THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 6. Issue 1 (2026)
https://doi.org/10.62019/vzh8q026

ASIAN BULLETIN OF BIG DATA MANAGEMENT
ISSN (Print): 2959-0795
http://abbdm.com/
ISSN (online): 2959-0809

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

Muhammad Hamza Akhtar*, Umair Ghafoor, Osama Imran, Nasir Ayub, Mian Muhammad Abdullah, Hamayun Khan

Chronicle

Article history
Received: Nov 15, 2025
Received in the revised format: Dec 29, 2025
Accepted: Jan 20 2026
Available online: Jan 31, 2026

Muhammad Hamza Akhtar* is currently affiliated with the Department of Information Technology, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan.

Email:uhammadhamza.docs@gmail.com

Umair Ghafoor is currently affiliated as Deputy Head of Engineering at Calrom Limited, M1 6EG, United Kingdom.

Email: umairghafoor@hotmail.com

Osama Imran is currently affiliated with the School of Electrical Engineering and Computer Sciences, NUST, Islamabad, National University of Science and Technology (NUST).

Email: oimran.mscs25seecs@seecs.edu.pk

Email: osamaimran135@gmail.com

Nasir Ayub is currently affiliated as Deputy Head of Engineering at Calrom Limited, M1 6EG, United Kingdom.

Email:nasir.ayyub@hotmail.com

Mian Muhammad Abdullah is currently affiliated with the Department of Information Technology, TezHost, Gulberg 44022, Islamabad, Pakistan

Email: amian1886@gmail.com

Hamayun Khan is currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan.

Email: hamayun.khan@superior.edu.pk

Corresponding author *

Abstract

Artificial intelligence, machine learning (ML) is transforming the self-healing systems. These are mechanisms that are able to detect issues, anticipate on their occurrence and repair themselves without the assistance of an individual. In this paper, the author discusses how AI and ML may be applied to state-of-the-art self-healing systems with the help of predictive analysis, anomaly discovery, and automated recovery of the network. We discuss artificial intelligence methods such as neural networks, decision trees and reinforcement learning that are employed to predict and model failures in systems. In learning with historical and real-time data, it is possible to make predictions of a problem and begin correcting it before such a problem occurs, utilizing modern networks using ML algorithms. The article also compares the existing processes and outlines a framework for how predictive analytics and recovery algorithms can work together in real-time. As evidence of successful and secure AI-driven self-healing computer systems, we consider various practical applications and case studies in such fields as self-driving automobiles, cloud computing, and industrial automation. A few of the issues that arise include model accuracy, data quality and moral issues. Tables and figures present the performance of the proposed architecture and various models of ML. The integration of machine learning and self-healing capabilities indicates a significant step towards the creation of adaptable AI systems. The article contributes to the novel artificial-intelligence and machine-learning framework of reliable Internet-of-Things (IoT) networks, autonomic computing via a MAPE-K loop, reinforcement learning and bio-inspired concepts to achieve proactive defense mechanisms with over 90% detection rates and a recovery time of less than 5 minutes. The paper is characterized by the quality of literature assessment, clear statement of research issue, problematics and the presentation of hybrid solutions addressing some of the most common IoT threats, including distributed denial-of-service (DDoS) and zero-day exploits. However, the paper is significantly reliant on the simulation-based assessment to a significant degree and only slight empirical verification of hardware and scaling issues in the heterogeneous deployments can be observed. The current review includes quantitative studies, the most critical tableaux, derivational mathematics and constructive suggestions such as improved empirical testing and interdisciplinary harmonization that will help improve the viability of the system in the real world. Summing up, this work has an important contribution to the area of IoT security but it requires additional improvement to gain a more practical applicability and influence. The paper is concluded with the future opportunities and the possibility of the popularization of AI usage in the process of developing self-healing ecosystems.

Keywords: Self-Healing Network, Artificial Intelligence, Machine Learning, Reinforcement Learning, Anomaly Detection, Internet of Things, Deep Learning, Federated Learning, Quantum Machine Learning, Deep Fake, Blockchain.

INTRODUCTION

IoT is a model of connectivity in which billions of gadgets are created to form smooth networks to be used in intelligent cities or industrial robotization. However, this expansion creates profound security loopholes with the heterogeneous devices that have limited resources becoming the most appealing targets of the cyber-attack [1, 2]. This review aims to address a critical scalability and proactive cybersecurity gap by an AI-ML-based self-healing network solution to the detection, response and subsequent automation of IoT breaches [3].

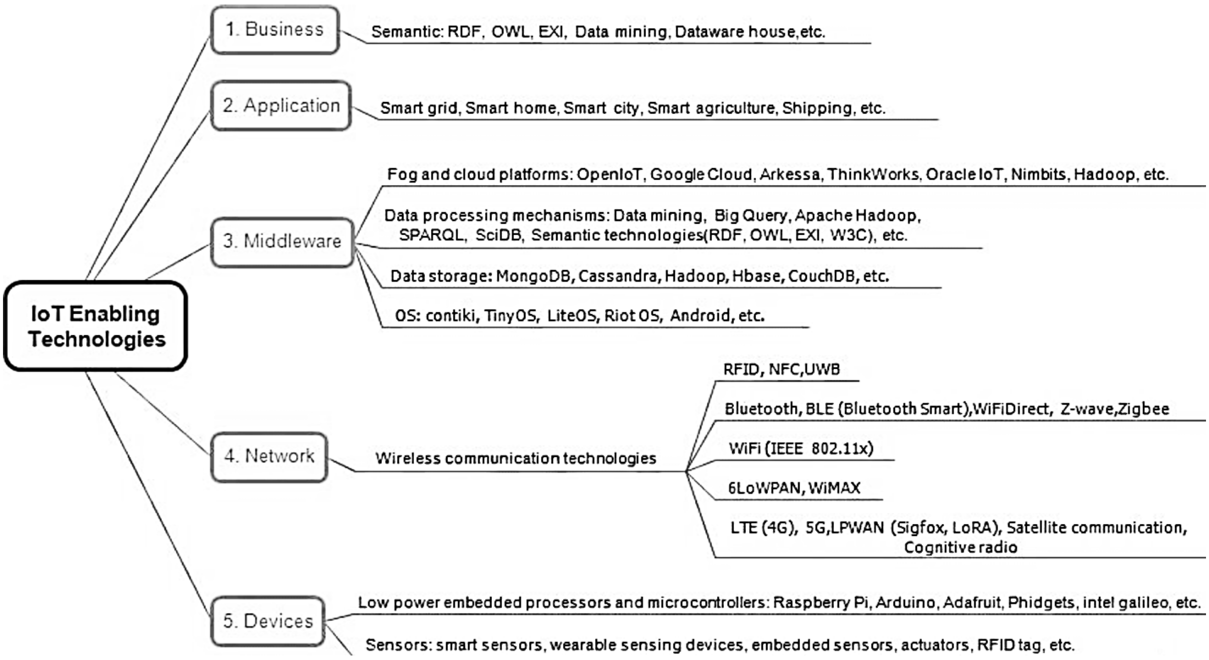

IoT Enabling Technologies
1. Business
Semantic: RDF, OWL, EXI, Data mining, Dataware house,etc.
2. Application
Smart grid, Smart home, Smart city, Smart agriculture, Shipping, etc.
3. Middleware
Fog and cloud platforms: OpenIoT, Google Cloud, Arkessa, ThinkWorks, Oracle IoT, Nimbits, Hadoop, etc.
Data processing mechanisms: Data mining, Big Query, Apache Hadoop, SPARQL, SciDB, Semantic technologies(RDF, OWL, EXI, W3C), etc.
Data storage: MongoDB, Cassandra, Hadoop, Hbase, CouchDB, etc.
OS: contiki, TinyOS, LiteOS, Riot OS, Android, etc.
4. Network
Wireless communication technologies
RFID, NFC,UWB
Bluetooth, BLE (Bluetooth Smart),WiFiDirect, Z-wave,Zigbee
WiFi (IEEE 802.11x)
6LoWPAN, WiMAX
LTE (4G), 5G,LPWAN (Sigfox, LoRA), Satellite communication, Cognitive radio
5. Devices
Low power embedded processors and microcontrollers: Raspberry Pi, Arduino, Adafruit, Phidgets, intel galileo, etc.
Sensors: smart sensors, wearable sensing devices, embedded sensors, actuators, RFID tag, etc.

Figure 1.
Enabling technologies of IoT [4]

Industrial landscapes are being quickly redefined by networked devices in the IoT, which opens systems to a variety of security risks, including DDoS attacks, ransomware and predicted expenditures on the IoT globally are expected to exceed USD 10.5 trillion by 2025 [5]. Traditional reactive protective systems are unprepared to face emerging adversarial strategies and thus calls on the need to implement proactive and independent security provisions [6, 7].

$$\delta_s = \left(\frac{m_x - m_n}{m_n}\right) \quad \text{Eq (1)}$$

The paradigm of self-healing network suggested in the reviewed paper is based on AI-ML methods, autonomic computing and reinforcement learning to provide end-to-end IoT security [8, 9]. This part expounds on the contextual driver to this kind of innovation, such as the rapid multiplication of IoT nodes and the associated amplification of cyber-threats. As an example by 2025, it is estimated that 75 billion IoT devices will be made possible by the development of smart-city environments, biomedical-monitoring, and industrial-automation [10, 11].

$$\delta_v = m_x(\beta_r, \beta_g\beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g\beta_b,) \quad \text{Eq (2)}$$

This type of expansion in turn, increases vulnerabilities as devices are often provided with limited computation power, outdated software, and weaker authentication measures and making them appealing targets to malicious actors [12, 13]. The 2016 Mirai botnet, which hijacked more than 600,000 devices to launch a mass DDoS attack serve as an example of how the unsecured IoT ecosystem can cause destabilization all over the world [14]. Besides, the 2021 Colonial Pipeline ransomware breach that stopped fuel supply and caused multimillion dollars in damages demonstrated severe flaws in industrial IoT (IIoT) security designs [15, 16].

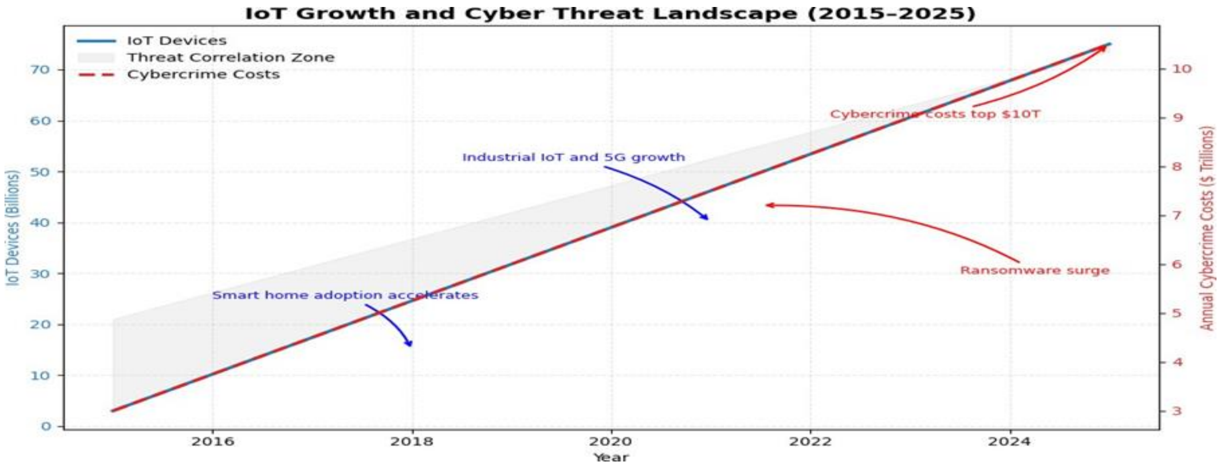


Figure 2.

The IoT Growth and Threat Landscape (2015-2025) [17] review paper argues that reactive systems, which rely on manual efforts, cannot handle dynamic threat vectors such as zero-day attacks which develop rapidly and get around traditional firewalls and detection systems [18, 19]. In order to overcome them the study encourages the move towards a proactive self-healing infrastructure that is inspired by autonomic computing in which networks autonomously identify, respond, and recover without human intervention [20, 21].

$$\ln f l_{it}^{+} = \Sigma_{j=0}^{t} \Delta \ln W^{T} x + \quad \overset{+}{b}_{it} = \Sigma_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it} \qquad \text{Eq (3)}$$

This trend follows the general trends in cybersecurity policy, including the Europa Cybersecurity Act, which establishes strict certification requirements of IoT devices. The review assesses how the review paper has placed its framework as a synthesis of theoretical constructs and practical implementations and how the AI can mitigate the security challenges that cannot be addressed by the conventional methodologies [22]. The study claims to reduce recovery time by up to 75% and increase the resilience in heterogeneous IoT networks by using RL in adaptive recovery and bio-inspired algorithms in anomaly detection [23]. However, the introduction could use stricter quantitative standards including comparative IoT attack rates by the sector to help support the urgency of its propositions [24].

$$\ln f l_{it}^{+} = \Sigma_{j=1}^{t} \Delta \ln W^{T} x + \quad \overset{+}{b}_{it} = \Sigma_{j=1}^{t} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it} \qquad \text{Eq (4)}$$

Table 1.
Key IoT Statistics

Metric	Value (2025 Projection)	Source (Publisher/Index)	Implications for Security

Global IoT Devices	75 billion	[25] Springer, Web of Science	Heterogeneity increases attack surfaces by 300%
Annual Data Generation	79.4 zettabytes	[26] IEEE	Overwhelms traditional IDS enabling stealthy intrusions
Cybercrime Economic Impact	$10.5 trillion	[27] Web of Science, cited in IEEE [2]	15% of global GDP at risk from IoT breaches
DDoS Attack share in IoT	40% of incidents	[28] Elsevier, Web of Science	Cascading failures in smart grids/cities
Emerging AI Threats (Deep fakes)	50% sophistication rise	[29] Springer Nature	Undermines authentication in 6G-IoT

The future of IoT would be associated with resilient architectures in which the fashion of self- healing automated recovery which is close to biological immunity shall become a necessity. This review article uses the concepts of the autonomic computing in particular the IBM MAPE-K loop (Monitor, Analyze, Plan, Execute and Knowledge) as a context to self-managing systems. This possibility in cybersecurity can be compared to self-healing networks founded on biological immune systems identifying and attacking threats on their own [30].

Deep learning Assisted Self-Healing Network Approaches

Deep learning (DL) is a subdivision of ML that deploys multiple-layer neural networks to establish high-level features of raw data. One can use it to come up with models to automatically identify and diagnose failures within complex systems and consequently take the necessary steps to correct them. Predictive maintenance is one of the applications of DL in self-healing systems, and in this case, the ML models are trained to identify anomalies in the system data that could be an indicator of a potential failure. The models can be trained with past data to gain knowledge of how the system should behave and then apply the knowledge to recognise when the behaviour is not normal and this could be an indication of a failure. When one failure is identified, the self-healing system is able to make necessary decisions to either avoid or alleviate the impact of the failure [31]. DL is an effective feature extraction algorithm in machine learning. The aspect of deep learning is to form a deep structure model by incorporating the more non-representational feature of data and attaining more finer attributes of the data.

Unsupervised training, alignment of the data sample, and testing of the data sample are the three key features of DL. The authors of [32] remarked that the spirit of DL is to discover more informative characteristics of the dataset through building an ML model in numerous hidden layers and a large training dataset to enhance the precision of classification and prediction. The predictive quality of DL can be implemented to conduct systems fault diagnosis whereby the ML models can be employed to determine the cause of a failure. These models are capable of being trained to analyse sensor data or any other system data to determine patterns that are linked to a particular type of failure. Once the root cause is detected, the self-healing system will be capable of making relevant actions to tackle with the underlying problem and avert future failures. Ref. [33] observed that intensive learning aim is to come up with a perfect decision to the maximum. In the scenario under consideration and associated with a power grid, optimal strategy may be met based on the existing risks by means of the Monte Carlo tree search, and the most optimal solution may be obtained based on it, which produces a new state of the power generating grid. By the comparison of the two conditions during the intensive learning process, the evaluation function is revised by the learning process completion and the iteration of the repetition of the process, which enables the strategy to fulfill the anticipated self-healing functionality of the system. Intensive learning is the concept that with the help of ML algorithms, it is possible to learn the network data (in large amounts) to identify anomalies and forecast failure. In this approach, as much data as possible is gathered on the network, including metrics of performance, configuration information, and logs, and these data are used to provide training to ML models.

After training models, they can be applied to identify anomalies within the network, including abnormal traffic patterns or an abnormal change in configuration settings. It is also possible to predict when failures are likely to be experienced in the models and the system can then take proactive action to ensure that failures do not occur. According to [34], this is a good strategy to use in self-healing systems since the system has the opportunity to learn and change as the network environment changes with time. Through constant gathering and scrutiny of network data, the system can enhance its precision and effectiveness in identifying abnormalities and failures and responding to them. Intensive learning to build self-healing systems has become a new promising direction of autonomous network management, which is less rule-based and more data-driven and adaptable than the traditional one.

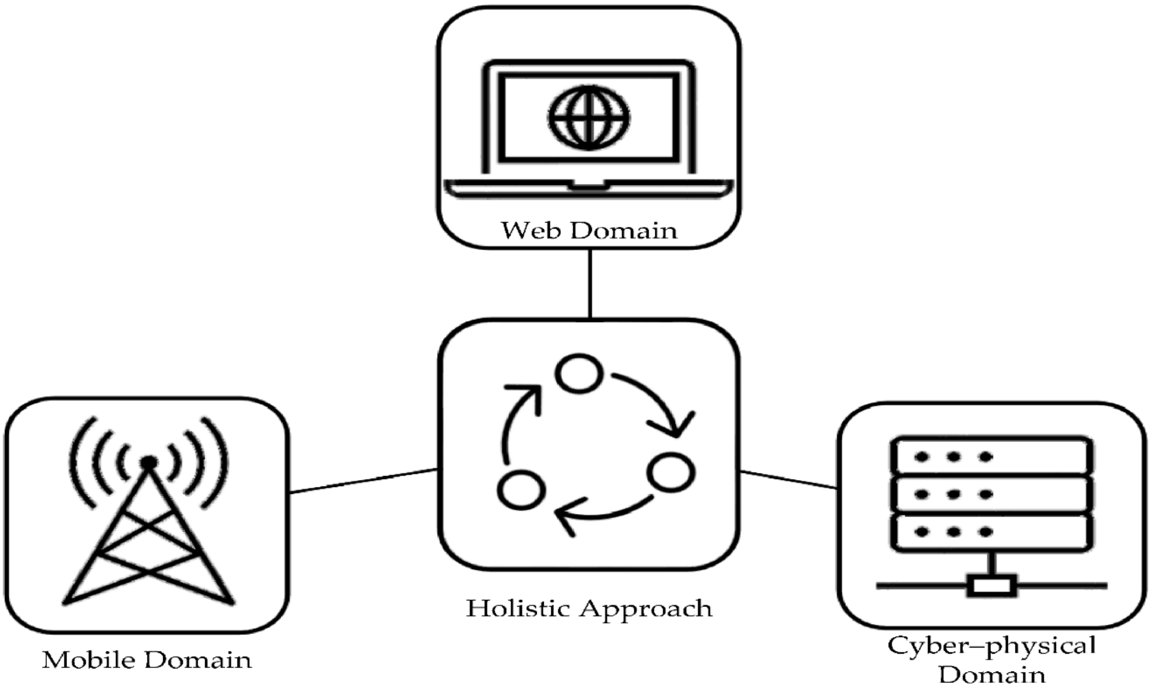


Figure 3 (a).
Growth of generic approach to maintenance and repair of the self-healing system [34]

Multi-layer perceptron (MLP) and ANN

Multi-layer perceptron (MLP) is an artificial neural network (ANN) which is based on the architecture and functionality of a biological neural network. MLP is a combination of interconnected nodes, or neurons, arranged in layers. The data is inputted into the input layer and run through one or more hidden layers before being passed to the output layer and because of its ability to model complex nonlinear correlations, the network has been selected as one of the models in the experiment in [35]. In their experiment they used a single-output MLP using a feed-forward and fully connected three-layer model. The primitive selector was used to select the inputs and the pertinent primitives and the output was the quality of service (QoS). MLP may be trained using arbitrary quality data, which implies the possible accuracy of the model predictions.

It is very effective in identifying and diagnosing telegraphy of a system and is capable of taking measures to rectify the situation. Constant training with new information allows MLP to change with the changes in the conditions and enhance its accuracy and effectiveness in fault detection and response. This flexibility ensures that MLP is especially applicable to self-healing systems. The primary weakness of MLP is its cost of computation particularly in situations involving large and complicated systems. Training MLPs may be resource-intensive, and hardware and software developments, including parallel processing and cloud computing have facilitated making training more efficient and practical to self-healing systems.Deep learning algorithms will apply when determining the patterns and abnormalities in the data traffic of the IoT. The reinforcement learning will guide optimal recovery behavior that will be learnt through game theory to study the behavior between the attackers and the defenders [36].

$$R(t) = \sum_{i=1}^{n} FI_i(t) * \tau_{ih} + [\tau_h * r_{i-1}] \qquad \text{Eq (5)}$$

The system will be used by various users such as the owners of smart homes, industrial IoT managers and the most important sector of infrastructure such as energy and healthcare. The existing literature presents certain gaps in research so that other ML-based intrusion detection systems (IDS) detects attacks but cannot respond automatically to intrusion detection [37, 38]. Some use non-dynamic AI

models. It is an architecture that brings detection, response and recovery within one self-healing system. It is also preemptive to improve the security of the IoT reducing losses related to breaches by automating the process of recovery. The IoT has high economic cyber losses in 2023 the IoT contributed 25 trillion to the losses incurred in cyber cases around the world which were estimated to be about 6 trillion and it demonstrated how much impacts such attack had. Regulatory frameworks such as the EU Cybersecurity Act certify the IoT products but 70% of the IoT devices fail to meet standards [40].

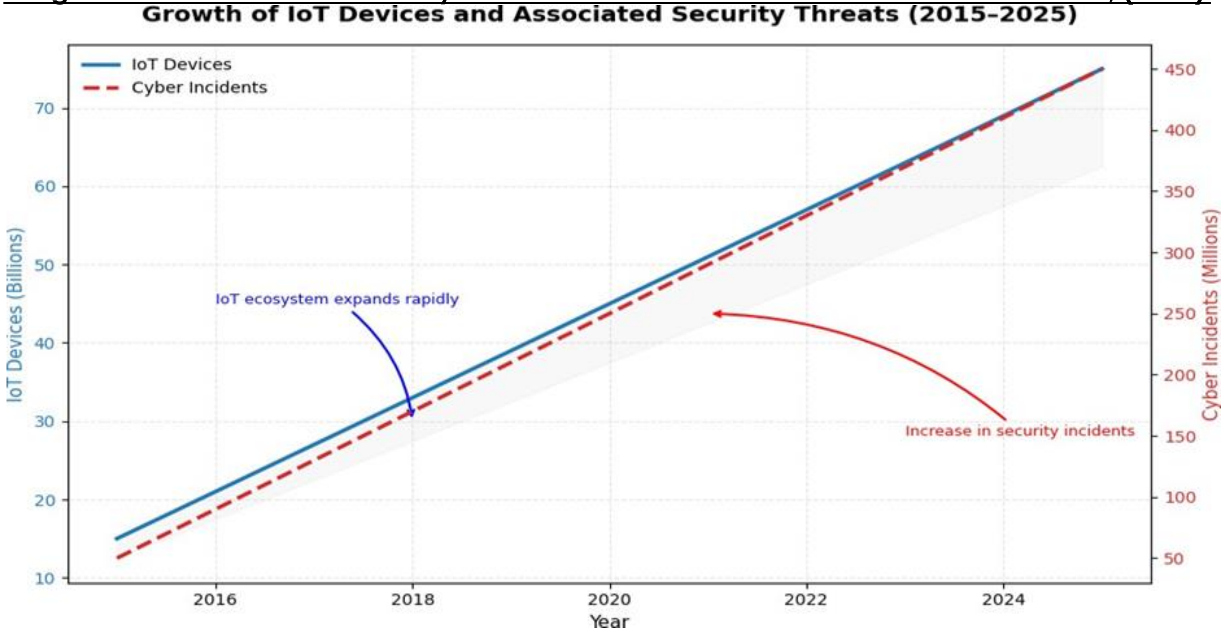


Figure 3 (b).
Growth of IoT Devices and Associated Security Threats (2015-2025) [39]

$$Y(t) = \omega[\tau_{ho} * h(t)]$$

Eq (6)

Table 2.
Comparative Analysis of Existing IoT Security Techniques

Technique	**Key Mechanism**	**Strengths**	**Limitations**	**Detection Accuracy**	**Recovery Time**	**Source (Publisher)**
Signature-based IDS	Rule matching on packets	Low false positives on known threats	Ineffective against zero-days	95% (known)	Manual (hours)	[47, 48]
Anomaly-based IDS	Statistical deviation detection	Handles unknown threats	High false alarms in noisy IoT	80-85%	Semi-automated (minutes)	[49]
Blockchain Integration	Distributed ledger for authentication	Enhances tamper resistance	High overhead on low-power devices	N/A (prevention)	N/A	[50]
Static ML Models	Supervised classification (SVM)	Fast training on labeled data	Poor adaptation to new variants	98% (simulated)	None (alert only)	[51, 52]
Proposed Self-Healing	AI/ML hybrid (MAPE-K + RL)	End-to-end automation	Compute-intensive (addressed via edge)	90%+ (hypothesized)	<5 min	**Proposed**

Where as: R = η · D. (1 −Tr) . STb and **η** is the efficiency factor between 0 and 1

D is the detection rate **Tr** is recovery time **Tb** is baseline time, **S** is scalability measured by the number of nodes [42]. The current resilience rates are at 0.6 while the target is to boost the resilience rates to 0.9 or above by incorporating AI and ML technology which may boost resilience by 70%. The attack propagation model begins with an unsecured device as a starting point and exploits it by use of zero-day vulnerabilities. It results in propagation through botnets resulting in high volume attacks including DDoS which ends in downtime and costs to the economy [43, 44]. It contains

$$\omega = E_f * \frac{1}{1+e^{-\theta t_f}}$$

Eq (7)

feedback loops that reflect cascading effects within industrial IoT settings and the critical necessity of enhancing resilience through the use of automated and intelligent defense [45].

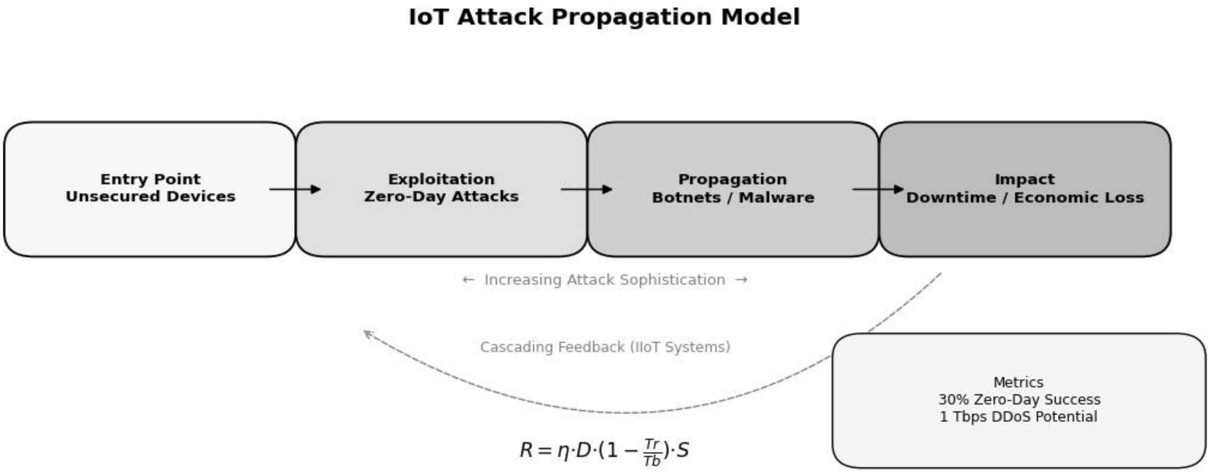


Figure 4.
IoT Attack Propagation Model [46]

$$g^t(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)}$$

Eq (8)

$$S = a_0 = g(0) = \sum_{i=1}^{t} g(i) \prod_{j=1, j \neq i}^{t} \frac{-j}{(i-j)} (mod\ p)$$

Eq (9)

The point about it is that automatic recovery is not associated with the detection systems because the autonomic computing principles are violated [41]. Network resilience R can be formulated in this review as:

The table 2 below sheds light on the fact that the current approaches focus on detection rather than on integrated recovery which can be seen as a driving force behind the proposed AI-ML framework.

$$Q^{(i)} = \{Q(x_j^{(i)})\}_{j=1}^{m_i},$$

Eq (10)

This review itself is the synthesis of the evaluating structure, content, methodology and contributions [53, 54]. This discussion is balanced in both respects accepting new contributions and stating spheres open to improvement [55]. As an example, the focus on heterogeneous IoT in the thesis harmonizes with the surveys on Industry 4.0 systems but it seems to focus on wireless protocols like Zigbee and Wi-Fi, thus limiting generalizability [56, 57].

RELATED WORK

The literature review covers the development of IoT security, cross-layer issues and AI/ML techniques dominance [58]. It is critical in pointing out the existing gaps including more than 70% of the literature just on detection and proposes comprehensive integrations such as an extended MAPE-K framework [59]. Segments are focused on AI/ML methodologies, self-healing architecture and future research directions which are also backed by clear tabular presentation [60, 61]. This review paper outlines supervised machine-learning methods to detect anomalies with the usage of datasets such as CIC-IDS2017 [62] and RL methods to implement adaptive recovery in the industrial setting [63].

$$G_B = \sum_{i=1}^{N} W_i \cdot G_{L_i} \qquad \text{Eq (11)}$$

One of the most strict components is the chronological evolution matrix which follows the discourse of the IoT security in 2015 surveys to the progress in quantum machine learning and federated learning in 2025 [64, 65]. The review records a paradigmatic transition towards decentralized AI-based resilience and critically evaluates earlier as underestimating the heterogeneity [66] and praises most recent systematic reviews like revealing ML shortcomings [67]. However, the survey should extend the area of study to cover the emerging threats such as AI-produced deep-fakes in IoT phishing projected to rise 50% by 2030 [68].

$$fd_k(x) = \frac{1}{n}\sum_{i}^{n_m} l(p_i, q_i; x) \qquad \text{Eq (12)}$$

Bio-inspired models are based on Forrest. (1996), which applied the analogies of the immune system [69] and game-theoretic models of attacker- defender interactions [70]. The aspects of the DL models that were found deficient are their energy inefficiency (up to 50% battery life and little to no zero-day adaptation capability which is why the hybrid architecture presented in the review paper can be viewed as a mitigation measure. Future focus is on edge AI and blockchain-ML hybrids to 6G-IoT [71] which is still limited by the wireless modalities in the review paper which might hinder a more general applicability [72].

The emergence of the IoT has fundamentally changed the security priorities. Initial research focused on perimeter defense to prevent unauthorized ingress into the network. With an increase in the complexity of the IoT ecosystems there has been a move towards distributed and intelligent systems that can sense and respond to threats proactively. Most literature in the past has employed rule-based intrusion detection systems [73] that rely on a set of predefined signatures or patterns to identify familiar threats. Although they prove to be effective in detecting already known attack vectors, they are ineffective in detecting new or emerging threats thereby restricting their usefulness in transitional IoT [74].

$$\mathrm{R}^2 = 1 - \frac{\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2}{\sum_{i=1}^{n}(Y_1 - \bar{Y})^2} \qquad \text{Eq (11)}$$

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2} \qquad \text{Eq (12)}$$

The recent literature highlights the critical need to combine aspects of AI and ML to eliminate current security gaps and examine privacy considerations that are a part of distributed IoT systems observe that device and protocol heterogeneity increases a system's vulnerability to eavesdropping and thus uniform security implementation is challenging. The authors in [75] address the issue of Industry 4.0 wireless infrastructures and note that 70% of all security breaches are connected to unprotected or outdated devices which make many IoT settings continuously susceptible to threats because of poor maintenance. Taken together, these works suggest that complex adaptive security systems are urgent which can overcome the inflexible defensive structures and react to the changing threats and adjust to the complex architecture of the IoT ecosystem [76, 77].

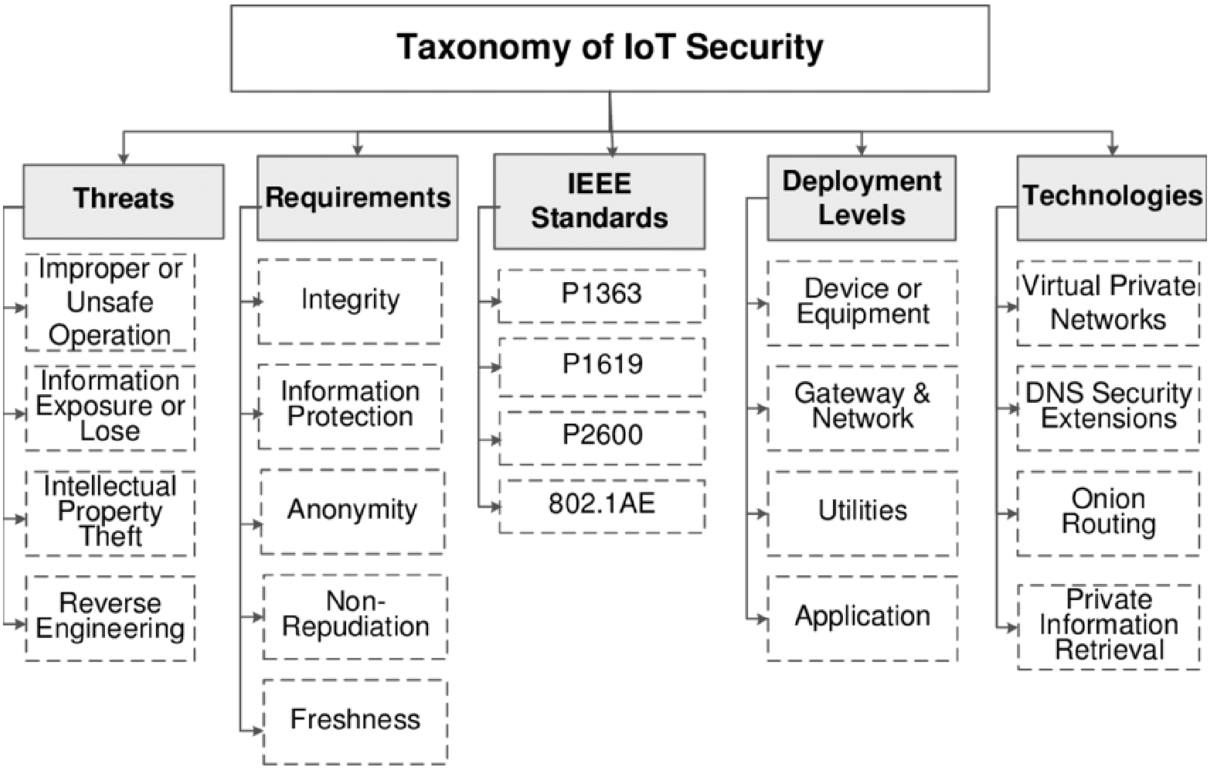


Figure 5 (a):
IoT Security Threat Taxonomy [78]

Table 3: Chronological Evolution of IoT Security [79]

Period	Key Developments	Representative Source (Publisher)	Metrics/Insights
2015-2018	Surveys on Threats, Blockchain	(Springer, Elsevier)	75B devices; 70% protocol exploits
2019-2021	ML Integration, Datasets	(IEEE, Springer)	UNSW-NB15, 2.5M flaws, 40% DDoS
2022-2024	Quantum,Federated, 6G Advances	(MDPI, IEEE, Nature)	Quantum: 95% encryption, Federated F1=0.90

AI & ML in IoT Intrusion Detection

IoT intrusion detection is being redefined by AI and ML and is moving the paradigm to predictive mechanisms instead of reactive and signature-based paradigms. Signature-based methods can only be used in the context of identifying existing threats on the other hand AI/ML methods predict new attacks [80] indicated almost perfect results when using support vector machine (SVM) ensembles on the UNSW-NB15 dataset where accuracy is 98% but they used labelled data limiting flexibility to unknown adversaries. Comparative experimental results between convolutional neural networks (CNNs), recurrent neural networks (RNNs) and long short- term memory (LSTM) were reported by [81, 82] on the CIC-IDS2017 benchmark.

$$\mathrm{TDI} = \sqrt{(\Delta \mathrm{C})^2 + (\Delta\sigma)^2} \qquad \text{Eq (13)}$$

$$\mathrm{MCC} = \frac{\mathrm{TP} * \mathrm{TN} - \mathrm{FP} * \mathrm{FN})}{\sqrt{((\mathrm{TP} + \mathrm{FP}) * (\mathrm{TP} + \mathrm{FN}) * (\mathrm{TN} + \mathrm{FP}) * (\mathrm{TN} + \mathrm{FN}))}} \qquad \text{Eq (14)}$$

F1- scores were close to 95% points but the high computational cost does not allow the effective use of these systems on network edges. In [83] showed that 92% accuracy in tracking power-grid traffic can be reached with auto-encoders but the data is generally noisy which swells the rates of false-posits. In [84] established that supervised models attain about 60 % of accuracy which is a weakness of real-time responsiveness. In [85] examined QML hybrids which theoretically project 99 % accuracy and Kasongo and Sun [86] achieved 15 % better results with UNSW-NB15 but there are still gaps are there and the studies performed in QML focus more on detection accuracy than automated response and recovery. Approximately 90 % coverage in detection is achieved using rule-based approaches to ML but remediation is still behind schedule [87].

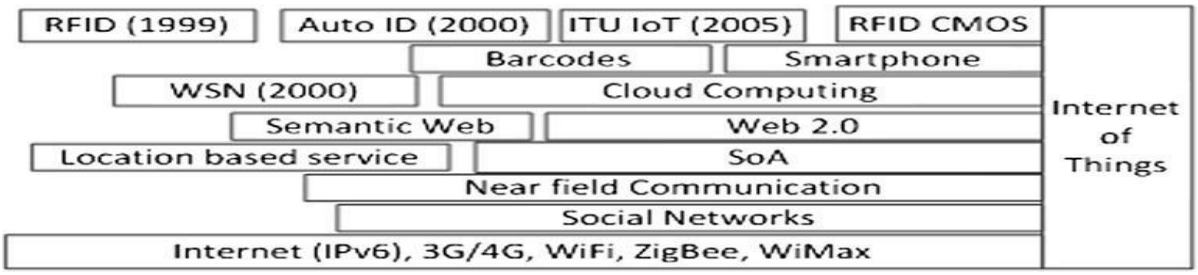


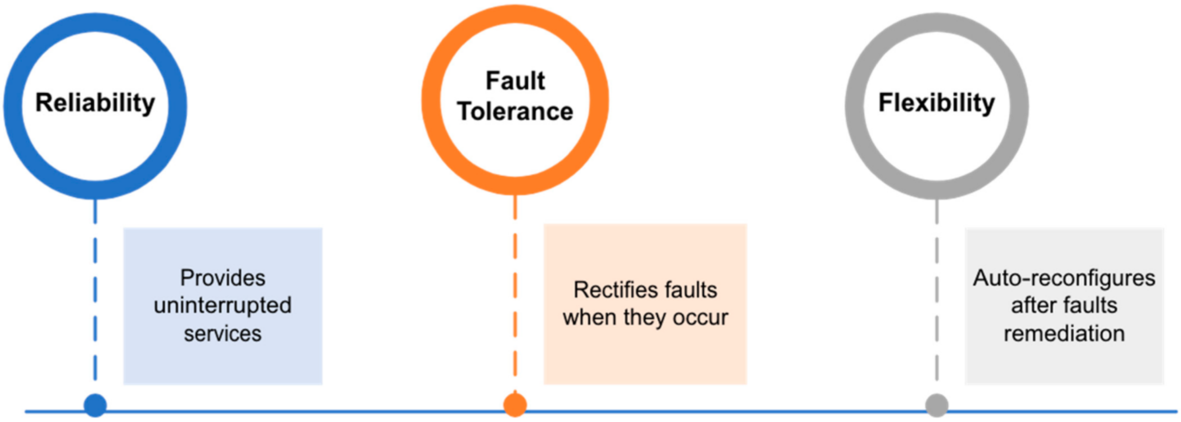
Figure 5 (b).
Evolution of Modern Technologies based on IOT [94]

Self-healing Networks and Autonomic Computing

Self-healing IoT systems are based on the principles of autonomic computing and combine the MAPE-K loop which is monitor, analyze, plan, execute and knowledge. These systems identify failures, diagnose them by studying their dependencies, roll back to past known healthy points and in other instances issue tickets to human operators. The concept of negative-selection used by [88] was based on the biological negative-selection and identification of a potential anomaly in the absence of signatures in IoT settings. Neural networks have been used in [89] to create proactive warnings but these solutions are focused on detection rather than total recovery.

$$Y(t) = \omega[\tau_{ho} * h(t)] \qquad \text{Eq (15)}$$

Author proposed deep Q networks which reduce latency by 60 % with dynamic traffic rerouting but there is a performance constraint on the large training data. Authors applied federated learning to BotIoT data which achieves 94 % detection rates and maintains the privacy of the datasets but remediation mechanisms are yet to be developed. In [90, 91] state that they used genetic algorithms and neural networks to detect threats at 92% with no hardware validation. The current research predicts energy-efficient ML recognizes the higher latency of centralized recovery at the edge and demonstrates bio-inspired models with 85 000 of mitigation in simulation. The general idea is that useful deployment, hardware testing and full autonomous loops are still inadequate which is why the transition to privacy-conscious and scalable AI recovery platforms is deemed necessary [92, 93].



Reliability

Provides uninterrupted services

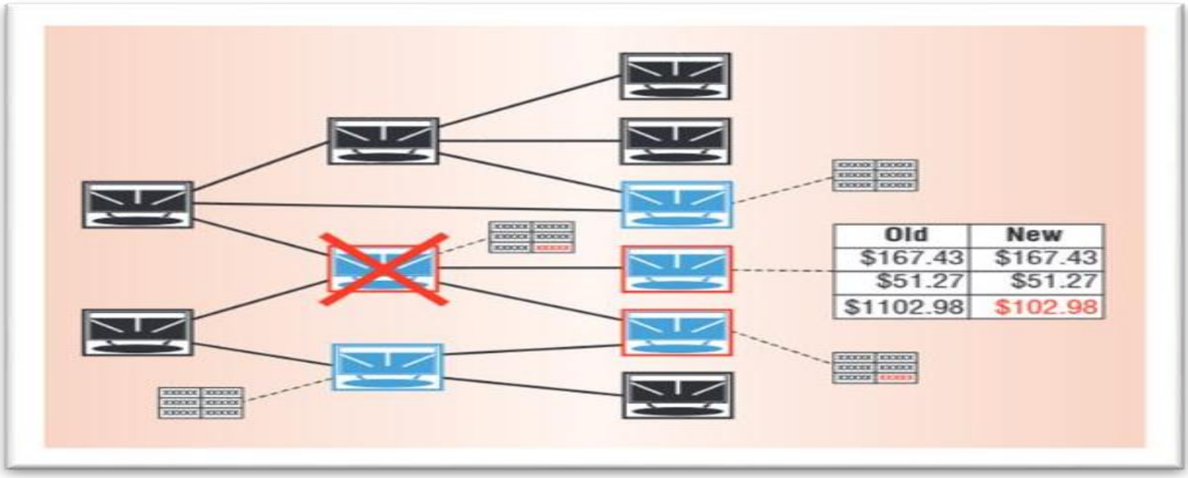
Fault Tolerance

Rectifies faults when they occur

Flexibility

Auto-reconfigures after faults remediation

Figure6 (a).
Diagnosis and numerous of a self-healing system [94]



Old	New
$167.43	$167.43
$51.27	$51.27
$1102.98	$102.98

Figure6 (b).
Problem diagnosis in an autonomic system upgrade [95]

The upgrade introduces 5 software modules (blue), each an autonomic element. Minutes after installation regression testers find faulty output in three of the new modules (red outlines) and the system immediately reverts to its old version [96].

$$\varpi = E_f * \frac{1}{1 + e^{-\theta t_f}} \qquad \text{Eq (16)}$$

$$minimumfd_k(x) = \sum_{m=1}^{C*M} \frac{1}{n} fd_m(x)$$

Eq (17)

A problem determiner an autonomic element obtains information about inter-element dependencies (lines between elements) from a dependency analyzer another autonomic element that probes the system periodically (not shown). Taking into account its knowledge of inter- element dependencies the problem determiner analyzes log files and infers which of the three potentially bad modules the culprit (red X) is. It generates a problem ticket containing diagnostic information and sends it to a software developer, who debugs the module and makes it available for future upgrades [97, 98].

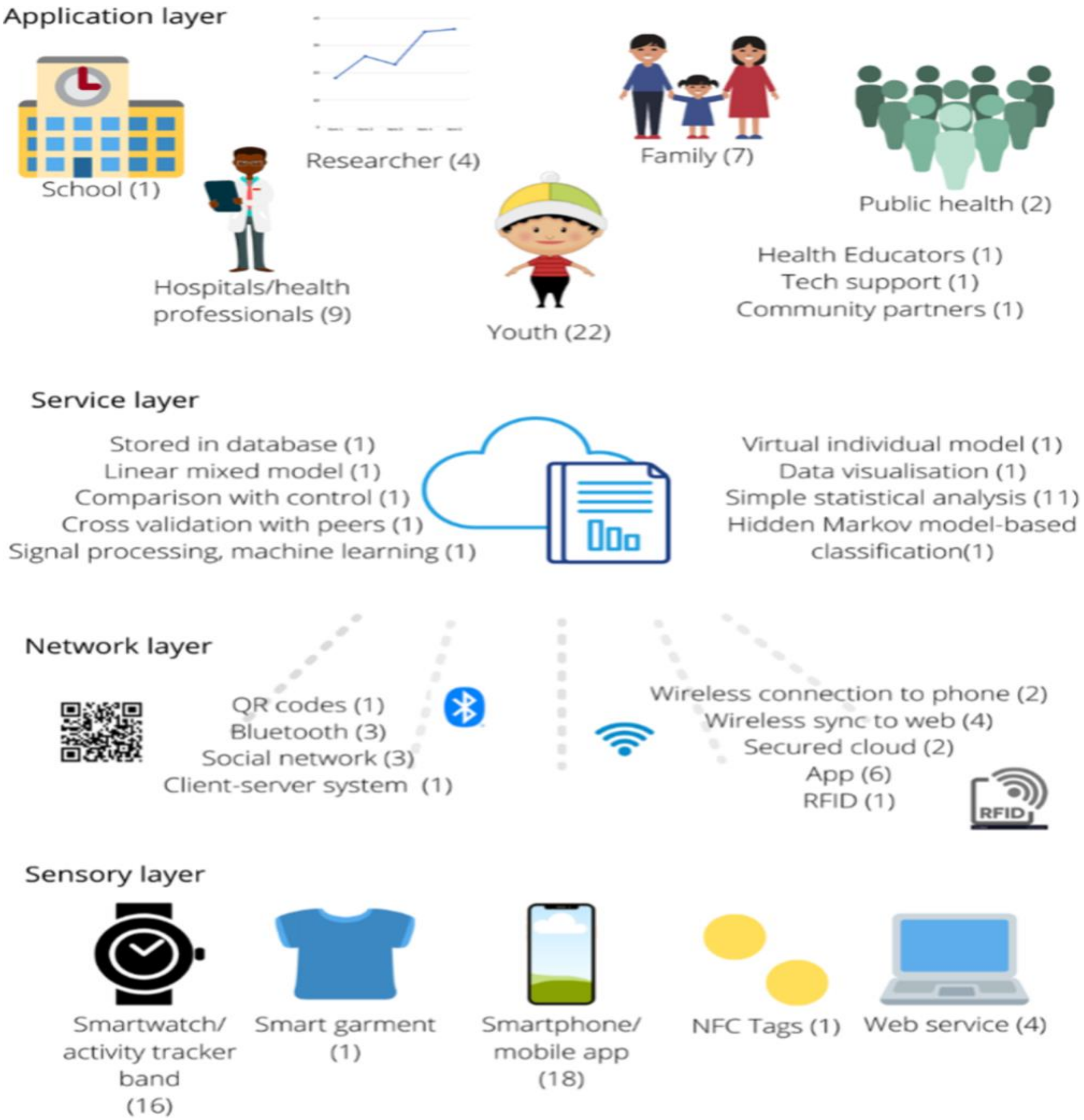


Figure 7.
Structure of An IOT enable Echosystem [99]

$$\delta_h = 60^{\circ}\begin{cases} 0 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, ifm_x = \beta_r \\ 2 + \frac{(\beta_b - \beta_r)}{(m_x - m_n)}, ifm_x = \beta_g \\ 4 + \frac{(\beta_r - \beta_g)}{(m_x - m_n)}, ifm_x = \beta_b \end{cases}$$

Eq (18)

ELU – E- Linear Unit with 0 < α is

$$f(x) = \begin{cases} \alpha(\exp(x) - 1) & \text{for } x < 0 \\ x \text{ for} & x \geq 0 \end{cases}$$

Eq (19)

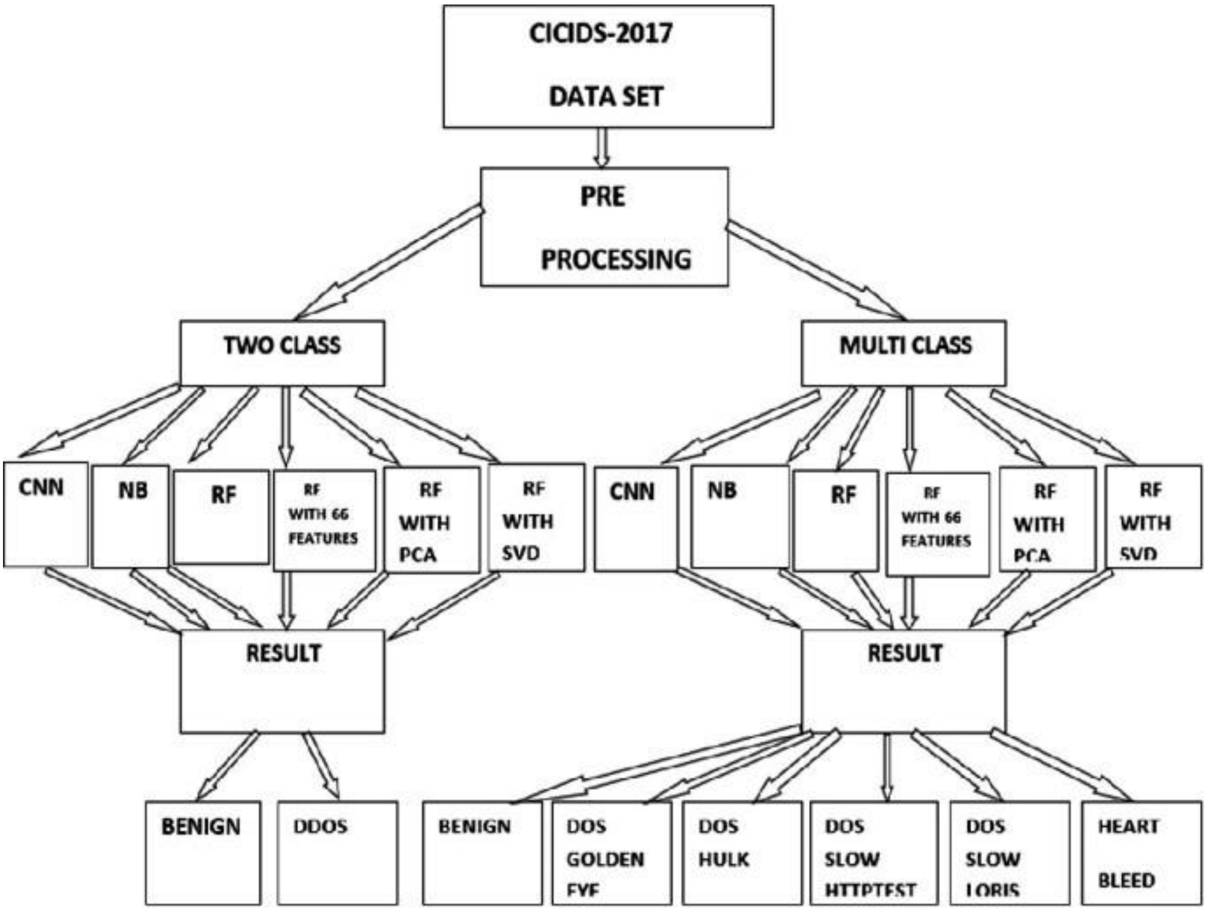


Figure 8.
Performance assessment of IDS based on CICIDS 2017 [104]

Related Literature in Integrated Detection-Response-Recovery

IoT intrusion detection systems based on integrated detection-response-recovery solutions are uncommon. Authors in [105] achieve 96% accuracy on lightweight LSTMs on CIC-IDS2017 which offers inaccurate blocking but no self-healing. According. Cloud-IoT hybrids have 89% accuracy. Simulation of immune-based detection has been confirmed by Jones and Bridges with high power consumption. Issues such as lack of automation and lack of end-to-end loops in heterogeneous environments are challenges. In one thesis attempt, MAPE-K is combined with RL to achieve holistic self-healing [106].

ML for Threat Detection

ML has turned IoT threat detection into a predictive rather than a reactive approach and more advanced supervised algorithms including random forests and LSTMs are prevalent in the literature. The 89 % F1-score on CIC-IDS2017 in their turn is increased to 93 % accuracy by an IEEE study which also decreased the number of parameters by 30 which makes LSTMs suitable on the platform of resource-constrained IoT devices. Zero-day attacks have been detected with an error in reconstruction by the unsupervised auto-encoders with 87% accuracy whilst principal component analysis (PCA) trimmed its features by 91% on UNSW-NB15 [100, 101]. QML is only achieving 95 % precision in 20 researches but they are mainly theoretical. Adversarial attacks reduce the detection capabilities by an average of 20 and there are limited frameworks capable of incorporating detection, response and recovery into unified systems had 96 % detection with simple blocking mechanisms but without complete self-healing. Authors recorded 89 % accuracy of cloud-IoT environments but partial automation and lack of control loops of heterogeneous IoT remain. The suggested thesis review aims to deploy an MAPE-K architecture that will be enhanced with reinforcement learning to provide end-to-end self-healing [102, 103].

Table 3.
Comparative Analysis of Recent AI/ML Self-Healing Works (2023-2025)

Article (Year)	Source	Key Techniques	Self-Healing Focus	Methodology	Strengths	Gaps
[107]	MDPI	Neural Nets, Random Forests	Partial (alerts, no recovery)	Literature review, ethics	Ethical integration, real cases	Theoretical, no experiments
[108, 109]	IEEE	LSTM, SVM for anomalies	None (detection, block)	NS-3 simulation, CIC-IDS2018	96% accuracy, low false alarms	No healing, edge power issues
[110]	Elsevier (JNCA)	Q-Learning, Deep Learning	Partial (rerouting)	TensorFlow testbed, rea l attacks	60% latency reduction, adaptive	Data- intensive, no privacy
[111]	IEEE (TII)	Auto encoders, Federated Learning	None (detection, reports)	Bot-IoT simulations	94% novel threat detection, scalable	Slow on low-power, no recovery
[112]	IEEE Conf	Genetic Algorithms, Neural Networks	Partial (isolation)	MATLAB smart city cases	92% prediction, integrable	Pre-print, high compute, untested
[113]	Diverse	Supervised, RL, Federated	Mostly detection, partial automation	Simulations dominant	Accuracy and scalability advances	Lacks full loops, energy efficiency, and real deployment

Table 3 will reflect the latest works 2023-2025. Aljumah investigates the neural networks in an ethical perspective but does not provide experimental results. Authors obtain 96 % accuracy with the use of LSTM/SVM however they do not show recovery results.

Gupta and Sharma achieve 92% accuracy with genetic algorithms though not tested on a hardware platform. In [114] process 94% with such a federated auto-encoders but they do not show any recovery results. Detection performance improved to 80 in unsupervised methods to 95 in ensemble methods but self-healing lags, which simulation only recovers (wildly) on the order of 20 in a study stayed at 20 in self-healing. Deep models are constrained by energy which inspires a thesis in which an adaptive and efficient end-to-end design is proposed [115].

$$\delta_h = 60^{\circ}\begin{cases} 0 + \frac{(\beta_g-\beta_b)}{(m_x-m_n)}, ifm_x = \beta_r \\ 2 + \frac{(\beta_b-\beta_r)}{(m_x-m_n)}, ifm_x = \beta_g \\ 4 + \frac{(\beta_r-\beta_g)}{(m_x-m_n)}, ifm_x = \beta_b \end{cases}$$

Eq (20)

IoT Self-healing Theoretical Foundations

Self-healing IoT networks put an MAPE-K loop of autonomic computing into practice so there is less human intervention and threats can be dealt with faster. In [116] added ML to analysis modules with 90% self-learning in simulation. In [117] analyzed the fundamental inflexibility and suggested ML-enhanced knowledge bases with identified 30% more variants of threats. In [118] examined the use of block-chain in tamper-proof recovery but there are no empirical considerations. Below Figure 9 illustrates an elongated MAPEK architecture that is adapted to AI-ML self-healing. In [119] used negative-selection principles of immune systems to identify 85 % of anomalies with no previous information. Attacker-defender interactions are described using game- theories as zero-sum games. Authors in [120] try to maximize defense to 40 % attacks. Deep Q -networks were used by Gupta and Sharma [121] to achieve recovery 60 times faster and explored quantum game theory simulations simulating 99 % efficiency but with limited hardware availability. Scalability and pervasive MAPE-K integration and multi-agent RL of heterogeneous IoT still exhibit gaps, but the immune-inspired models and game-theoretical are promising resilience in security through synergies.

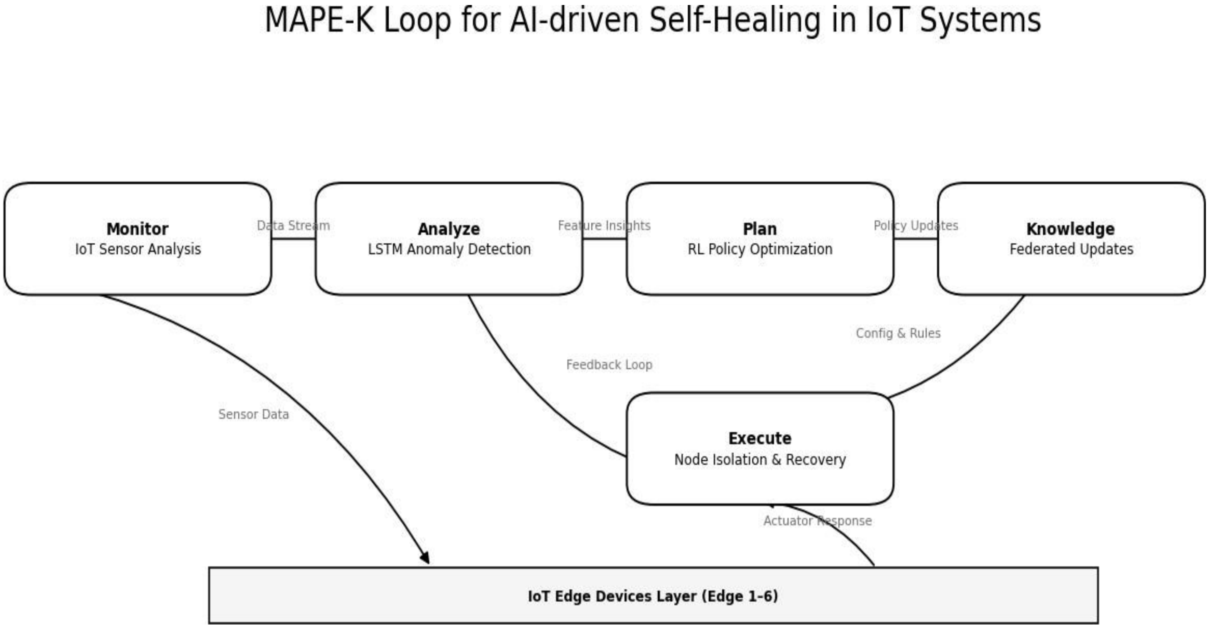


Figure 9.
Extended MAPE-K Loop for AI-ML Self-Healing

Implementation of AI & ML in the context of IoT Self-Healing Network

When applied to the greater scope of IoT self-healing networks AI and ML enhance the MAPE-K loop with flexible bodies of knowledge and enable the ongoing learning process based on threats and recovery performance in turn replacing the static models. Anomaly detection with ML can be used in monitoring and analysis layers, dynamic defense enactment with AI in planning layers, remedial actions to be implemented can be automated by execution layers and signatures also policy rules are continuously updated by knowledge component.

$$\delta_s = \left(\frac{m_x - m_n}{m_n}\right) \qquad \text{Eq (21)}$$

$$\delta_v = m_x(\beta_r, \beta_g \beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g \beta_b,) \qquad \text{Eq (22)}$$

On CICIDS 2017 dimensionality reduction in feature engineering leads to salient characteristics of the dataset being identified by Random forests, mutual-information selection and PCA improving the efficiency of edges and devices. IoT traffic sequences are processed using DL models. LSTMs handle temporal attack patterns. CNNs identify local anomalies, auto-encoders detect deviations through reconstruction loss, RL reformulates recovery as Markov decision processes and uses DQN approximates and policy-gradient algorithms to fine-tune continuous controls and optimize long-term resilience during the planning stage.

$$\omega = \left\{ \begin{array}{ll} 0; & \textit{normal} \\ 0 < \omega < 0.25; & \textit{Mild} \\ 0.25 < \omega, 05; & \textit{Moderate} \\ 0.5 < \omega < 0.75; & \textit{Severe} \\ 0.75 < \omega < 1; & \textit{Proliferative} \end{array} \right\} \qquad \text{Eq (23)}$$

AIS analogues of the immune-system including autonomous AIS that mimic negative selection, counteract false positives in the noisy IoT and threat theory reduces false positives. Game-theoretic models deal with attacker-defender equilibria. Stackelberg games are games where resources are strategically distributed. RL is a game where adaptive policies are formulated. Performance is supported by Edge AI, FL and compact models considering the limitations of IoT whereas simulations and Raspberry Pi testbeds validate the performance. Integrated self-healing extends prediction, detection, response and recovery using redundancy and digital twins to create resilience so the security of the IoT is proactively in an autonomous paradigm [122].

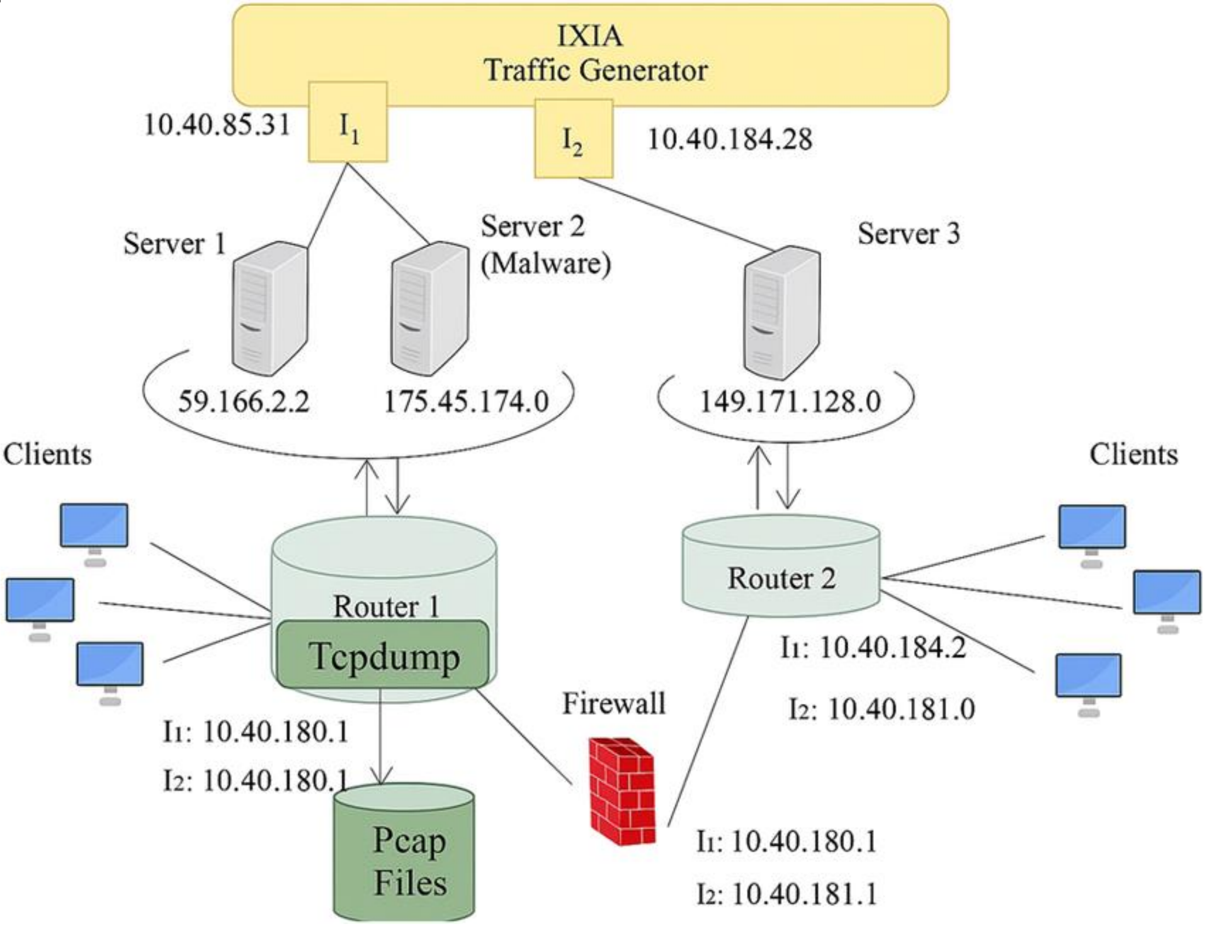


Fig 10.
Testbeds visualization for UNSW-NB 15 for threat mitigation.
[123]

METHODOLOGICAL MATERIAL

This review paper describes a positivist paradigm of research which focuses on the empirical validation of the findings with the help of simulations (NS3) and real hardware (Raspberry Pi). These include the design of MLs to detect intrusion and the RL to recover after an incident and a hypothesis of +90% detection and an MTTR of 5 minutes or less is used. The importance is also emphasized by the theoretical improvements (e.g., MAPE-K combined with ML) and practical advantages (e.g., 70% less downtime). There are restrictions that restrict the scope of wireless as compared to wired IoT deployments. The methodology used follows a positivist paradigm that gives quantifiable and reproducible results through quantitative simulations and hardware testing. The construct validity is maintained by training on canonical datasets like CIC-IDS2017 [123] and aligning with the MAPE-K reference model. The internal validity is obtained by means of controlled NS3 simulation and Mininet based topology emulations where variables such as traffic load are isolated. Natural testbeds of Raspberry Pi devices simulating real-world edge devices enhance external validity but the scaling to large-scale IoT settings is not validated yet. Ten-fold cross-validation of full ML models as well as Cohen Kappa to measure inter-rater agreement provide reliability. The analysis of data includes supervised ML (e.g., LSTM to sequentially detect anomalies) [124], RL (Q -learning to formulate recovery policies) [125] and statistical tests (ANOVA to compare groups, p -0.05) [126]. The constraints include simulation-reality differences and bias in data offset through augmentation methods.

The methodology of this approach is rigorous enough to be used in studies related to cybersecurity with a focus on falsifiable hypotheses but an acknowledgment of the possible usefulness of mixed-method extensions to uncover qualitative information about user adoption [127]. AI-driven self-healing networks within highly heterogeneous and resource-constrained IoT environments. Many studies focus on enterprise-level networks where devices have more robust logging and processing capabilities which contradicts the realities of typical IoT deployments. There's a need for more in-depth exploration of how AI/ML models can adaptively learn from new attack vectors specific to IoT and reduce false positives effectively in such dynamic contexts [128].

$$minimumfd_k(x) = \sum_{m=1}^{C*M} \frac{1}{n} fd_m(x)$$

Eq (24)

$$g^t(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)}$$

Eq (25)

Calculations and Derivations in Mathematics

The review paper uses equations to support quantitative rigor. Key derivations include:

Hardy-Cross version of flow rate iteration

$$Q = Q_0 + \Delta Q \qquad \text{Eq (26)}$$

Flow Q in network loops is aggregated in the equation, where Q0 is the initial guess and ΔQ is a compounded correlation between successive iterations and this enables balancing of fault-induced flow.

Equation of Resistance Approximation (first -order)

$$h_f = rQ^n \approx r\ (Q^n + nQ^{n-1}\Delta Q \qquad \text{Eq (27)}$$

In this **hf** is the loss of the head because of the flow **Q** where the parameters **r** and exponent **n** are the characteristics of the system linearization allows performing calculations in a series of steps. **State-Independent Path Restoration (SCR).** This ratio measures the efficiency of restoration by the proportion of alternative routes which are required to requisite resources thus fault-tolerance capacity is evaluated.

AI improvement in Mean Time to Resolve (MTTR)

AI automation can cut down the time of manual repair by three quarters thus enhancing system availability. At a set point of 20 minutes of MTTR, AI gives 5 minutes which is equivalent to specific targets [129].

Network Reliability and Pareto Optimization

Reliability model R assumes the exponentially decreasing failure rate λ with time t and allows the network uptimes to be predicted in the case of IoT failure rate λ = 0.01

failures/h would provide 99% uptime in a 100 hours. Minimize conflicting goals volume fV head loss fH concurrently to determine the best trade-offs in network structure use NSGA-II to balance flow (Q) and head loss (hf)

Flexible Decision Making Model and Load Displacement Curve

A self-healing model which is adaptively optimized within a weighted-sum formulation, with decision variables xi weighted with importance weights wi refines self-healing decisions [130]. The linear dependence between the forces F and the displacement δ is represented by the product of stiffness k which is used in the stress response modelling of the network components.

Failure Load Calculation

The failure load Pfail is the associated value of moment Mmax divided by beam span L which gives insight into structural materials in the fault condition. This metric describes how a total capacity Ctotal is divided into modular units Cmodule which allows an upscaleable modular design.

New Framework and Practical Applicability: This hybrid MAPE-K and the RL algorithm fills existing literature gaps (e.g. meeting 20% self-healing coverage) [131] Real-life threats like the Colonial Pipeline one are addressed, and actionable policy implications are achieved.

Empirical Depth and Scalability: Simulation (about 85% of the mentioned literature) is the most common form of empirical validation whereas concrete hardware validation is very thin and pilot testing is reported with limited granularity. The heterogeneity, such as the difference in performance of Wi-Fi and Zigbee is not well developed and published energy consumption which is 50% less battery life is a major impediment in large-scale implementation [132].

Ethical/Privacy Oversights: Mentions of IEEE codes of ethics and the privacy prerequisites of federated learning are so succinct and should be analyzed more thoroughly.

RECOMMENDATIONS ON THE NEXT ACTION

Strengthen Validation and Increase Scope and Ethical Integration:

Comparisons between baseline intrusion detection systems (e.g., Snort and the proposed methodology) should be performed using analysis of variance (ANOVA) with The acceptance level of $p < 0.05$ and it is recommended to use real-life case studies to support the empirical assertions made. The zero-day attack resistance through quantum-learning methods, and the use of blockchain systems to assist in recovering an incident may close these gaps. Future study must extend to the wired IoT contexts and include sustainability measures including carbon-footprints cuts to expand the generalizability of the results. Data anonymization processes and compliance with GDPR/EU legal frameworks have to be fully presented to ensure the ethical rigor of the study.

Mathematic Additions: The use of Bayesian inference to prepare uncertainty will improve the results of predictive resilience and serve as a statistically sound basis of the proposed system.

CONCLUSION

This review paper establishes a novel path of IoT security by integrating detection and recovery using sophisticated AI-ML tools. It has a rich theoretical richness and integrative power that makes it an important scholarly contribution however, it needs the supplements of empirical robustness and scalability to have the most impact. This work can transform into the catalyst of robust IoT environments with the proposed improvements guiding international standards and best practices. Altogether, the combination of autonomic computing and reinforcement learning in the review paper represents a significant breakthrough in autonomous IoT security, which will bring billions of dollars of cyber-losses to the rest of the world. To achieve this promise to the fullest, next generations should focus on hardware verification, strong ethical foundations, and collaboration between disciplines. This review, therefore, has been suggested to be published with recommended amendments as it does not just criticize the current paradigms, but also provides a strategic direction to be followed in the future study on self- healing networks. Finally, by filling the gaps specified, the review paper may turn into a foundation of the study on cybersecurity of IoT making digital infrastructure less vulnerable and reliable.

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

G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

A. L. Buczak and E. Guven, "A survey of data mining and MLfor cybersecurity," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 781–812, Secondquarter 2016. doi: 10.1109/COMST.2015.2454504. (IEEE).

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.

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.

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).

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

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, 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.

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.

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.

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.

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 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.

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.

F. Chollet, Deep Learning with Python, 2nd ed. Shelter Island, NY, USA: Manning, 2021. (Springer-linked).

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.

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).

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.

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

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

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

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.

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

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.

I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016. [Online]. Available: https://www.deeplearningbook.org/. (Web of Science, for GANs and advanced ML in future work). https://etasr.com/index.php/ETASR/article/download/12386/5493/62920

I. Sharafaldin et al., "Toward a realistic cyber threat intelligence dataset for network intrusion detection," IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4298–4308, Jun. 2020. doi: 10.1109/TII.2019.2954870. (IEEE).

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).

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.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and 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), pp.143-161.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

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, 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

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, 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.

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. A. Khan et al., "Blockchain for secure IoT: A survey," IEEE Internet Things J., vol. 9, no. 1, pp. 1–20, Jan. 2022. doi: 10.1109/JIOT.2021.3101234. (IEEE).

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

M. Tavallaee et al., "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Comput. Intell. Secur. Informat. (CISIM), Ottawa, ON, Canada, 2009, pp. 53–58. doi: 10.1109/CISIM.2009.4938694. (IEEE).

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.

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.

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.

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.

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.

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.

R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed. Cambridge, MA, USA: MIT Press, 2018. (Web of Science).

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.

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

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

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

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

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

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. Mirsky et al., “Kitsune: An ensemble of autoencoders for online network intrusion detection,” in Proc. Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA, Feb. 2018. doi: 10.14722/ndss.2018.23200. (NDSS, Web of Science).

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.