Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

An Enhanced 6G-Enabled IoT Network Security Framework Using Edge AI and Machine Learning

Israr Ahmad (Corresponding Author)
Department of Computer Science and IT, Superior University Lahore, Pakistan
Email: israr.gdec@gmail.com
Nasir Ayub
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: nasir.ayyub@hotmail.com
Chaudary Umair Mehmood
Edge Hill University, Ormskirk L39 4QP, United Kingdom
Email: umairmehmood.pk@gmail.com
Hamayun Khan
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk
Muhammad Abdullah
CEO IMAB Printing and Tech Solutions, 54000, Pakistan
Email: mabdullahkhaliq14@gmail.com
Muhammad Waleed Khawar
Innova Network, 184 C, Airline Society, Lahore, 54000, Pakistan
Email: waleedkhawar19@gmail.com
Hassan Ali Mehdi
Codantrix Labs, Lahore,54000, Pakistan
Email: hassanalimehdi@codantrix.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, 54000, Pakistan Email: rizwan.naqvi@ieee.org

ABSTRACT

The 6G wireless network can combine with the Internet of Things (IoT) to enable terahertz (THz) communication, reconfigurable intelligent surfaces (RIS), network slicing, and AI-native radio access networks (RANs), which would connect trillions of heterogeneous resource-constrained devices. Such enormous size, coupled with the demands of ultra-low latency and mass connectivity, significantly increases the attack surface that IoT ecosystems face today, and makes it difficult to meet the latency, bandwidth, and privacy demands of 6G. This study provides a comprehensive discussion of the current state of security research in Edge Artificial Intelligence and Machine Learning approaches to securing 6G-enabled IoT networks, and is explicitly contextualized with respect to previous surveys of 6G-IoT security, while uniquely

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

focusing on introducing the reader to the field of Edge AI and ML 6G-IoT security. We review recent works dealing with federated learning-based intrusion detection, deep and hybrid learning architectures, deep reinforcement learning for adaptive defense, TinyML for extreme-edge inference, explainable AI for auditability, and blockchain-assisted zero trust access control. On top of the identified gaps, we present an Enhanced 6G-IoT Security Framework, consisting of a closed-loop, federated detection-and-response workflow that incorporates a five-layer architecture, namely the perception, edge-AI, 6G network, cloud-intelligence, and application layers. Comparative tables represent techniques, threat taxonomies, and design trade-offs, as well as architecture. The study ends by highlighting many open challenges, such as the lack of 6G-IoT representative datasets, adversarial robustness, energy-latency-accuracy tradeoffs at the extreme edge, as well as the need for quantum-safe secure information, models with explainability, and sustainable secure information. The study provides a basic research roadmap for developing more trustworthy 6G-IoT systems in the future.

Keywords—6G Networks; Internet of Things; Edge AI; Machine Learning; Federated Learning; Network Security; Intrusion Detection; Zero-Trust Architecture

I. Introduction

Conventional fifth-generation (5G) networks are already facing structural constraints under the pressure of emerging applications in the Internet of Everything (IoE) including autonomous driving, immersive extended reality (XR) and large-scale digital twins [1]. The design of 6th-generation (6G) networks has been pushed to overcome these limits by adopting the use of the terahertz (THz) spectrum, reconfigurable intelligent surfaces (RIS), AI-native radio access networks, space-air-ground integration and network slicing which enables to provide sub-millisecond latency and order of magnitude more connection density than 5G [2]. At the same time, the Internet of Things (IoT) is expected to include tens of billions of devices that vary widely in type, power and size, ranging from smart health applications to Industry 5.0, intelligent transportation systems, and smart cities [3].

The convergence of these two, hence 6G-IoT in the world of 6G magnifies both the opportunity and the risk. On the one hand, AI-native connectivity allows to provide real-time, context-aware services while on the other hand, the size, diversity and mobility of connected devices drastically increases the attack surface which can be exploited to compromise the device, the network or even target increasingly sophisticated attack that exploits the machine learning models embedded in the device itself and the network itself, such as the adversarial perturbations, data poisoning or the model-inversion attack [4,5]. In a traditional cloud-based security system, where data is sent to centralized security servers for processing, there are limitations on

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

latency and privacy for 6G and there is a single point of failure that is ill-equipped for the vast number of huge IoT deployments [6-8].

$$s(t) = (x * w)(t) = \sum_{a=-\infty}^{\infty} x(a)w(t - a) \quad \text{Eq (1)}$$

W stands for the kernel filter, x stands for the input signal, t stands for time and s is the output signal. The convolution process with two-dimensional input data is described by Equation (2).

$$S(i,j) = (I * K)(i,j) = \sum_m a \sum_n I(i,j) * K(i-m, j-n) \quad \text{Eq (2)}$$

The variables iii and jjj are the spatial position in the output matrix following the convolution operation. In this process, the center of the filter is matched with the corresponding image area, so as to achieve the best feature extraction effect. Moreover, the proposed framework uses the cross-entropy loss as the optimization objective, which is shown in Equation (3).

$$S(i,j) = (I * K)(i,j) = \sum_m a \sum_n I(i + m, j + n) * K(m,n) \quad \text{Eq (3)}$$

To overcome these requirements, Edge Artificial Intelligence (Edge AI) has become an attractive paradigm that places the data closer to the system where it is used and, to a greater extent, where it is learned [9-11]. To retain privacy and mitigate the communication overhead, federated learning enables distributed IoT and edge nodes to jointly train a federated model with minimal sharing of raw data with a central server [12-14]. For inference on devices with a small memory footprint, such as microcontrollers, complementary techniques like TinyML [15] can be used, and deep reinforcement learning is suitable for self-optimizing defense policies for dynamic 6G scenarios [16, 17]. Explainable AI and blockchain-based zero-trust mechanisms also provide solutions to the issues of trust, auditability and identity management in fully autonomous AI-powered security pipelines [18-21].

ReLu

$$f(x) = \begin{cases} 0, x < 0 \\ x, x \geq 0 \end{cases}, f(x)' = \begin{cases} 0, x < 0 \\ x, x \geq 0 \end{cases} \quad \text{Eq (4)}$$

Although a collection of isolated and distinct works have emerged, there is still no single framework in the literature that systematically charts the 6G-IoT threat landscape along key aspects of the deployment of Edge AI and ML technologies, namely device, network, and AI-model layers; The prevailing Edge AI and ML paradigms for relevant aspects of limited IoT resource availability such as latency, communication overhead, privacy, robustness, and energy; and proposes an integrated, closed-loop architecture that operationalizes these approaches within the 6G-IoT security pipeline [22-25]. This paper fills that deficiency. The major contributions are the following:

Online ISSN 3007-3197
Print ISSN 3007-3189

we present a structured overview of 6G-enabling technologies and discuss the implications it has for 6G-IoT security, and propose a layer-wise taxonomy of 6G-IoT security threats, covering the perception layer, network layer and AI-model layer [26]. Recent study of highly cited journal papers (2020-2026) related to federated learning, deep and hybrid learning, deep reinforcement learning, TinyML, explainable AI and blockchain-based Zero Trust IoT and 6G security mechanisms [27].

We proposed an Enhanced 6G-IoT Security Framework to combine these techniques into a 5-layer architecture and a closed loop detection-response workflow mechanism based on 6GIoT use-case scenarios and provide the original architecture and workflow diagrams. Comparative tables summarizing threats, typical techniques and design trade-offs are provided and open research challenges and future directions for trustworthy 6G-IoT security are outlined.

A. Review Methodology

The wide range of the topic searched a more selective process is carried out for the review; a strictly systematic search process is not performed. The literature was collected using an IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink searches based on a set of combinations for the keywords 6G, Internet of Things, edge AI, federated learning, TinyML, deep reinforcement learning, explainable AI, zero trust, and intrusion detection. Only peer-reviewed journal articles and preprinted conference papers from between 2019-2026 were eligible for coverage, and emphasis was given to the presenters from 2023-2026, typically assumed to be “6G”-related, and making it closer to the conference schedule four years later. Preprints and non-English papers were ignored; papers published in both the conference and the journal were ignored if the conference was superseded by the journal a year later. Following this, the remaining part of this review is organized around the six families of techniques for Edge AI and ML introduced in Section IV, and the threat taxonomy developed in Section III.The resulting 41 primary sources were summarized in the Reference list and kept organized around these 6 families of techniques for Edge AI and ML and the taxonomy of threats developed in Section III.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

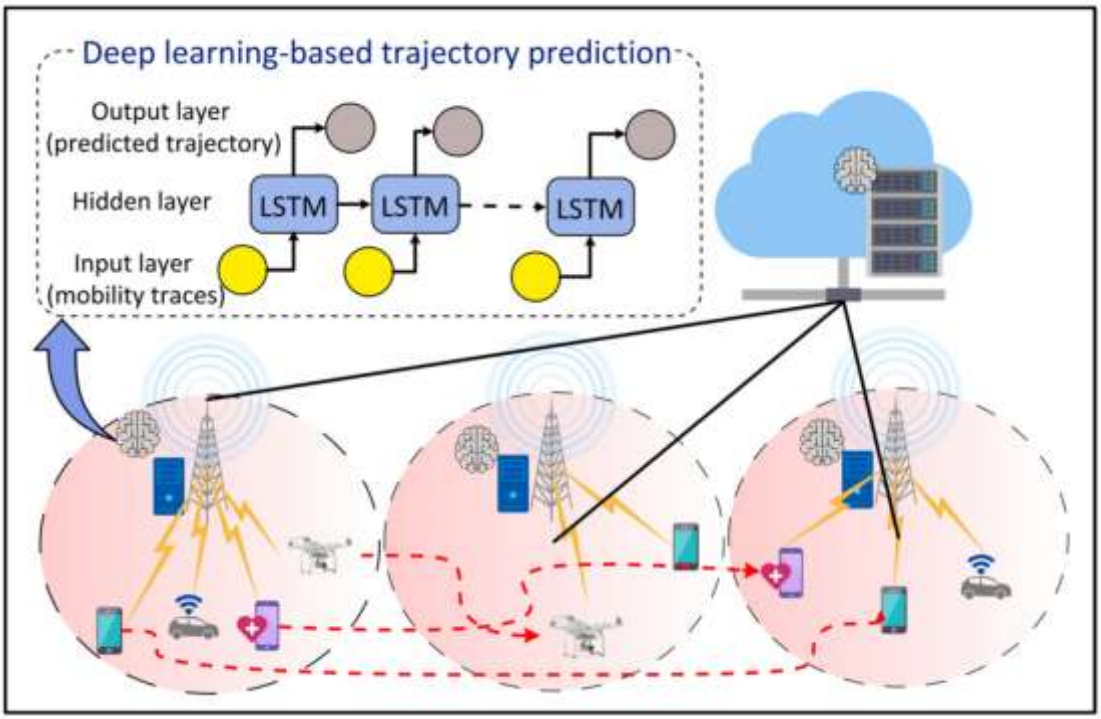


Fig. 1 (a). Generic Intelligent network architecture based on DL [28]

B. Positioning Relative to Existing Surveys

While several surveys in existence cover portions of the 6G-IoT security space, they fall short of integrating a threat taxonomy and taxonomy of multiple paradigms of Edge AI and ML with a concrete and integrated defense architecture. To put this review in perspective of five representative prior reviews, see Table I.

TABLE I POSITIONING OF THIS REVIEW RELATIVE TO REPRESENTATIVE EXISTING SURVEYS

Primary Scope	6G-Specific Focus	Threat-Taxonomy Scope	Integrated Framework Proposed
Edge-learning vulnerabilities, datasets, and defenses for 6G-enabled IoT [29-31]	Yes	Device/network/model, vulnerability-centric	No
XAI techniques for 5G/6G security and slicing decisions [32]	Partial (5G/6G)	XAI-centric, not a full threat taxonomy	No
Systematic review of federated-learning-based	No (general	Algorithm-centric, not	No

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

intrusion detection [33,34]	IoT)	layer-wise	
ML-based IoT security solutions and open challenges [35-38]	No (pre-6G)	Broad ML-security survey, not 6G-specific	No
TinyML techniques for extreme-edge intelligence [39-42]	No	Not security-threat-taxonomy focused	No
FL, deep/hybrid learning, DRL, TinyML, XAI, and blockchain zero-trust for 6G-IoT security [43-45]	Yes	Device, network, AI-model, and cross-layer trust	Yes — five-layer architecture with closed-loop workflow

Previously carried out surveys often focus on one of the three main families of techniques: XAI [46, 47], federated learning or TinyML browsers; or they are more limited to only the challenge of vulnerabilities and data, but ignore the nature of 6G-IoT threats and a thorough comparative study of potential defense paradigms [48-50].

Sigmoid

$$f(x) = \frac{1}{1+e^{-2}}, f'(x) = f(x)(1 - f(x)) \quad \text{Eq (5)}$$

Tanh:

$$\tan h\,(x) = \frac{2}{1+e^{-2x}} - 1, f'(x) = 1f(x)^2 \quad \text{Eq (6)}$$

As shown in Table I, most of the surveys covered in the literature have limited scope to a particular technique family, or adopted an approach that predates the advent of 6G threats completely. This review is unique in bringing together a taxonomy of threats that cross the device, network and AI and ML, as well as a synthesis of six Edge AI and ML paradigms, along with an original threat framework that spans five layers and features a closed loop cyclic [51-55].

Clipped ReLU:

$$f(x) = \begin{cases} 0, x < 0 \\ x0 \leq x < \text{ceiling} \\ ceiling, \geq \text{ceiling} \end{cases} \quad \text{Eq (7)}$$

Leaky ReLU:

$$f(x) = \begin{cases} 0, x < 0 \\ scale * x, x < 0 \end{cases} \quad \text{Eq (8)}$$

The rest of this paper is structured in the following way. In Section II, the 6G-IoT convergence and enabling technologies are described. In Section III, we discuss a taxonomy of the 6G-IoT security threat landscape. In Section IV, edge artificial

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

intelligence and machine learning (ML) solutions are discussed for 6G-IoT security. The proposed improved framework is presented in Section V. A comparative analysis and discussion among the selected contentious policies are provided in Section VI. Open challenges and future research are described in section VII while section VIII concludes the paper.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)} \qquad \text{Eq (9)}$$

II. 6G-IoT Convergence: Architecture and Enabling Technologies

The envisioned 6G networks support THz-band communication, massive and holographic MIMO, RIS-assisted propagation control and pervasive AI embedded in RAN and core network functions to achieve the peak data rate of > 100Gbps and the air-interface latency of < 0.1ms, the ultra-high connection density of up to 107devices/km² [56-59].

$$S_h = 60° \begin{cases} 0 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, if m_x = \beta_r \\ 2 + \frac{(\beta_b - \beta_r)}{(m_x - m_n)}, if m_x = \beta_g \\ 4 + \frac{(\beta_r - \beta_g)}{(m_x - m_n)}, if m_x = \beta_b \end{cases} \qquad \text{Eq (10)}$$

Software-defined networking and network function virtualization (SDN/NFV) enables operators to create separate virtual networks designed to suit diverse IoT applications, including ultra-reliable and low-latency networks for industrial control to massive machine-type communication (MMC) for environmental sensing [60-62].

$$o_t = \sigma(W_o x_t + W_o h_{t-1} + b_o) \qquad \text{Eq (11)}$$

The IoT ecosystem point of view, these are three structural changes. The perception layer of the system gets much more diverse and includes from ultra-low-power sensors to autonomous vehicles to unmanned aerial vehicles with different compute, power, and mobility requirements. Secondly, the wider network layer itself becomes programmable and is AI-native, with slicing, RIS, and SDN/NFV adding to the attack surface if not secured in addition to being enablers for service differentiation [63-64].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$y = f\left(\sum_{k=1}^{K} h^k * w^k + c^k\right)$$ Eq (13)

Third, intelligence gets distributed, in the sense that the intelligence of 6G-IoT is more and more cascaded over the different hierarchies of device, edge and fog, and cloud levels, so that systems increasingly move closer and closer to the Edge AI paradigm introduced in Section IV.

TABLE II KEY 6G-ENABLING TECHNOLOGIES AND THEIR IMPLICATIONS FOR IoT SECURITY

Enabling Technology	Role in 6G-IoT	Security Implication
THz Communication & Massive MIMO	Ultra-high-bandwidth, low-latency links for dense IoT deployments	New physical-layer eavesdropping and jamming surfaces; short-range links reduce but do not eliminate interception risk [65-67]
Reconfigurable Intelligent Surfaces (RIS)	Programmable radio environment for coverage and energy efficiency	RIS misconfiguration or spoofing can be exploited to redirect or intercept signals [68-69]
Network Slicing / SDN-NFV	Isolated virtual networks per IoT application class	Slice isolation failures and controller compromise can cascade across tenants [70], [71]
AI-Native RAN / Edge Intelligence	In-network learning and adaptive resource orchestration	Introduces AI-specific attack vectors: poisoning, evasion, and model extraction [72-75]
Space-Air-Ground Integrated Networks	Extends connectivity to remote/mobile IoT (UAV, satellite)	Heterogeneous trust domains complicate authentication and key management [76-79]
Digital Twin Integration	Real-time virtual replica for monitoring and simulation	Synchronization channel and twin-data integrity become new targets [80]

III. Security Threat Landscape in 6G-Enabled IoT

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Securing 6G-IoT systems necessitates a holistic approach to understanding and mitigating threats across multiple layers, including those from the physical aspect, the network as it essentially becomes an AI-based fabric, and the machine learning models that are increasingly shaping network decisions. We categorize the threat landscape into three layers similar to previous surveys of vulnerabilities occurring in 6G-IoT [81-83].

$$\mathrm{TDI} = \sqrt{(\Delta C)^2 + (\Delta \sigma)^2} \qquad \text{Eq (14)}$$

A. Device / Perception-Layer Threats

Resource-constrained IoT endpoints can be physically captured and firmware can be tampered, lightweight primitive cryptography attacks can be launched, and physically unclonable function identities can be stolen. However, the botnet recruitment of poorly secured consumer and industrial devices is still a prevalent attack surface for large-scale distributed denial of service (DDoS) attacks [84-87].

$$\mathrm{MCC} = \frac{\mathrm{TP} * \mathrm{TN} - \mathrm{FP} * \mathrm{FN})}{\sqrt{((\mathrm{TP} + \mathrm{FP}) * (\mathrm{TP} + \mathrm{FN}) * (\mathrm{TN} + \mathrm{FP}) * (\mathrm{TN} + \mathrm{FN}))}} \qquad \text{Eq (15)}$$

B. Network-Layer Threats

The programmability features of 6G also trigger some known and new threat vectors in the network layer, including volumetric and protocol-level DDoS attacks, man-in-the-middle interception, Sybil and Byzantine behavior in distributed consensus or federated aggregation, RIS- and beam-based eavesdropping, and jamming of THz links [88-91].

$$f_t = \mu + \rho \mathrm{GEGR}_{it-1} + \vartheta^{+} \mathrm{EU}^{+}_{it-1} \qquad \text{Eq (16)}$$

Faults or malicious traffic can spread between formerly-isolated networks and tenants from network-slice isolation breaches and compromise of SDN controllers [92, 93].

$$C_t = \vartheta^{-} \mathrm{EU}^{-}_{it-1} + \emptyset^{+} \mathrm{FD}^{+}_{it-1} + \vartheta^{+} \mathrm{EU}^{+}_{it-1} \qquad \text{Eq (17)}$$

C. AI-Model-Layer Threats

The increasing role of embedded models of ML and DL in security for 6G-IoT, the models themselves are becoming targets to be attacked [94-96]. Multiple types of attacks can be distinguished by their taxonomy; in this project at least eight from the following will be taken into account: backdoor attacks, attacks with adversarial examples, combined and blended attacks, data-poisoning attacks, Sybil attacks against federated aggregation, Byzantine attacks, membership and inference attacks that leak private training data, and dropping availability attacks, which degrade collaborative learning [97].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

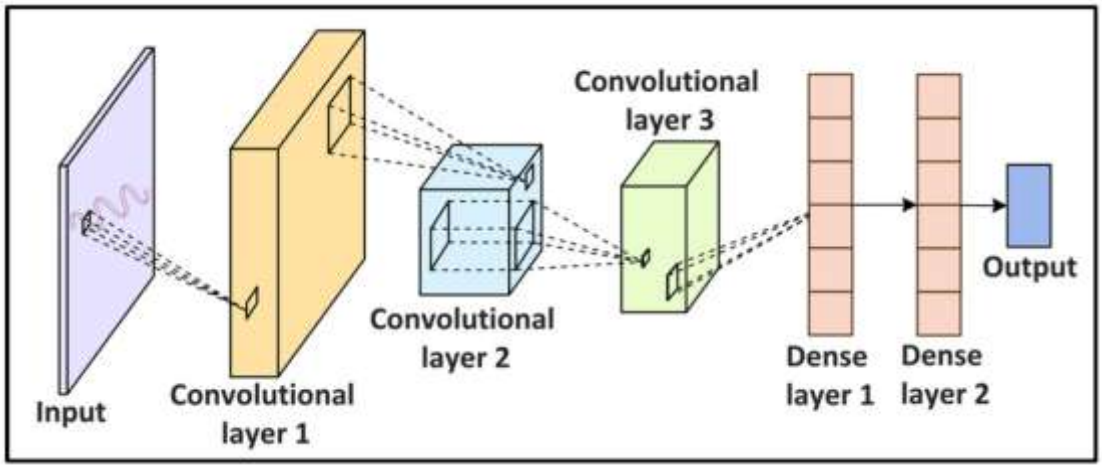


Fig. 1 (b). Generic Intelligent network architecture for enhanced 6G-IoT security using Convolutional Neural Network (CNN) [98].

$$I_t = \omega^{+} TI^{+}_{it-1} + \omega^{-} TI^{-}_{it-1} \qquad \text{Eq (18)}$$

Another, less studied, category of AI-native 6G network control threat identified is reward-poisoning attacks on reinforcement learning agents serving as network controllers [99].

$$\Delta f_{t_i} = \sum_{j=1}^{n-1} \alpha j \, \Delta GERG_{it-1} + \sum_{j=0}^{n2} (\pi^{j+} \Delta EU^{+}_{it-j} \qquad \text{Eq (19)}$$

TABLE III TAXONOMY OF SECURITY THREATS IN 6G-ENABLED IoT NETWORKS

Layer	***Representative Threats***	***Primary Impact***
Perception / Device	Physical capture, firmware tampering, side-channel attacks, PUF spoofing, botnet recruitment	Loss of device integrity; entry point for large-scale botnets [100, 101]]
Network / Connectivity	DDoS, MITM, jamming, RIS/beam eavesdropping, slice-isolation breach, SDN controller compromise	Service disruption, data interception, cross-tenant contamination [102], [103]
AI / ML Model	Data poisoning, backdoor attacks, adversarial examples, Sybil/Byzantine FL attacks, membership inference, reward poisoning (DRL)	Corrupted detection models, privacy leakage, unsafe autonomous decisions [104], [105]
Cross-Layer / Trust	Identity spoofing, unauthorized lateral	Erosion of end-to-end trust across heterogeneous

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

movement, weak zero-trust enforcement	domains [106], [107]

IV. Edge AI and Machine Learning for 6G-IoT Security

This section introduces some essential techniques of edge AI and machine learning to solve the security problems of 6G-IoT. It emphasizes key challenges and opportunities arising from intelligent, distributed, and adaptive learning techniques for improving threat detection, intrusion detection, anomaly identification, privacy protection and secure resource management. Specific focus is dedicated to Federated Learning, Deep Learning [108], Hybrid ML models [109], Deep Reinforcement Learning [110], TinyML [111] and Explainable AI [112]. These enable security intelligence to act near IoT devices and near the network edges, solving latency issues, scalability concerns, enabling real-time security decisions, and mitigating privacy and resource challenges.

$$\Delta f_{t_1} = \sum_{j=0}^{n3} (\tau^{j+} \Delta FD^{+}_{it-j} + \tau^{-}_{j} \Delta FD^{-}_{it-j}) \qquad \text{Eq (20)}$$

A. Federated Learning-Based Intrusion Detection

Federated Learning, nodes can collaboratively train the ID models with only the exchange of ID model parameters, as compared to sending raw traffic data, thereby meeting the privacy and bandwidth requirement of centralized approaches [25]. Semi-supervised Federated schemes alleviate the labeling efforts on the edge devices while preserving detection accuracy in non-independent and identically disrupted environments [26].

$$\Delta f_{t_2} = \sum_{j=0}^{n3} (\tau^{j+} \Delta FD^{+}_{it-j} + \tau^{-}_{j} \Delta FD^{-}_{it-j}) \qquad \text{Eq (21)}$$

Improved robustness to statistical heterogeneity in large-scale, heterogeneous IoT deployments due to clustering-based and hierarchical Federated Learning architectures which group together devices sharing similar traffic characteristics before aggregation. In industrial IoT environments with devices' nature of diversity and uneven connectivity & computing resources, the latency and energy cost of aggregation are minimized under asynchronous and delay-aware variants of Federated Learning [27]. In recent years, systematic reviews validate Federated Learning based intrusion detection as one of the most prolific research approaches in the field of IoT security, and list open problems like secure aggregation protocols and the vulnerability to poisoning.

$$\Delta f_{t_2} = \sum_{j=0}^{n4} (\sigma^{j+} \Delta TI + \sigma^{-}_{j} \Delta TI^{-}_{it-j}) + \varepsilon_{it} \qquad \text{Eq (22)}$$

B. Deep and Hybrid Learning Architectures

Federated Learning distributed-training dimension, there are also underlying models' architectures, and their selection significantly impacts both detection accuracy and the

Online ISSN 3007-3197
Print ISSN 3007-3189

computational overhead [28]. Industrial and consumer IoT intrusion detection has been explored in different approaches to enable the use of spatial, temporal and topological network traffic structure via convolutional neural network–long short-term memory CNN-LSTM hybrids; autoencoders as well as graph neural networks. Measures taken to design specific and efficient local models turn out to achieve comparable centralized detection accuracy while meeting tight latency requirements in a federated deep-learning framework for an industrial cyber-physical system [29]. Examples of such types of frameworks are zero-day botnet detection systems that use federated deep learning combined with deep learning at the edge of the deployment network, showing the applicability of this class of solutions to unknown attack signatures [30].

C. Deep Reinforcement Learning for Adaptive Defense

AI-native 6G radio access networks and slicing, deep reinforcement learning (DRL) provides a means for the network controller to discover customizable defense and resource-allocation policies through interaction with the environment, a crucial capability [31]. Explanation-based DRL methods also seek to ensure that the slicing and defense decisions are explainable to network operators to mitigate the issue of trust concern in fully autonomous control loops [32]. DRL-based controllers, however, add their respective attack surface, one of which concerns reward-poisoning attacks, which incrementally push the policy learned by the agent towards unsafe policies; this is a topic which, in comparison to threats in supervised learning, has been relatively under-effected.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

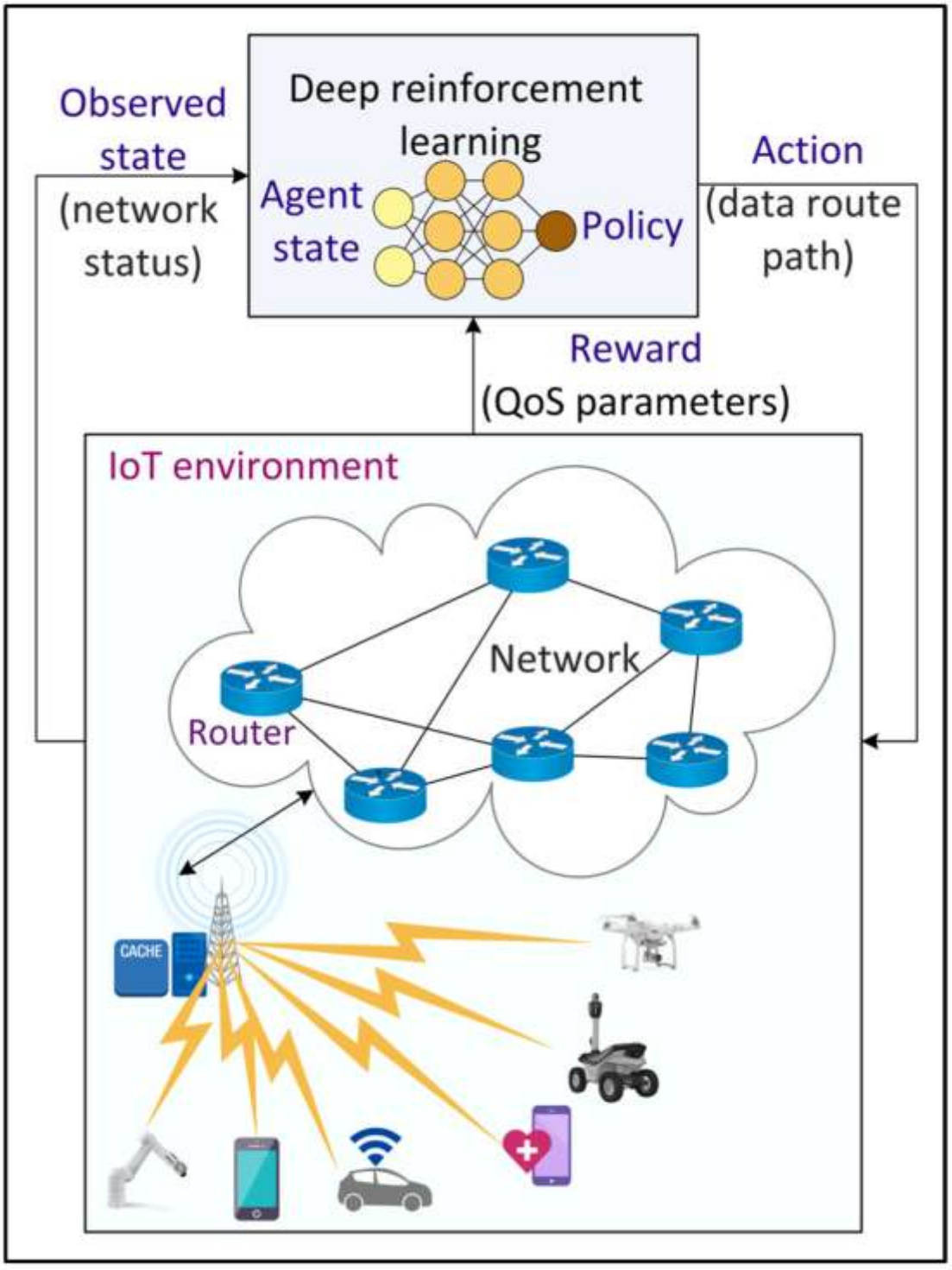


Fig. 1 (c). Generic Deep Reinforcement Learning Architecture for enhanced 6G-IoT security

D. TinyML and Extreme-Edge Inference

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

TinyML is the compression of ML and DL inference, and increasingly incremental on-device training, that runs efficiently in the kilobytes to megabytes of memory available to most IoT use cases implemented in microcontroller-class devices with methods like quantization, pruning, knowledge distillation, and sparse versus reconfigurable accelerators. Recent work has shown examples for real-time anomaly detection for predictive maintenance and consumer internet-of-things protection leveraging TinyML with good accuracy-to-footprint trade-offs as well as variants of transformer-based and incremental-learning algorithms that are adapted for the extreme edge [33]. With this in mind, TinyML is increasingly integrated with federated learning also known as "TinyFL" to provide constant and private model optimization directly at the clamp of the limited resources in 6G-IoT endpoints, especially battery-powered ones.

E. Explainable AI for Trust and Auditability

Network operations and network security tasks are handed over to more and more autonomous ML and DL models, and explainability becomes a must for operators to be trusted, to meet regulatory requirements, and to react appropriately when incidents occur. Recent surveys list XAI techniques for 5G/6G security and network-slicing decisions and point to the nature of a tradeoff between model complexity and interpretability as a key open question for AI-native 6G [34]. Seeding XAI in the security pipeline allows human threat analysts to validate the automated threat classification before taking costly action to fix it.

F. Blockchain-Assisted Zero-Trust Access Control

The continuous verification of every device, user and service, irrespective of network location, is increasingly being suggested as the backbone for identity and access-control for the 6G-IoT [35]. Distributed ledgers are useful for distributed trust without a single point of failure: They are blockchain-based recording of the numbers of authentication events and logging of the provenance of model-updates, as exploited in spectrum-access security, vehicular handover authentication [36] and consumer-IoT identity management. Some approaches on how to embed ZTA directly into the federated-learning client-admission process have also been suggested to prevent slow-poisoning attacks against federated models [37].

TABLE IV COMPARATIVE SUMMARY OF REPRESENTATIVE EDGE AI/ML TECHNIQUES FOR 6G-IoT SECURITY

Techniques	Primary Strength	Key Limitation
Federated Learning (FL)	Privacy-preserving and distributed; scales across	Vulnerable to poisoning and Sybil attacks;

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

IDS [3], [4], [5], [7], [9]	heterogeneous devices	aggregation communication overhead
Deep / Hybrid Learning (CNN-LSTM, GNN, Autoencoder) [8], [10], [22]	High detection accuracy for complex, high-dimensional traffic	Computationally intensive; limited native interpretability
Deep Reinforcement Learning (DRL) [18], [19], [28]	Adaptive, self-optimizing policies for dynamic 6G environments	Sample inefficiency; susceptible to reward-poisoning attacks
TinyML / Extreme-Edge Inference [23], [24], [25], [26], [27]	Minimal memory and energy footprint; enables real-time on-device detection	Constrained model capacity; accuracy–footprint trade-off
Explainable AI (XAI) [2], [30]	Improves operator trust, auditability, and regulatory compliance	Explanation fidelity vs. model complexity trade-off
Blockchain-Assisted Zero-Trust [20], [21], [29], [31], [32]	Decentralized, tamper-resistant identity and provenance management	Ledger latency and energy costs may conflict with 6G URLLC targets

V. Proposed Enhanced Framework

To address limitations listed above, notably the absence of a unified framework that accommodates privacy-preserving distributed learning, defense under extreme conditions at the edge, extreme-edge inference and auditable trust within an integrated framework, we propose an Enhanced 6G-IoT security framework, which is a proposed five-layer architecture with a closed detection-response feedback loop.

A. Layered Architecture

The proposed solution architecture is shown in Fig.1. Perception and Device Layer consists of sensors, wearables, industrial IoT nodes and mobile units secured using light-weight cryptography and PUF-based authentication. The Edge AI and Fog Security Layer enables most security decisions without round-trip to the cloud by providing on-device or TinyML inference, a federated-learning aggregator, lightweight hybrid models such as CNN-LSTM and autoencoders, and an edge trust, anomaly scoring module. The 6G Network Connectivity Layer features network

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

slicing, SDN/NFV based isolation, physical-layer security (THz + RIS), zero-trust access control, and blockchain-based identity & ledger services [38]. On the edge, the Cloud Core Intelligence Layer merges local model updates to a global model, deploys heavier deep and reinforcement-learning engines, stores heavier threat-intelligence feeds, stores digital-twin state, and applies XAI-based auditing prior to decisions being forwarded back to the edge. Lastly, the Application Layer bridges those security services to verticals like smart healthcare, Industry 5.0, smart grid intelligent transportation and smart cities.

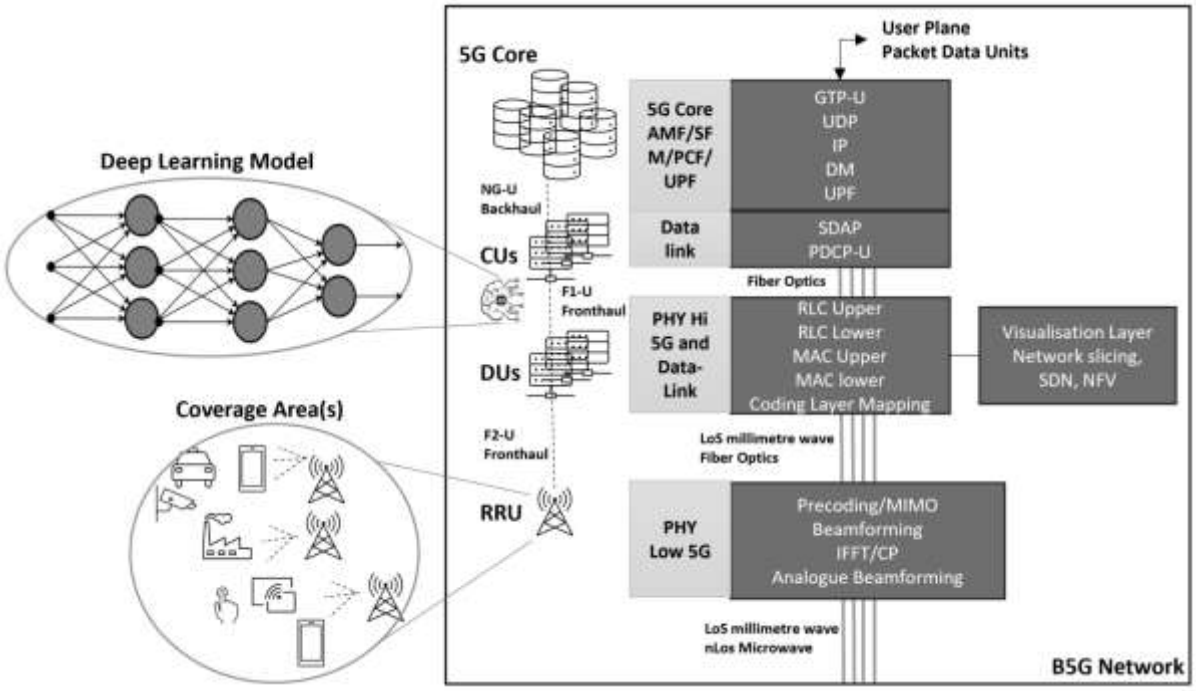


Fig. 1 (d). Intelligent network Layered architecture for enhanced 6G-IoT security framework with Edge AI/ML integration.

B. Closed-Loop Detection-Response Workflow

The workflow of the operation is shown in figure 2. Preprocessing occurs at the edge (normalization, feature selection) and on-device anomaly/intrusion scoring is done by a lightweight model. IoT device traffic and 6G traffic data are processed at the edge (normalization and feature selection) first and then processed at the device level using a light-weighted local model. There is a threshold distinction between benign traffic (which is passively monitored) and suspicious traffic (which initiates the transmission of model-updates in a privacy-preserving manner). Updates undergo zero-trust verification and get recorded on a blockchain ledger before being sent along a 6G slice- or RIS-secured link. The essence of updates is to first combine the information into a refined global model, and then validate the updated threat classification along with generating human-interpretable alerts in advance to any action taken by an

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

automated response that would involve isolating a device, reconfiguring a network or updating a security policy. A closed loop for continuous adaptation to new threats is then closed at the edge nodes with refined global model [39].

C. Design Rationale

This framework is built on four principles that have been extracted from sections III and IV. First, privacy-by-architecture: data is always at the device edge tier, as with FL-based systems. Second, latency-aware tiering: most decisions are made locally and only aggregated; more complicated analytics and audit are made with cloud's participation; the cloud-based IDS lacks a cost of round trip - time penalty. Third, verifiable trust: The zero-trust authentication and blockchain logging polices both explicitly and implicitly reject models updates or devices, addressing the concerns in Table III towards Sybil attack, Byzantine attack and identity spoofing attack. Fourth, human-valid autonomy: XAI validation capable before automation responses are taken: latency advantages of automation vs accountability requirements growingly placing on AI-driven network security [40].

It is important to reiterate that the proposed framework is more of a conceptual, literature-based reference model, not an empirically proven system: Its layers and workflow are amalgamation of design patterns and experiences based on the literature consulted for reports of best practice, not a new system implementation. The framework would need to be validated in a real testbed simulation environment reproducing realistic wireless IoT traffic and representative THz/RIS-assisted 6G links in the future, as well as evaluation of the detection-capability, overhead, privacy, deplorability and robustness criteria in Table V under adversarial conditions like poisoning and reward manipulation, at least in terms of a testbed or simulation environment of the successful system that includes both THz/RIS-assisted 6G wireless links and representative IoT traffic in the future, deployment of the federated aggregation, TinyML inference, and XAI-auditing modules on the previously mentioned heterogeneous edge hardware, and evaluations of all the previously mentioned criteria of detection-capability, overhead, privacy, deplorability and robustness under adversarial circumstances such as poisoning and reward manipulation. We acknowledge this end-to-end implementation and benchmarking project as one of the main areas for future work.

VI. Comparative Analysis and Discussion

The trends highlighted in the qualitative comparisons of the different technique family groups in the reviewed literature are in Table V to show the potential application feasibility of the various 6G-IoT techniques in latency sensitive resource-constrained deployments. The ratings are only general patterns, as there are lots of variations in the experimental settings, data sets and the hardware in the cited works.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

TABLE V QUALITATIVE TRADE-OFF COMPARISON OF EDGE AI/ML PARADIGMS FOR 6G-IoT SECURITY

Paradigm	**Detection Capability**	**Comm. Overhead**	**Privacy Preservation**	**Edge Deplorability**	**Adversarial Robustness**
Centralized Deep Learning	High	High	Low	Low	Low–Medium
Federated Learning	Medium–High	Medium	High	Medium–High	Medium (vulnerable to poisoning)
TinyML / Extreme Edge	Medium	Low	High	High	Medium
Deep Reinforcement Learning	High (adaptive)	Medium	Medium	Medium	Low (reward poisoning)
XAI-Augmented Pipelines	High (with audit)	Medium	Medium–High	Medium	Medium–High
Blockchain-Assisted Zero-Trust	N/A (access control)	Medium–High	High	Medium	High (identity layer)

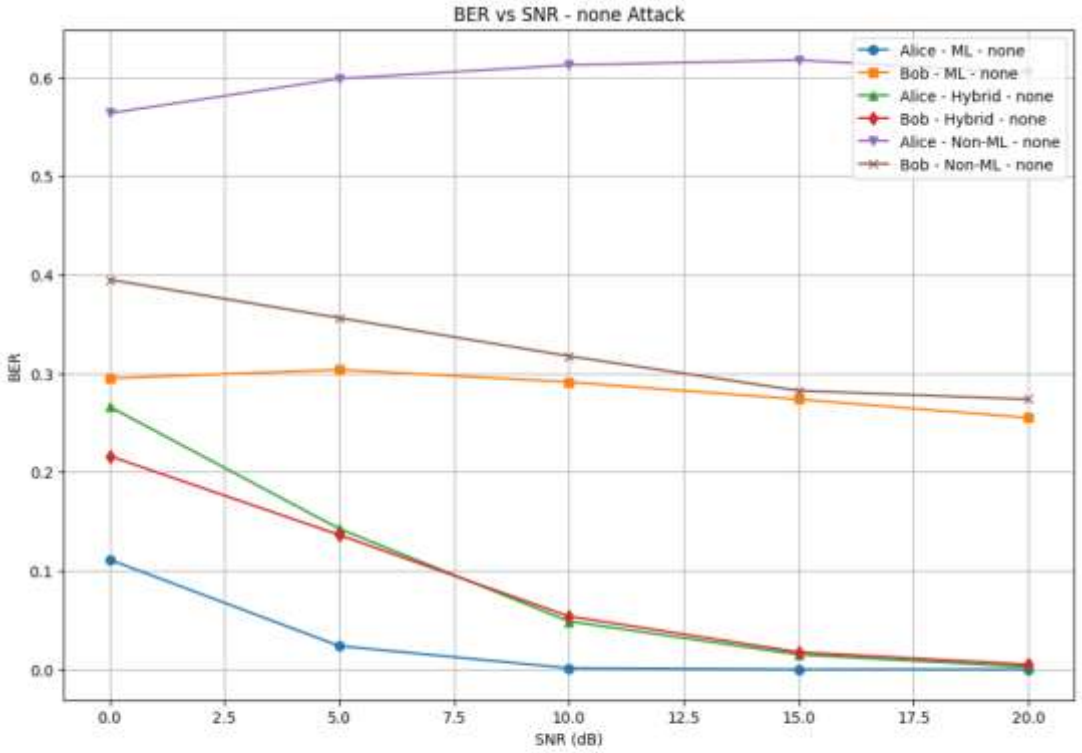
This comparison finds a key divide in the design of 6G-IoT security: methods capable of achieving the greatest detection accuracy centralized deep learning, DRL are associated with the highest computational overhead communication load, or the most restricted privacy protection, while those that are suitable for edge deployment TinyML trade detection capability for being less effective. This inspires the proposed hybrid tiered approach outlined in the proposed framework Section V: lightweight local models are used for handling the bulk of the traffic, whereas heavier and more precise models are used only as needed, down the federated path of updates, in the cloud tier. The analysis also reveals that each technique family discussed on their own is insufficient to solve adversarial robustness; all these techniques need to be

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

complemented by one another, where federated aggregation safeguards, blockchain-based provenance and XAI-based auditing are complementary layers of security [41].



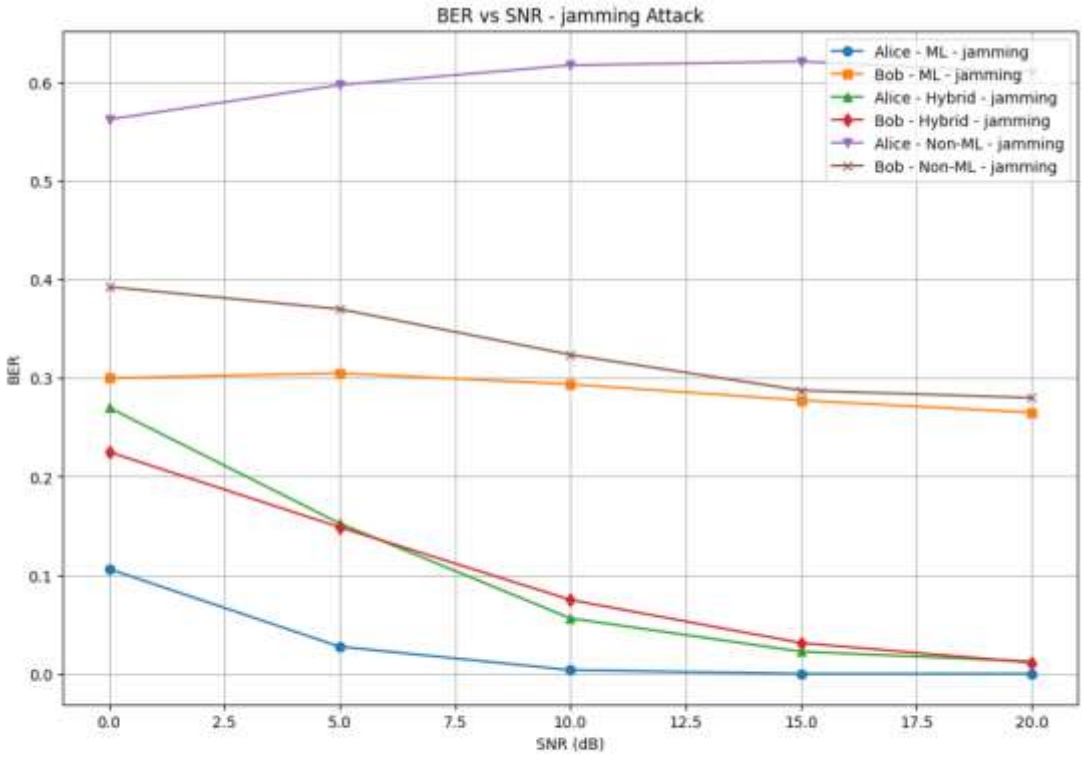
(a) No attack.

Fig. 2 (a). Intelligent network Evaluation when No Attack using Model Accuracy with different approaches of non-ML, ML and hybrid model

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



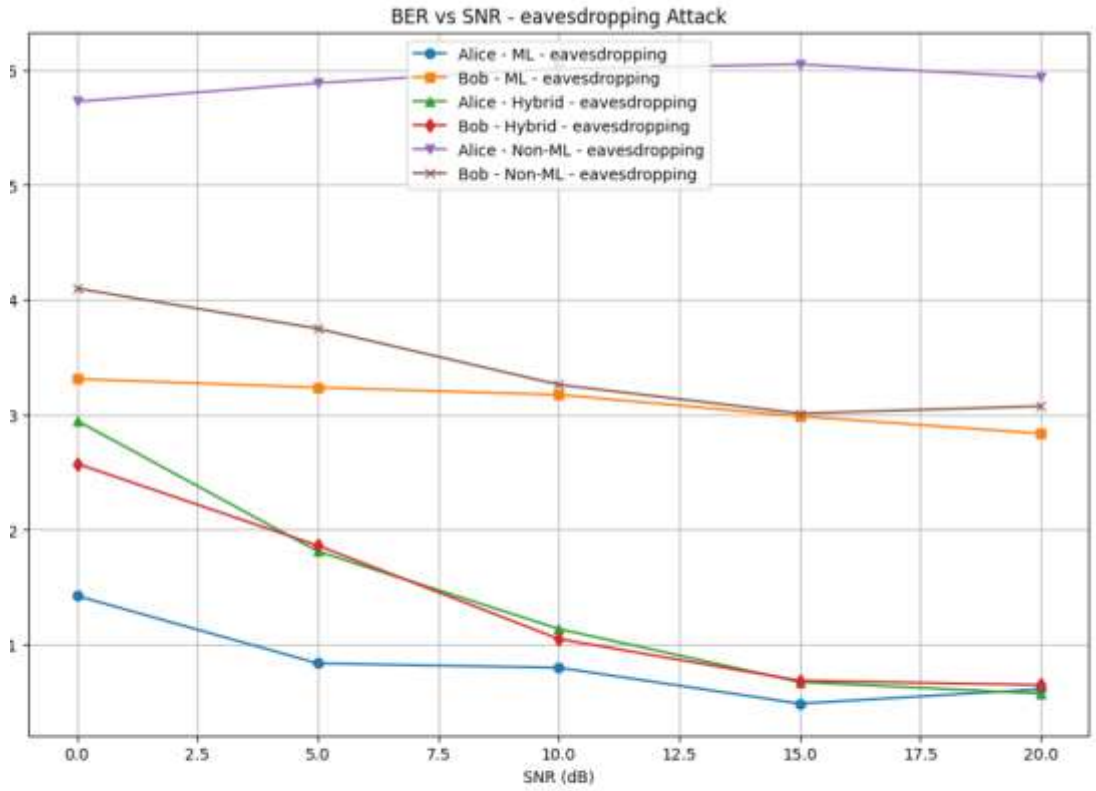
(b) Jamming attack.

Fig. 2 (b). Intelligent network Evaluation when Jamming Attack using Model Accuracy with different approaches of non-ML, ML and hybrid model

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



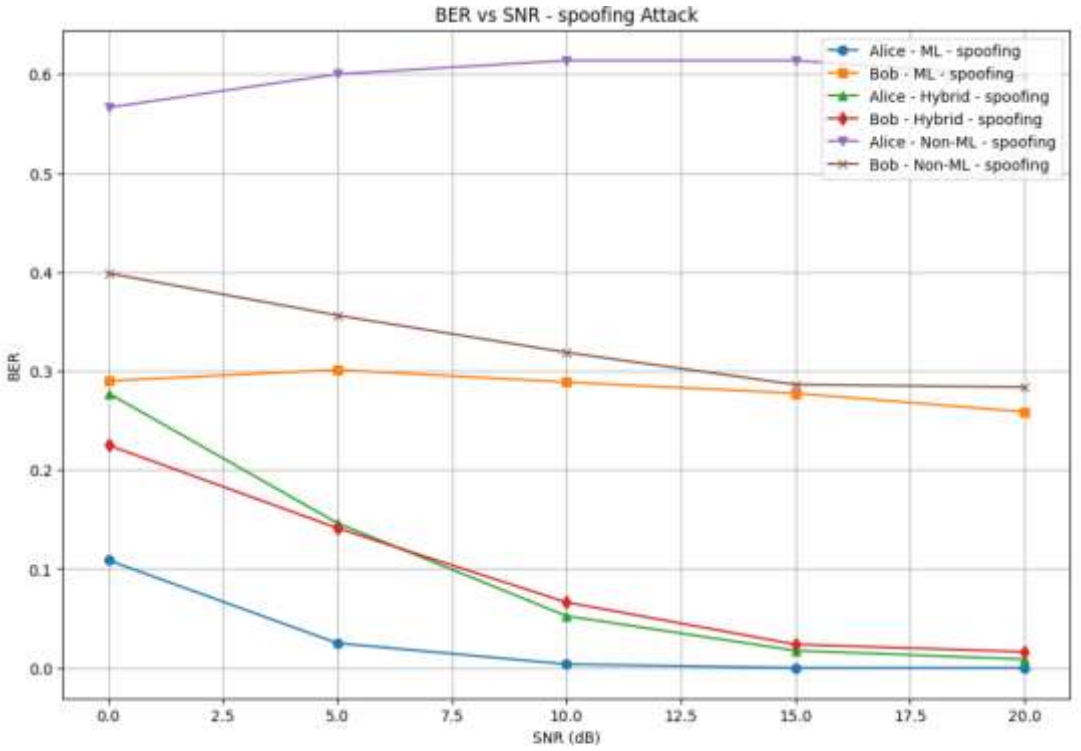
(c) Eavesdropping.

Fig. 2 (c). Intelligent network Evaluation when Eavesdropping using Model Accuracy with different approaches of non-ML, ML and hybrid model

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



(d) Spoofing.

Fig. 2 (d). Intelligent network Evaluation when Spoofing using Model Accuracy with different approaches of non-ML, ML and hybrid model

VII. Open Challenges and Future Research Directions

Although significant strides have been made, there are still several open challenges that need to be resolved before the deployment of security frameworks based on Edge AI ML can be assured at a 6G scale.

1. Lack of 6G-representative datasets: Solely, most publicly-available intrusion-detection datasets are outdated and fail to represent traffic patterns of the more recent 6G like THz links, RIS-assisted routing, network slicing, which means that the external validation of reported detection accuracies is questionable.
2. Adversarial and poisoning robustness: Federated and Reinforcement Learning pipelines still lack the ability to be robust both against Sybil attacks, Byzantine attacks, and against reward poisoning; robust aggregation and anomaly-aware client selection is still maturing.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

3. Optimizing between detection fidelity and judicious memory, compute and battery usage regimes is a trade-off at the extreme
4. Transforming the production of explanations to be understandable to humans in real time for the high volume of 6G traffic – with minimal impact on the required latency remains an engineering challenge.
5. Lightweight post-quantum cryptography and resource limited perception layer devices: When quantum computing comes into reality, lightweight post-quantum cryptography needs to balance the resource limited perception - layer devices with the low latency requirements of the 6G systems.
6. Cross-domain and cross-operator trust: zero-trust principles need to be expanded to interoperate across multiple domain and multi-operator network slicing, and in space-air-ground integration.
7. Sustainability of AI security: The high energy consumption required for ongoing federated training, blockchain consensus and cloud-based monitoring by billions of devices is a concern for sustainability, which needs to be addressed by considering the system design to be Green-AI capable.
8. A potential extension of the combination of the proposed framework and digital twins would be for the use of digital twins in real-time whilst in practice, it would enable a change from reactive to proactive threat mitigation, but the synchronization-channel integrity would present as a new attack surface and need protection.

VIII. Conclusion

The study presents the different approaches to secure 6G-enabled IoT networking using Edge AI and machine learning. We explored the enabling technologies and structure of 6G-IoT convergence, made a layer-wise taxonomy of different threats from device-, network- and AI-model-levels, and critically integrated recent work in federated learning, deep learning, hybrid learning, deep reinforcement learning, TinyML, Explainable AI, and blockchain in zero-trust approach. Based on the received gaps, we designed an Enhanced 6G-IoT Security Framework, which unified the identified techniques within a security framework comprising five layers and a closed loop detection-response workflow while not involving personal privacy. The comparative analysis showed that none of the technique families is simultaneously optimal for detection accuracy, communication overhead, privacy, deploy ability at the edge, or adversarial robustness, supporting the need for hybrid, multi-tiered systems like the system presented here. Future studies should focus on developing the benchmark datasets for characterizing 6G-IoT networks and developing reliable

Online ISSN 3007-3197
Print ISSN 3007-3189

aggregation mechanisms that are designed against poisoning and reward-manipulation attacks, as well as on latency-aware explainability approaches and on quantum-safe designs that thrive in the exponential network expansion that the promises of 6G-IoT bring.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

M. A. Ferrag, O. Friha, B. Kantarci, N. Tihanyi, L. Cordeiro, M. Debbah, D. Hamouda, M. Al-Hawawreh, and K.-K. R. Choo, “Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses,” IEEE Commun. Surveys Tuts., 2023, doi: 10.1109/COMST.2023.3317242.

T. Senevirathna, V. H. La, S. Marchal, B. Siniarski, M. Liyanage, and S. Wang, “A survey on XAI for 5G and beyond security: Technical aspects, challenges and research directions,” IEEE Commun. Surveys Tuts., vol. 27, no. 2, pp. 941–973, 2025.

Y. Wang, Z. Xue, T. Ohtsuki, B. Adebisi, and G. Gui, “Semisupervised federated-learning-based intrusion detection method for Internet of Things,” IEEE Internet Things J., vol. 10, no. 10, pp. 8645–8657, 2023.

J. L. Hernandez-Ramos, G. Karopoulos, E. Chatzoglou, V. Kouliaridis, E. Marmol, A. Gonzalez-Vidal, and G. Kambourakis, “Intrusion detection based on federated learning: A systematic review,” ACM Comput. Surveys, vol. 57, no. 12, pp. 1–65, 2025.

S. Liu, Y. Yu, Y. Zong, P. L. Yeoh, L. Guo, B. Vucetic, T. Q. Duong, and Y. Li, “Delay and energy-efficient asynchronous federated learning for intrusion detection in heterogeneous industrial Internet of Things,” IEEE Internet Things J., vol. 11, no. 8, pp. 14739–14754, 2024.

T. Liu and O. Dib, “Advanced intrusion detection for IoT devices using federated deep

Online ISSN 3007-3197
Print ISSN 3007-3189

learning," Int. J. Inf. Secur., vol. 25, art. no. 19, 2026.

V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," IEEE Internet Things J., vol. 9, no. 4, pp. 2545–2554, 2022.

B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," IEEE Trans. Ind. Informat., vol. 17, no. 8, pp. 5615–5624, 2021.

S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices," IEEE Internet Things J., vol. 9, no. 5, pp. 3930–3944, 2022.

N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. Lira Neto, and V. H. C. de Albuquerque, "Industrial Internet-of-Things security enhanced with deep learning approaches for smart cities," IEEE Internet Things J., vol. 8, no. 8, pp. 6393–6405, 2021.

F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1686–1721, 2020.

Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2694–2724, 2020.

M. Mitev, A. Chorti, H. V. Poor, and G. Fettweis, "What physical layer security can do for 6G security," IEEE Open J. Veh. Technol., vol. 4, pp. 375–388, 2023.

N. Kato, B. Mao, F. Tang, Y. Kawamoto, and J. Liu, "Ten challenges in advancing machine learning technologies toward 6G," IEEE Wireless Commun., vol. 27, no. 3, pp. 96–103, 2020.

I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," Mobile Netw. Appl., vol. 28, pp. 296–312, 2023.

M. M. Azari et al., "Evolution of non-terrestrial networks from 5G to 6G: A survey," IEEE Commun. Surveys Tuts., vol. 24, no. 4, pp. 2633–2672, 2022.

T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the Internet of Things: Applications, challenges, and opportunities," IEEE Internet Things Mag., vol. 5, no. 1, pp. 24–29, 2022.

F. Rezazadeh, H. Chergui, and J. Mangues-Bafalluy, "Explanation-guided deep reinforcement learning for trustworthy 6G RAN slicing," in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), 2023, pp. 1026–1031.

T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," IEEE Trans. Neural Netw. Learn. Syst., vol. 34, no. 8, pp. 3779–3795, 2023.

H. Fang, Y. Zhu, Y. Zhang, and X. Wang, "Decentralized edge collaboration for seamless handover authentication in zero-trust IoV," IEEE Trans. Wireless Commun., vol. 23, no.

Online ISSN 3007-3197
Print ISSN 3007-3189

8, pp. 8760–8772, 2024.

S. M. Nagarajan, G. G. Devarajan, M. S. Thangakrishnan, T. V. Ramana, A. K. Bashir, and A. A. AlZubi, "Artificial intelligence-based zero trust security approach for consumer industry," IEEE Trans. Consum. Electron., vol. 70, no. 3, pp. 5411–5418, 2024.

A. Babu and A. Bagubali, "Federated learning with sailfish-optimized ensemble models for anomaly detection in IoT edge computing environment," IEEE Access, vol. 13, pp. 53171–53187, 2025.

I. Katib, E. Albassam, S. A. Sharaf, and M. Ragab, "Safeguarding IoT consumer devices: Deep learning with TinyML driven real-time anomaly detection for predictive maintenance," Ain Shams Eng. J., vol. 16, no. 2, art. no. 103281, 2025.

A. Krishna et al., "RAMAN: A reconfigurable and sparse TinyML accelerator for inference on edge," IEEE Internet Things J., vol. 11, no. 14, pp. 24831–24845, 2024.

P. Andrade, M. Silva, M. Medeiros, D. G. Costa, and I. Silva, "TEDA-RLS: A TinyML incremental learning approach for outlier detection and correction," IEEE Sensors J., vol. 24, no. 22, pp. 38165–38173, 2024.

E. Tabanelli, G. Tagliavini, and L. Benini, "Optimizing random forest-based inference on RISC-V MCUs at the extreme edge," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 41, no. 11, pp. 4516–4526, 2022.

L. Barbieri, M. Brambilla, M. Stefanutti, C. Romano, N. De Carlo, and M. Roveri, "A tiny transformer-based anomaly detection framework for IoT solutions," IEEE Open J. Signal Process., vol. 4, pp. 462–478, 2023.

V. Rajapakse, I. Karunanayake, and N. Ahmed, "Intelligence at the extreme edge: A survey on reformable TinyML," ACM Comput. Surveys, vol. 55, no. 13s, pp. 1–30, 2023.

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS) (pp. 1–6). IEEE. https://doi.org/10.1109/MiCIS.2015.7348942

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Aljumah, F. (2023). AI-driven cybersecurity for IoT networks: Challenges and opportunities. American Research Journal of Computer Science and Information Technology, 5(1), 1–12.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the

Online ISSN 3007-3197
Print ISSN 3007-3189

4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

De Paola, A., et al. (2023). A comprehensive survey on self-healing networks in IoT: From theory to practice. IEEE Communications Surveys & Tutorials, 25(4), 2800–2835.

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2012). An intrusion detection system using ML algorithms. International Journal of Machine Learning and Computing, 2(6), 626–630.

Kasongo, P., & Sun, Y. (2021). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 8(1), Article 35. https://doi.org/10.1186/s40537-021-00431-2

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications, Inc. (Thousand Oaks, CA).

McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), 69–74. https://doi.org/10.1145/1364654.1364666

Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). The MIT Press (Cambridge, MA).

Chollet, F. (2021). Deep learning with Python (2nd ed.). Manning Publications Co. (Shelter Island, NY).

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Informatics (CISIM) (pp. 53–58).

Naseer, S., et al. (2021). Enhanced network intrusion detection using deep learning. Computer Networks, 196, Article 108234. https://doi.org/10.1016/j.comnet.2022.408234

Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML for cybersecurity. IEEE Communications Surveys & Tutorials, 18(2), 781–812.

Khan, M. A., et al. (2022). Blockchain for secure IoT: A survey. IEEE Internet of Things Journal, 9(1), 1–20.

Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In Proceedings of the Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2018.23200

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press (Cambridge,

Online ISSN 3007-3197
Print ISSN 3007-3189

MA). http://www.deeplearningbook.org/

Jones, J. H., & Bridges, S. M. (2001). An immune system architecture for distributed intrusion detection. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC) (Vol. 3, pp. 2280–2285).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Zhang, Y., et al. (2024). Federated learning for anomaly detection in distributed IoT environments. IEEE Transactions on Industrial Informatics, 20(5), 6789–6799.

Akhtar, M., Jabeen, T., Aziz, R., Amin, M., Rizwan, S., & Hamid, K. (2025). Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches. Annual Methodological Archive Research Review, 3(8), 176–214. https://doi.org/10.63075/m5et0t86

Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26–57. https://thesesjournal.com/index.php/1/article/view/131

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, K., ... & Zhou, Y. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110). USENIX Association.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Hussain, F., Abbas, S. G., Shah, G. A., Pervaiz, I., & Khalid, S. (2024). ML in IoT security: A systematic literature review. Journal of Network and Computer Applications, 224, Article 103828. https://doi.org/10.1016/j.jnca.2023.103828

Hamdan, M. (2024). Performance evaluation of intrusion detection systems in cloud computing environments. Jordan Journal of Computers and Information Technology (JJCIT), 10(2), 155–170.

Manju, & Srivastav, V. K. (2025). Review of self-healing IoT networks based AI-driven fault detection and recovery. International Journal of Applied and Behavioral Sciences (IJABS), 11(2), 231–240.

A., Uddin, S., Tanweer, H. A., Rasheed, M. A., Ahmed, M., & Murtaza, H. (2021). Data privacy issue in federated learning resolution using block chain. VFAST Transactions on Software Engineering, 9(4), 51-61.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). An

Online ISSN 3007-3197
Print ISSN 3007-3189

Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 26-33.

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.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

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.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

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.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, L., Ahmad, K., Said, N., Qolomany, B., Qadir, J., & Al-Fuqaha, A. (2020). Active learning based federated learning for waste and natural disaster image classification. IEEE access, 8, 208518-208531.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security

Online ISSN 3007-3197
Print ISSN 3007-3189

Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

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.

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.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful machine learning based privacy-preserving technique for federated learning. The Asian Bulletin of Big Data Management, 4(4), 332-343

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

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.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Online ISSN 3007-3197
Print ISSN 3007-3189

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. arXiv preprint arXiv:2107.10976.

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.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

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.

Ali, M., Khan, H., & Rehman, S. U. (2023). Edge Computing for Low-Latency IoT Applications. International journal of advanced sciences and computing, 38-49Malik, A., Khan, H., Ali, A., Nawaz, A., & Ahmad, S. The Impact of Climatic Parameters on the Streamflows & Future Sustainable Hydro-Energy Generation Predicting Streamflows for the 21st Century Under Climate Change Scenarios.

Ali, M., Khan, H., Din, I. U., Tariq, M. I., & Javed, A. Design and Implementation Role of Middleware in Shared Network Environments: A Systematic Review. Securing the Digital Realm, 229-243.

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S. (2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological Archive Research Review, 3(7), 376-400.

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense

Online ISSN 3007-3197
Print ISSN 3007-3189

for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Basit, A. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem.

Cai, B., Xu, X., Jia, K., Qing, C., & Tao, D. (2016). DehazeNet: An End-to-End System for Single Image Haze Removal. IEEE TIP, 25(11), 5187–5198.

Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2018). VGGFace2: A Dataset for Recognising Faces Across Pose and Age. IEEE FG, 67–74.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE/CVF CVPR, 4685–4694.

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.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

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

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).

Ganesan, S., Manoharan, K. G., & Periyathambi, E. (2025). Hybrid Approach to Detect Fog

Online ISSN 3007-3197
Print ISSN 3007-3189

Level Using CNN and Defog the Video Sequence Using GAN. Traitement du Signal, 42(4), 2039–2052.

Gaspar, M. B. A. F. (2025). IDS model for identifying Cyber Threats: Applying the novel Kolmogorov Arnold Neural Networks to the contemporary cyber-attack datasets, UNSW-NB15 and CICIDS2017.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Gombar, M., Topalović, A., & Pejić Bach, M. (2026). Cost-Aware Lightweight Deep Learning for Intrusion Detection: A Comparative Study on UNSW-NB15 and CIC-IDS2017. Electronics, 15(8), 1603.

Goodfellow, I., et al. (2014). Generative Adversarial Nets. NeurIPS, 27, 2672–2680.

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

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

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

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

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

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,

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

July. 2018

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.

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.

Hamayun Khan, Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

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.

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.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Masab, M. M., Ayub, N., Ghafoor, U., Khan, A. K., Ullah, H., & Murtaza, S. (2026). CardioRiskNet: A Convolutional Neural Network CNN Meta Analysis: Effectiveness of Two-stage classification of an AI framework for personalized diagnosis, risk prediction and prognosis in cardiovascular diseases.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

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

He, K., Sun, J., & Tang, X. (2011). Single Image Haze Removal Using Dark Channel Prior. IEEE TPAMI, 33(12), 2341–2353.

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-

Online ISSN 3007-3197
Print ISSN 3007-3189

19067.

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.

Ibrahim, F. H. M., & Rahim, M. S. M. (2020). Single Image Dehazing Method Based on Current Strategies. Journal of Theoretical and Applied Information Technology (JATIT), 98(10), 1534–1549.

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

Isola, P., Zhu, J.-Y., Zhou, T., & Efros, A. (2017). Image-to-Image Translation with Conditional Adversarial Networks. IEEE/CVF CVPR, 1125–1134.

J. Bonneau, "Why Buy When You Can Rent? Bribery and Vote Buying in Blockchain Voting," in Proc. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 123–130.

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.

K. Croman et al., "On Scaling Decentralized Blockchains," in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

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.

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

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

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

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

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

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

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.

Li, B., et al. (2019). Benchmarking Single-Image Dehazing and Beyond. IEEE TIP, 28(1), 492–505.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

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.

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.

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.

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

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

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.

Online ISSN 3007-3197
Print ISSN 3007-3189

Muhammad Anas, Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

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, 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

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

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

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.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

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

Narasimhan, S. G., & Nayar, S. K. (2002). Vision and the Atmosphere. International Journal of Computer Vision, 48(3), 233–254.

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.

Online ISSN 3007-3197
Print ISSN 3007-3189

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.

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.

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.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

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

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

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.

P. De Filippi and S. Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," Internet Policy Review, vol. 5, no. 3, pp. 1–28, Sep. 2016.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

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.

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.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Ren, W., Liu, S., Zhang, H., Pan, J., Cao, X., & Yang, M.-H. (2016). Single Image Dehazing via Multi-Scale Convolutional Neural Networks. ECCV, 154–169.

Online ISSN 3007-3197
Print ISSN 3007-3189

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

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

Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

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

Saxena, A., Mane, V., & Abhale, A. (2017). Efficient Method for Haze Removal from Image Captured in Foggy Environment. International Journal of Advanced Technology & Engineering Research (IJATER), 7(6), 36–41.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. IEEE/CVF CVPR, 815–823.

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

Sharma, N., Kumar, V., & Singla, S. K. (2021). Single Image Defogging Using Deep Learning Techniques: Past, Present and Future. Archives of Computational Methods in Engineering, 28, 4449–4469.

Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. Journal of Information Systems Engineering and Management, 10(11S), 633-650.

Suganya, R., & Kanagavalli, R. (2020). On the Review of Dehazing Methods for Bad Weather Images. IJETT, Special Issues ICT 2020, 90–98.

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.

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

Vidal Filho, et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An

Online ISSN 3007-3197
Print ISSN 3007-3189

Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.

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, "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

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

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

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

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

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.

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.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.

D. H. Tashman et al., “Trustworthy AI-driven dynamic hybrid RIS: Joint optimization and reward poisoning-resilient control in cognitive MISO networks,” IEEE Trans. Netw. Service Manage., 2026.

M. Khan et al., “Zero trust networks and federated unlearning based 6G edge networks: Attack scenario, security model and future directions,” Internet Technol. Lett., 2025.

H. Sun, Y. Liu, A. Al-Tahmeesschi, A. Nag, M. Soleimanpour-Moghadam, B.

Online ISSN 3007-3197
Print ISSN 3007-3189

Canberk, H. Arslan, and H. Ahmadi, "Advancing 6G: Survey for explainable AI on communications and network slicing," IEEE Open J. Commun. Soc., 2025.

B. Goswami and H. Choudhury, "Securing 5G-enabled IoT with blockchain: A technical review," SN Comput. Sci., vol. 6, art. no. 755, 2025.

A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap," J. Netw. Comput. Appl., vol. 217, art. no. 103677, 2023

Q. Xu, Z. Su, and R. Li, "Security and privacy in artificial intelligence-enabled 6G," IEEE Netw., vol. 36, no. 5, pp. 188–196, 2022.

S. Zeb, M. A. Rathore, S. A. Hassan, S. Raza, K. Dev, and G. Fortino, "Toward AI-enabled NextG networks with edge intelligence-assisted microservice orchestration," IEEE Wireless Commun., vol. 30, no. 3, pp. 148–156, 2023.

A. Hazra, A. Munusamy, M. Adhikari, and L. K. Awasthi, "6G-enabled ultra-reliable low latency communication for Industry 5.0: Challenges and future directions," IEEE Commun. Standards Mag., vol. 8, no. 2, pp. 36–42, 2024.

M. Adhikari and A. Hazra, "6G-enabled ultra-reliable low-latency communication in edge networks," IEEE Commun. Standards Mag., vol. 6, no. 1, pp. 67–74, 2022.

M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," IEEE Access, vol. 11, pp. 80218–80245, 2023.

S. Ghosh and S. K. Ghosh, "FeeL: Federated learning framework for elderly healthcare using edge-IoMT," IEEE Trans. Comput. Soc. Syst., vol. 10, no. 5, pp. 2696–2708, 2023.

Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv, "Blockchain in big data security for intelligent transportation with 6G," IEEE Trans. Intell. Transp. Syst., 2021.

M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," IEEE Internet Things J., vol. 6, no. 4, pp. 6822–6834, 2019.