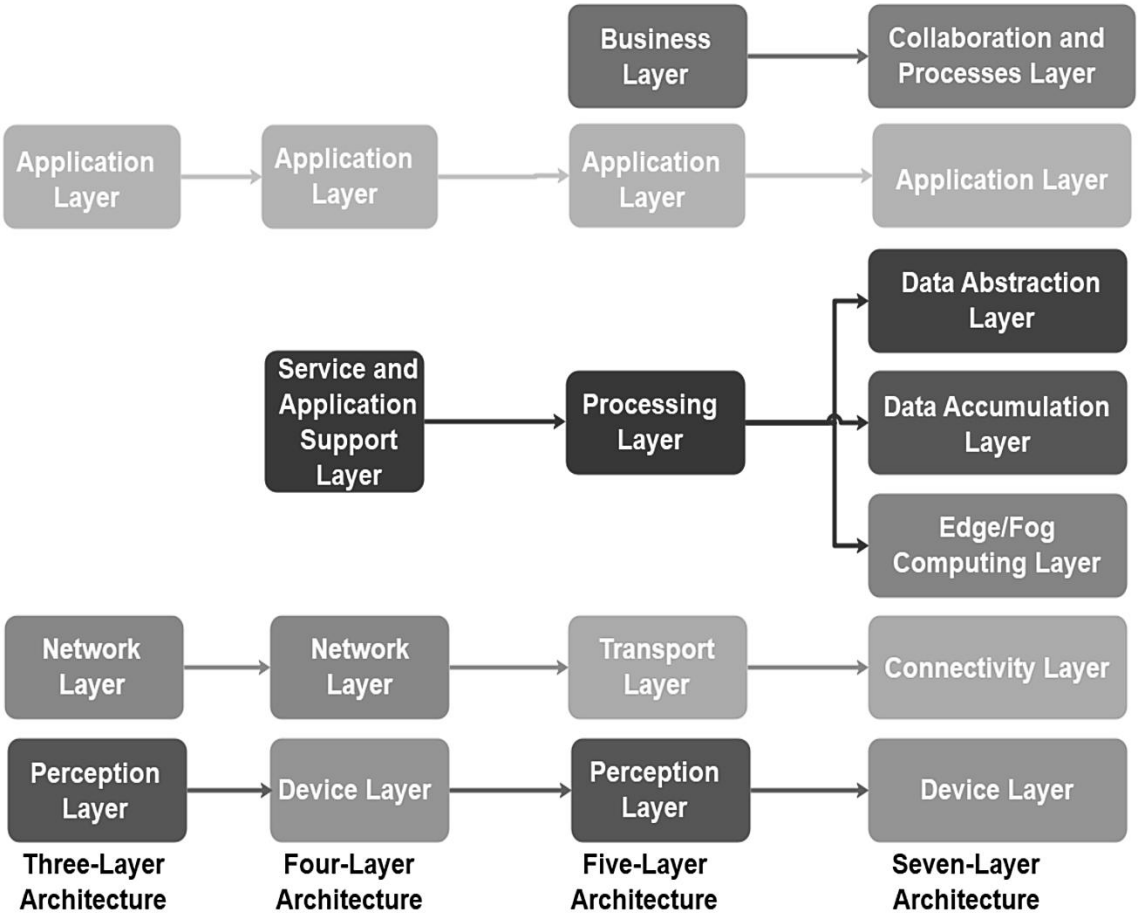

FIGURE 2: LAYERS OF IIOTS FOR SECURE NETWORK [20]

TABLE 1: NUMEROUS APPROACHES FOR SECURE IIOTS FRAMEWORK

Ref.	Security Requirements	Security Objective	Dataset	Accuracy
[27, 28]	Confidentially(C)	Malware Detection in IIoTs	(CIC APT IIoT) Dataset 2024	97.35%
[29, 30]	Integrity(I)	Medical Image Attack Security	IoT-Botnet 2020	95.93%
[31, 32]	DT	Malware attack detection	IoT_Malware dataset	97.35%
[33, 34]	Reinforcement Learning	Malicious data identification	Kitsune network attack database	98.1%
[35, 36]	Unsupervised Learning	Intrusion detection in IIoT resources.	NSL-KDD	97.35%
[37, 38]	Authorization and Access	The prevention of unauthorized use of IIoT resources.	DARPA	98.91%
[39, 40]	Authentication	Anomaly detection	KDD Cup'99	99%
[41, 42]	MLP	Botnet attack detection	Captured from various IoT devices	95.93%

IIOT ARCHITECTURE

A connection between IIoT and the physical world is where the discussion started. In the early 1990s, the Internet was used to control "things" all over the world [28]. While IIoT helpers have been created as the industry was just getting started in its evolution. For instance, IETF and IEEE both RFID and sensors set boundaries on the concepts of definitions [43, 44]. The W3C discusses how the IoT relates to online interactions through the World Wide Web [45]. IoT's objective is to permit anything to be connected at any time. In most situations we studied in the industry, we noticed these "things" have three main characteristics: they are not the same and they are always unique. Unique traits and the relationship among them. Concurrently, as the IIoT develops for various industries, there should be significant attention to its security and privacy. The difficulties associated with global issues are growing [46, 47]

OVERVIEW OF IOT AND IIOT FRAMEWORKS

The new IIoT characteristics include large amounts of heterogeneity. In addition, these systems deal with matters of "things" and cyber-physical systems between the safety of regular systems and that of Industrial IoT. Since there are so many types of "things" in a large system, interoperability is needed. The difficulty of sharing data between networks, cyber-physical systems and technologies powered by the IIoT integration [48, 49]. Interoperability problems exist whenever Devices and sensor nodes in the network are called and addressed using different terms. One should try (i) to develop various schemes, (ii) use various data types and formats and (iii) interact. With various security settings set by the network (such as reliability). Various factors such as communication cost, latency and bandwidth are combined to support different service applications. The issue of whether these standard ways of ensuring safety are that it would be beneficial to design defence approaches for IoT that are consistent and potentially universal. No plan has been successfully created to address the issue of security difficulty. The internet operates between client smartphones and medical workers through smartphones acting as communication proxies. The system integrates HTTP and CoAP conversion on the doctor's smartphone, which enhances compatibility with server(doctor's smartphone) functions [50, 51-55]. Figure 3 shows the Generalized threat identification in IIOTs based Network Framework [12]. The observed functionality within CoAP technology decreases the need for continuous server-client data transmissions. The server operates in combination with the client to obtain medical sensor information. The system functions by getting periodic system responses rather than continuous ones. This design benefits from CoAP as an IoT protocol that requires minimal computational resources [56, 57].

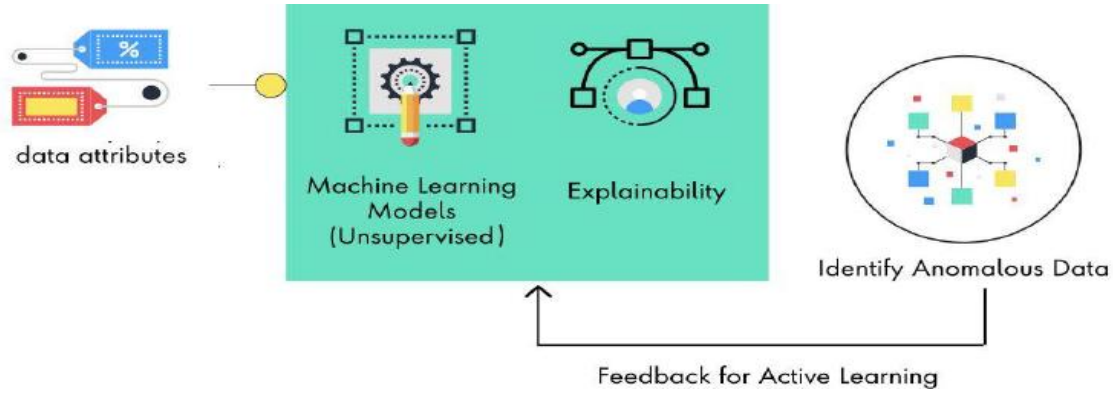

FIGURE 3: THREAT (ANOMALY) MITIGATION IN IIOTS BASED ON NETWORK FRAMEWORK [58]

IIoT infrastructure is more sensitive because of its size, greater complexity, strong robustness and necessary ecosystem compared to the regular IoT. The risks related to cyberattacks on IIoT vary a lot from those in IoT in terms of threat surface, ability to scale, connectivity, interoperability and integration of OT. Most IoT networks use the same regular IT gear, including workstations, servers, routers and switches and these gadgets are known to be vulnerable to attacks. On the other hand, the IIoT opens up more opportunities for cyber-attacks by attaching many control systems, cobots, sensors, actuators and other field devices across industries that use different protocols for communication [59, 60]. Figure 4 represents the Non-Confirmable messages based Framework for Transmission and Receiver in IIoTs

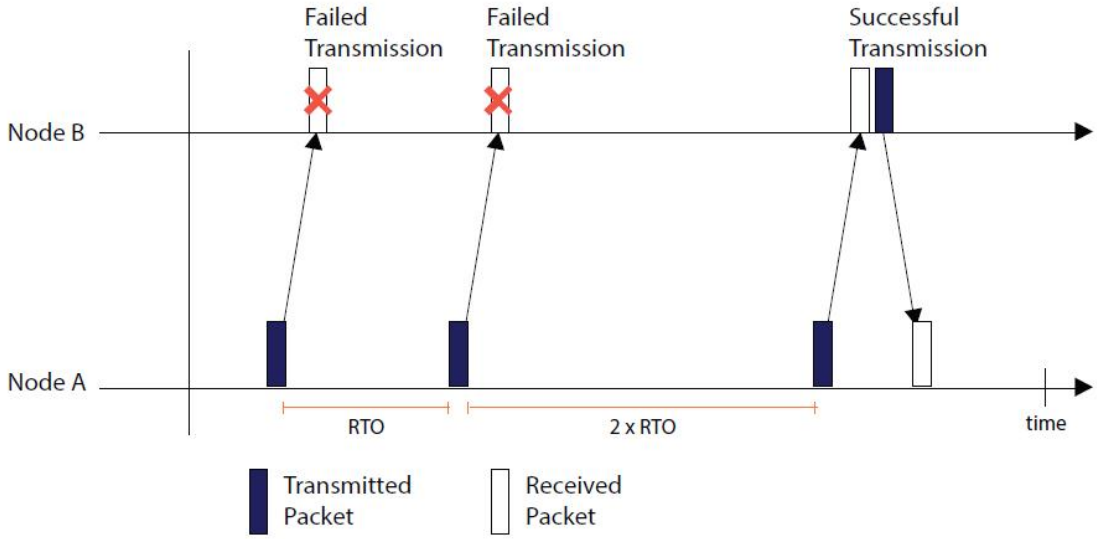

FIGURE 4: NON-CONFIRMABLE MESSAGES BASED FRAMEWORK FOR TRANSMISSION AND RECEIVER IN IIOTS [61]

For this reason, the types of dangers and risks that come with IoT tools, systems and services are numerous and keep changing over time. A wide range of threats to safety, security and privacy exist in the IIoT. Hence, it is necessary to identify all items in the IoT environment that should be protected and design accurate rules to keep these items secure from cyberattacks. The Pending Event Descriptor (PED) containing OSGP packet information resides within the options field of the mapping process [61, 62]. The CoAP packet contains a software field that receives its information through a count value from the OSGP packet and the data field uses values from the OSGP packet's offset [63, 64]. IIoT infrastructure is more sensitive because of its size, greater complexity, strong robustness and necessary ecosystem compared to the regular IoT. The risks related to cyberattacks on IIoT vary a lot from those in IoT in terms of

threat surface, ability to scale, connectivity, interoperability and integration of IOT [65, 66]. Most IoT networks use the same regular IT gear, including workstations, servers, routers and switches and these gadgets are known to be vulnerable to attacks. On the other hand, the IIoT opens up more opportunities for cyber-attacks by attaching many control systems, cobots, sensors, actuators and other field devices across industries that use different protocols for communication [67, 68].

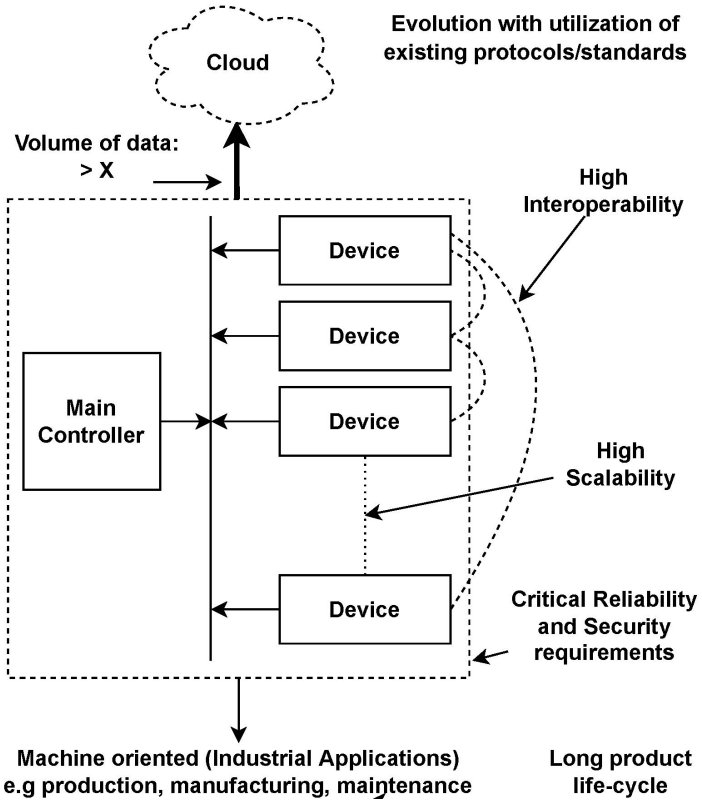

FIGURE 5: STRUCTURE OF IIOTS BASED ON ARTIFICIAL NEURAL NETWORK CONTROLLER [69]

For this reason, the types of dangers and risks that come with IoT tools, systems and services are numerous and keep changing over time. Figure 5 represents the Structure of IIoTs based on an Artificial Neural Network Controller. A wide range of threats to safety, security and privacy exist in the IIoT. Hence, it is necessary to identify all items in the IoT environment that should be protected and design accurate rules to keep these items secure from cyber attacks [70, 71].

PROPOSED FRAMEWORK BASED ON IIOTS USING MACHINE LEARNING

The IIoT requires managing, processing and saving data. Then, we classify events from recent history. The IoT security architecture ought to include industry IoT technologies and standards. An entire security analysis was carried out and the conclusions are presented in Section 5. The main purpose of the analysis on the device level is to identify the different physical and virtual "things" services available to get access to IIoT networks. Some of the schemes include EPC, plus the uCode. The layer describes IIoT communication technologies and standards, such as capillary. These people also build backhaul and backbone networks. Here, data is processed through the whole journey from start to finish. Issues related to the security of IIoT data processing. Also, the application layer is responsible for the challenges related to threats in applications, connections between different computers and using client-server protocols. The research paper addresses the key management issues found in the current ML-based IDS. The system provides secure IoT device-server communication within resource-limited IoT networks with reduced communication overhead. The proposed method consists of five sequential stages, including (i) Session initiation, followed by (ii) Server challenge phase, then (iii) Client response and challenge phase, after which (iv) Client authentication and server response phase occurs before (v) Key negotiation and server authentication phase. The protocol starts with a session initiation phase that is followed by server challenge, then client response and challenge, before client authentication and server response, followed by key negotiation and server authentication. The five protocol phases consist of session initiation, followed by server challenge phase and client response and challenge phase, followed by client authentication and server response phase, before key negotiation and server authentication. The detailed implementation sequence of ECC-CoAP shows how the server and client devices exchange messages. The sequence of operations between the user/IoT device and the server can be observed in the following figures. Users authenticate to remote servers using their valid inputs under the presumption that the servers can be trusted. Security experts have observed occasional instances where an insider from the remote server detects malicious activities. Once an opponent acquires essential user credentials stored in the server platform, they assume the role of an adversary. Proposed ECC-CoAP implements crucial HU and DIDU storage on the server. Figure 6 shows the proposed Artificial Neural Network (CNN) based Framework for Secure Network. The IoT device requires additional authentication credentials, which the server stores during the process.

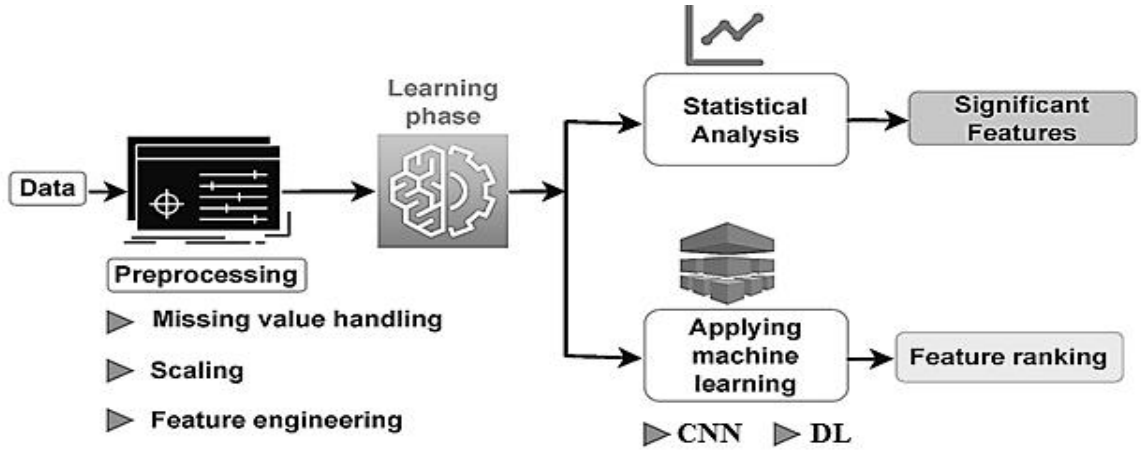

FIGURE 6: PROPOSED ARTIFICIAL NEURAL NETWORK (ANN) BASED FRAMEWORK FOR SECURE NETWORK USING CNN

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

The process involves analyzing the structure of a binary file and breaking down its functions in a process called static detection. During the creation and testing phases of a software application, static detection does its primary work. Currently, the means of detecting statics are explained in Fig. 7. Cybersecurity today is challenged by serious APT attacks. They move in a very unnoticeable way. Experts have looked into various ways to solve these issues. In their work, researchers have used three methods: machine learning (ML), deep learning (DL) and Explainable AI (XAI).

Next, I will look at the major contributions of these technologies. Combining Decision Trees and Bayesian Networks with other Machine learning and deep learning algorithms detects known security issues well.. The security gaps mentioned are solved by DL's autoencoders and reinforcement learning processes. Such systems look into various developing types of attacks. The autoencoder in IIoTs performs remarkably when extracting useful features and lowering the number of dimensions. Using DRL, systems can adapt to new changes in malware. Using these tools helps detect which APT group is connecting to specific malware. By using XAI, it is easier to see how machine learning and deep learning models work. By using this methodology, the black box challenge is given importance. LIME and SHAP are techniques that can display the importance of each feature. With XAI, analysts are more confident in the decisions AI makes. In times when demand is high, the insights from

every system must be easy to interpret for better decision-making. Employing XAI usually increases the complexity of systems and their associated operating costs. Figure 8 represents the Proposed Machine Learning based CNN Architecture for IIOTs. No gaps in cyber protections are required to improve security. Because of these systems, it is now easier to address the evolution of APT. One of the key strengths of ML is that it can identify threats as they happen. Even so, there are still some limits.

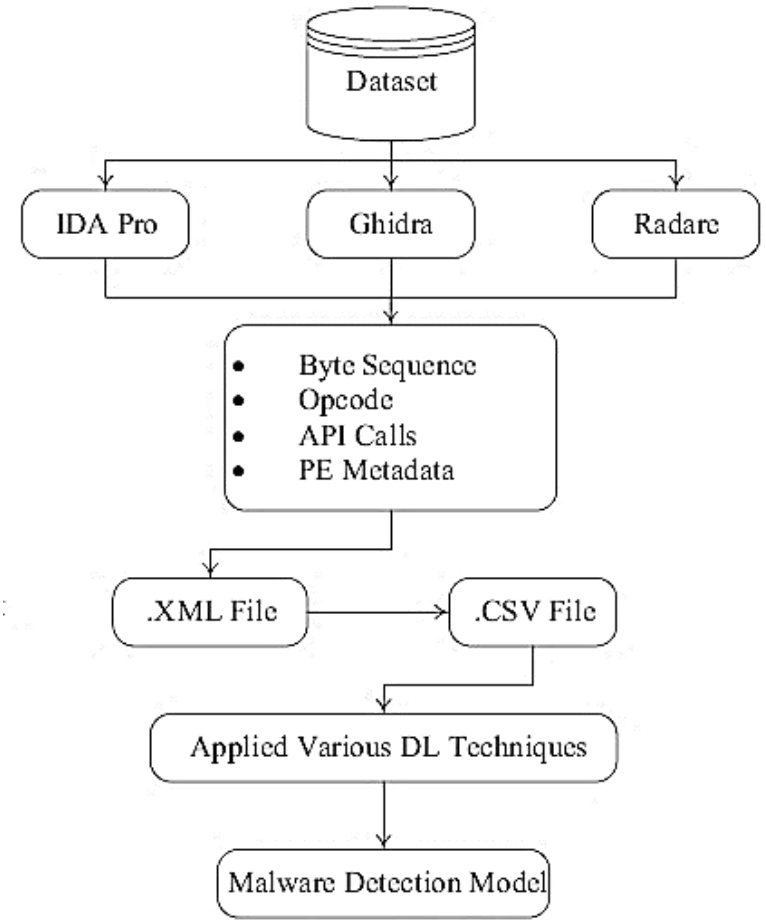

FIGURE 7: FLOW CHART FOR MACHINE LEARNING BASED STATIC INTRUSION DETECTION FOR IIOTS

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)}) \quad \text{Eq (2)}$$

$$J^{(b,t)} = \beta^{(b)} \times (W^{(b)} \times J^{(b-1,t)} + W^{(b)} \times J^{(b,t-1)}) \quad \text{Eq (3)}$$

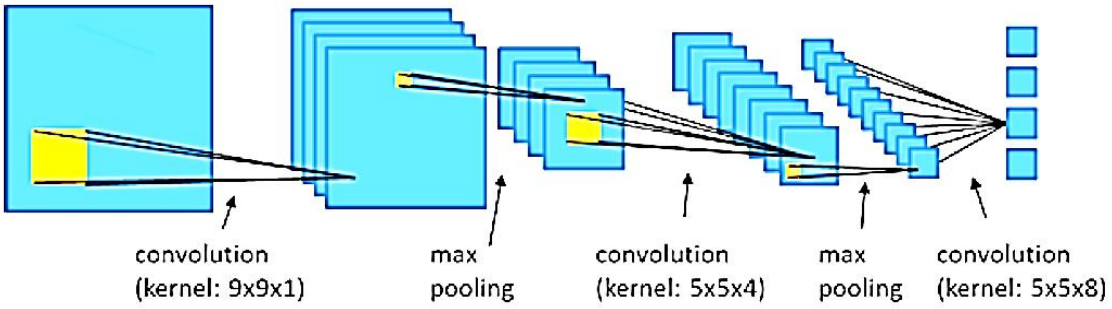

FIGURE 8: PROPOSED MACHINE LEARNING BASED CNN ARCHITECTURE FOR IIOTS

$$\ln fl_{it}^{+} = \Sigma_{j=0}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it} \qquad \textbf{Eq (4)}$$

$$\ln fl_{it}^{+} = \Sigma_{j=1}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=1}^{t} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it} \qquad \textbf{Eq (5)}$$

SIMULATION TESTING

This section elaborates on the simulation results in Table 2 represents the Analysis of Packet Loss Using P-ANN, while Table 3 shows Comparative Analysis of IIoTs Tire parameters Using Multiple Nodes.

TABLE 2: ANALYSIS OF PACKET LOSS USING P-ANN USING (CIC APT IIOT) DATASET

Dataset	ML Techniques	Packet Loss Tire 1	Packet Loss Tire 2	Packet Loss Tire 3	Packet Loss Tire 3	Packet Loss Tire 4	Packet Loss Tire 5	Packet Loss Tire 6	Packet Loss Tire 7	Packet Loss Tire 8
CIC APT IIoT Dataset	IrDA	156,13	196,23	181,33	196,23	181,33	300,12	156,13	220,3	202,21
	RFID	196,23	196,23	211,01	156,13	211,01	200,25	196,23	216.71	214.11
	NFC	196,23	181,33	300,12	196,23	211,01	200,25	196,23	519.89	217.92
	INSTEON	196,23	211,01	200,25	196,23	211,01	200,25	156,13	196,23	60.21
	Smart BLC	196,23	211,01	200,25	196,23	196,23	181,33	196,23	196,23	213.68
	IIoT EQP 1	211,01	211,01	200,25	196,23	196,23	211,01	196,23	181,33	202,21
	IIoT EQP 1	156,13	196,23	181,33	181,33	181,33	300,12	196,23	211,01	214.11
	IIoT EQP 1	211,01	217.92	181,33	196,23	211,01	200,25	196,23	211,01	217.92

2024	IIoT EQP 1	111.34	60.21	211,01	156,13	211,01	200,25	196,23	911.34	60.21
	IIoT EQP 1	217.11	213.68	300,12	196,23	211,01	200,25	196,23	217.11	213.68
	IIoT EQP 1	196,23	181,33	196,23	156,13	196,23	181,33	181,33	300,12	317.97
	IIoT EQP 1	181,33	300,12	156,13	196,23	181,33	300,12	156,13	220,3	202,21

TABLE 3: COMPARATIVE ANALYSIS OF IIOTS TIRE PARAMETERS USING (CIC APT IIOT) DATASET 2024

Dataset	IIoTs Server	Packet Loss	Specificity	Accuracy	F-1 Score	R^2 Score	Data Rate
(CIC APT IIoT) Dataset 2024	IIoTs Tire 1	3.198	2.581	3.581	0.3411	3.916	0.64 bps
	IIoTs Tire 2	2.118	3.1	3.198	0.5431	1.5	0.61 bps
	IIoTs Tire 3	3.4	2.581	1.41	0.6321	1.1	0.72 bps
	IIoTs Tire 4	3.198	3.5	3.198	0.7531	1.51	0.83 bps
	IIoTs Tire 5	1.41	5.1	2.1	0.8451	3.1	0.97 bps
	IIoTs Tire 6	1.51	1.21	3.1	0.6751	2.51	0.86 bps
	IIoTs Tire 7	2.41	5.1	3.581	0.3411	3.916	0.64 bps
	IIoTs Tire 8	6.55	4.21	4.3	0.5431	5.5	0.61 bps
	IIoTs Tire 9	7.11	5.1	3.581	0.6321	5.1	0.72 bps
	IIoTs Tire 10	3.8	3.198	2.581	0.7531	1.51	0.83 bps
	IIoTs Tire 11	4.1	2.118	3.1	0.8451	3.1	0.97 bps
	IIoTs Tire 12	4.128	3.4	2.581	0.6751	1.51	0.86 bps
	IIoTs Tire 13	5.7	5.1	3.1	0.3411	7.11	0.64 bps
	IIoTs Tire 14	6.55	4.21	4.3	0.5431	3.8	0.61 bps
	IIoTs Tire 15	7.11	5.1	3.581	0.6321	4.1	0.72 bps

CONCLUSION AND RECOMMENDATIONS

This research has presented the design and development mechanism and framework for IIoTs using ANN. The adoption of the IIoT has improved how industry, businesses and organizations work. Higher efficiency, greater productivity and cost reduction. At the same

time, there are privacy concerns that arise from the IIoT. Safeguards are necessary for the protection of every computer connected to a network and the people who use them and for privacy. This paper aims to highlight the privacy requirements present in the IIoT ecosystem. Defending personal data and the privacy aspects set up by officials in the industry. The paper has also given details about present-day ways and techniques to deal with some privacy risks in the IIoT, involving using encryption, anonymization, access controls, authorization and monitoring and surveillance technology. Furthermore, the paper points out why personal data must be protected in criminal cases. Organizing investigations or applying criminal penalties, mostly in fields sensitive to regulatory oversight. In short, the paper offers ideas about the privacy needs and dangers involving IIoT. The Proposed model outperforms the other renowneded RNN, DT and LSTM models and gives significant improvement in results using (CIC APT IIoT) Dataset 2024 with an accuracy of 98.67%, a Recall 86.1% achieved F1-score. that measures a model's accuracy by balancing precision and recall with a improvement of 2.3% as compared to RNN, DT and LSTM model. In this article, the Industrial Internet of Things technologies are split into four layers by developing the architecture for defense systems that fulfill the CIA security standards. Identify the weaknesses in today's countermeasures and point out the main issues that are still unresolved challenges. These points and policy recommendations are crucial for those who make laws and rules. Organizations need to learn to secure both their technology and the privacy of their end users. If companies act on privacy threats in advance, they can continue to protect themselves. They should earn their stakeholders' trust, watch their reputation and take advantage of their efficiency. Improved outcomes in productivity from using the IIoT. The key focus of this study in the future is to look at blockchain and privacy. It will reveal both the advantages and the drawbacks involved. Additionally, this would draw attention to in recent times, blockchain has become important for ensuring security and privacy online.

REFERENCES

[1] Abdullahi, S. M., & Lazarova-Molnar, S. (2025). On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advance . International Journal of Information Security, 24(1), 53.

[2] Al-Turjman, F., & Alturjman, S. (2018). Context-sensitive access in industrial internet of things (IIoT) healthcare applications. IEEE Transactions on Industrial Informatics, 14(6), 2736-2744.

[3] Cecílio, J., & Souto, A. (2024, May). Security issues in industrial Internet-of-Things: Threats, attacks and solutions. In 2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0 & IoT) (pp. 458-463). IEEE.

[4] Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Computer Networks, 153, 36–48. Khoramshahi, M., & Billard, A. (2019). A dynamical system approach to task adaptation in physical human-Network interaction. Autonomous Networks, 43(4), 927–946.

[5] 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

[6] 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

[7] 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

[8] 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.

[9] 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.

[10] 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

[11] 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

[12] 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

[13] 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.

[14] 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.

[15] 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

[16] 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.

[17] 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.

[18] 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

[19] 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

[20] 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

[21] 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.

[22] 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

[23] 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

[24] 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

[25] 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

[26] 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

[27] 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

[28] 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

[29] 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.

[30] 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

[31] 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.

[32] 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

[33] 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

[34] 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

[35] 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

[36] 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

[37] 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.

[38] 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.

[39] 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).

[40] 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.

[41] 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.

[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] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[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., 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.

[61] 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).

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] Katsikeas, S. Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol. In Proceedings of the

[69] 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 1193–1200.

[70] Bartman, T.; Carson, K. Securing communications for SCADA and critical industrial systems. In Proceedings of the 69th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 4–7 April 2016; pp. 1–10.

[71] Ma, M.; He, D.; Kumar, N.; Choo, K.K.R.; Chen, J. Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. IEEE Trans. Ind. Inform. 2017, 14, 759–767. [CrossRef]