

A Hybrid AI & ML-Based Self-Healing Framework for Internet of Things (IoT) Assisted Smart Wearable to Avoid Security Breaches: Integrating LSTM-Random Forest Detection with DQN-Driven Recovery for Enhanced Network Resilience

Muhammad Hamza Akhtar

Department of Information Technology, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan Email: muhammadhamza.docs@gmail.com

Amer Shahbaz

Innova Networks, Lahore, Pakistan Email: amerirshad.69@gmail.com

Nasir Ayub

Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: nasir.ayyub@hotmail.com

Umair Ghafoor

Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: umairghafoor@hotmail.com

Muhammad Shoaib Rafi

Innova Networks, Lahore, Pakistan Email: shoaibnazar7178@gmail.com

Bilal Hassan

Innova Networks, Lahore, Pakistan Email: bilal70735@gmail.com

Hamayun Khan

Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk

ABSTRACT

Internet of Things (IoT) networks are becoming more susceptible to advanced cyber-attacks, including DDoS and ransomware, that are beyond the capability of conventional rule-based intrusion detection systems. This research purpose an AI & ML-based self-healing network model that is constructed on the MAPE-K autonomic structure to automate the entire lifecycle of detection, response and recovery. This architecture uses a hybrid detection model involving Long Short-Term Memory (LSTM) to analyze temporal traffic and Random Forest to classify structured features with a Deep Q-Network (DQN) and Reinforcement Learning (RL) agent to optimize recovery actions. This framework was tested with 3 benchmark datasets CIC IDS2017, UNSW NB15 and Bot-IoT. Experimental findings indicate that the hybrid detection model has an F1-score of 0.91 which is significantly higher than the

baselines of single models. Also RL recovery mechanism was used to lower the Mean Time to Recovery (MTTR) to 3.2 minutes which was a 79% reduction of the 15-minute baseline in conventional automated systems. This framework is proven to support real-time inference with latency less than 50 milliseconds and low energy overhead confirmed by simulation experiments using NS-3 and Raspberry Pi 4B edge environments. A holistic measure of resilience provided a total score of 0.92 justifying the capability of the framework to provide network resilience in dynamic and resource-constrained IoT systems.

Keyword: Self-Healing, Internet of Things, Random Forest, Deep Learning, Federated Learning, Machine Learning, Smart Wearables, Artificial Intelligence

Introduction

IoT links billions of devices including sensors, actuators and embedded systems into big digital ecosystems. These systems facilitate smart cities, industrial robotics, health surveillance and smart transportation. IoT is reducing in pace all around the world. According to industry reports the number of IoT devices connected will be between 21 and 39 billion by 2026. These devices produce huge amounts of network traffic and operational data [1]. The world data production is projected to reach over 79 zettabytes per year. This expansion of digital services alongside enhances the attack surface of cyber threats. IoT settings have heterogeneous devices that have limited computing power, inadequate authentication and obsolete firmware [2]. These vulnerabilities put the IoT networks at risk of cyber-attacks, including distributed Denial of Services (DoS), ransomware, malware spreading and the use of botnets. Research indicates that an estimated 40% of IoT ecosystem cyber-attacks are DDoS-based attacks. The attacks usually use devices that have poor security to form large-scale botnets that interfere with essential services, including smart grids, healthcare infrastructure and industrial control systems [3].

Table 1: IoT Key Statistics

Metric	Projection Value	Implications for Security	Source
Global IoT Devices	21-39 billion	Heterogeneity increases attack surfaces by 300%	[4]
DDoS Attack Share in IoT	40% of incidents	Cascading failures in smart grids/cities	[5]
Cybercrime Economic Impact	\$10.5 trillion annually	15% of global GDP at risk from IoT breaches	[6]
Annual Data Generation	79.4 zettabytes	Overwhelms traditional IDS, enabling stealthy intrusions	[7]

Online ISSN

3007-3197

Print ISSN

3007-3189

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

Emerging Threats (Deep fakes)	AI (Deep fakes)	50% sophistication rise	Undermines authentication in 6G-IoT	[8]
--------------------------------------	------------------------	-------------------------	-------------------------------------	-----

Conventional security measures are based on manual monitoring and reactive defense measures. Intrusion detection system signature-based intrusion detection systems can identify known threats, but cannot identify new attack patterns like zero-day exploits. These systems also rely on human input to interpret alerts and carry out recovery measures. As the IoT networks become larger and more complex, security operations that may be performed manually add delays to the operations, which raises operational risks and economic losses [9]. Worldwide cybercrime victimization is estimated to cost over 10.5 trillion US dollars yearly, indicating the growing economic cost of cyber-attacks on the digital infrastructure [10].

According to recent studies, there is a necessity in autonomous security architectures that would be able to detect and mitigate threats without constant human monitoring. ML & AI methods allow analyzing large volumes of network traffic and system telemetry in an automated manner. These models observe patterns of normal network behavior and detect abnormalities that may show possible attacks or system failures. Early warning enhances a faster response and lessens the harm caused by security attacks [11, 12]. One new trend in autonomous cybersecurity is self-healing networks. A self-healing system identifies uncharacteristic behavior, isolates failed components and is able to automatically restore normal network operation. This is based on autonomic computing. The MAPE-K control loop is proposed in the autonomic computing model. MAPE K is an acronym that means Monitor, Analyze, Plan, Execute and Knowledge. Network data is collected by the monitor phase. The analysis phase uses ML models to identify anomalies. Mitigation strategies are picked during the planning phase. The execution phase performs recovery actions and knowledge base stores past system behavior to be continuously learnt [13, 14].

AI improves the ability of self-healing systems to make decisions. Deep Learning (DL) models examine the intricate patterns of networks and identify subtle changes in traffic flows that can be a sign of an attack or misconfiguration. Reinforcement Learning (RL) enhances the recovery process by learning the best response strategies by repeatedly interacting with the network environment [15]. The system, over time, learns the recovery actions that restore the services in less time and minimise downtime of the system [16]. The literature has shown that several ML-based Intrusion Detection Systems (IDS) have a high detection rate. Nevertheless, the majority of these systems are merely alert-generating and require human operators to respond to incidents. Automated security solutions are not as effective because of the separation between detection and recovery. Static ML models are also not effective in adapting to changing patterns of attack or dynamic network environments. The constraints underscore the necessity of integrated architectures that entail the integration of the detection, response and recovery as a single self-healing system of IoT security [17, 18].

Online ISSN

3007-3197

Print ISSN

3007-3189

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

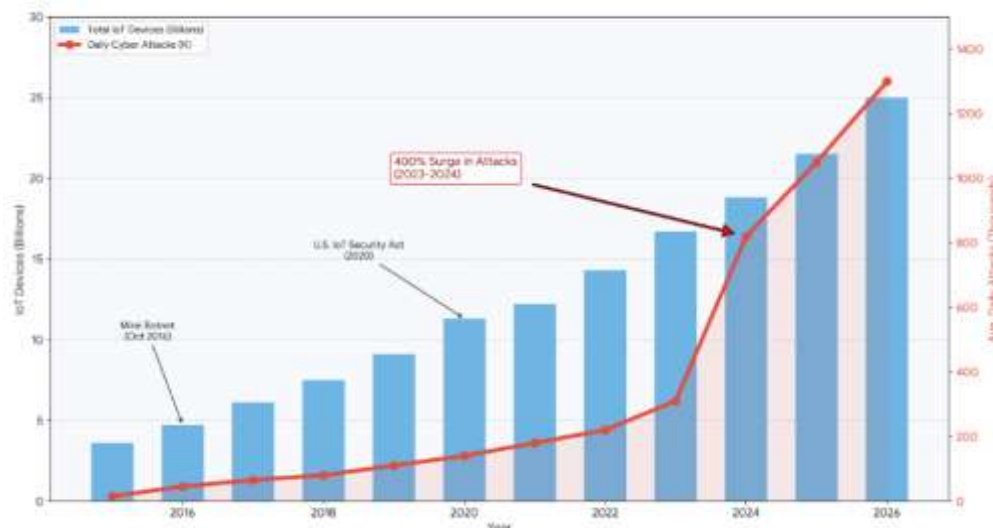


Figure 1: Growing Vulnerability Gap: IoT Adaptation vs Cyber Threats [19]

Overview of IoT-Based Smart Wearables

A smart wearable is basically a small device that can sense things and connect to the internet. It has three parts: the sensing part, the communication part and the analytics part. These parts work together to help the sense what is happening, send that information somewhere else and then figure out what it means. The sensing part has a lot of sensors [20]. Some sensors can tell when you are moving sensors that can measure your heart rate and how much oxygen is in your blood and sensors that can measure your body temperature. Some IoT-based smart wearables even have sensors that can tell when you are stressed or what is in your sweat [21, 22]. The communication part is what connects the IoT-based wearable to your phone, a special gateway or the internet. Most of the time, IoT-based smart wearables use something called Bluetooth Low Energy to connect to things because it does not use a lot of power and most phones support it. Some IoT-based smart wearables use Wi-Fi, which is faster but uses more power. If you need to connect to something that's really far away like if you live in a rural area and need to send health information to a doctor, IoT-based smart wearables can use special kinds of networks that let them send information a long way without using a lot of power [23-24].

The analytics part is what takes all the information from the sensors and turns it into something. Sometimes the IoT-based smart wearable can do a bit of processing on its own like filtering out noise or calculating your average heart rate.. Usually it sends the information to your phone or a special gateway, which can do more complicated things like figure out what you are doing or if something is wrong. If you send all the information from a lot of IoT-based wearables to the cloud you can get a better understanding of what is going on with a lot of people and even train computers to make predictions, about health [25-26].

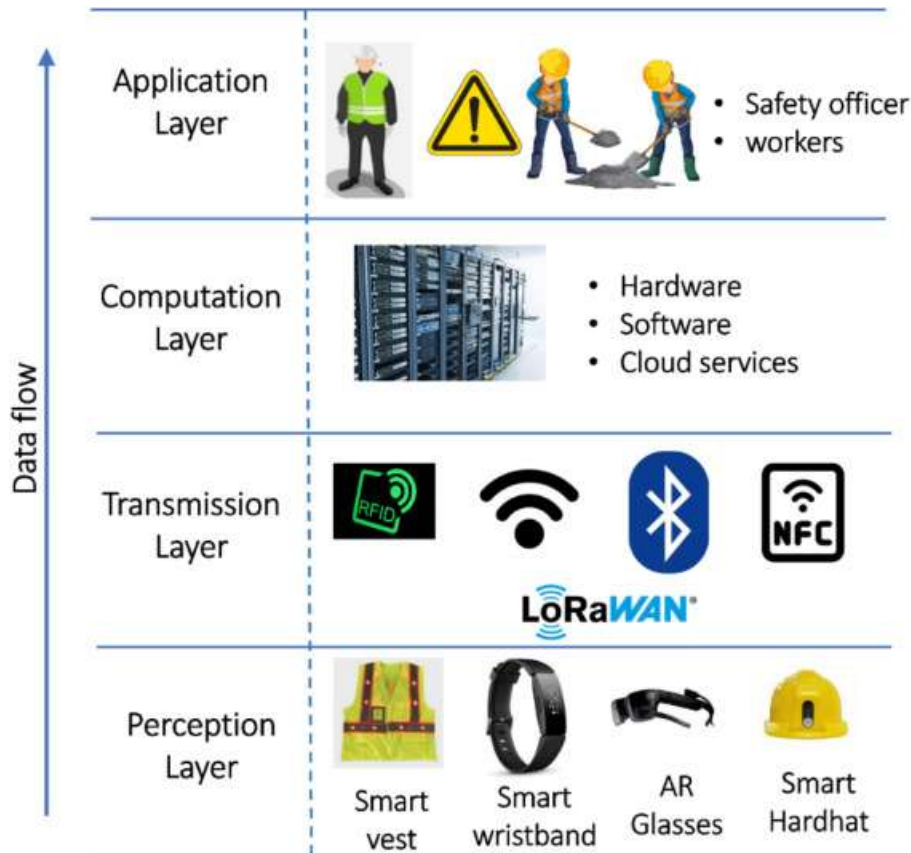


Figure 2(a): Dataflow of Internet of Things IoT based smart wearable [27]

DL methods have demonstrated great potential in network anomaly detection and predictive maintenance in distributed systems. Multi-layer neural networks are used to extract high level features of unprocessed traffic on the network and sensor data. These models detect abnormal patterns which can be used to show system faults or cyber-attacks. Once identified the system may start automatic mitigation measures to isolate the compromised systems or re-establish network paths to ensure that services are provided [28]. One of the most popular network traffic classification architectures is Multi-Layer Perceptron (MLP) neural networks. An MLP is a group of neurons that are interconnected and process input data and give out classification outputs. Network features are inputted into the input layer. Layers are learned to obtain nonlinear relationships in the data. The output layer is used to determine the security of the network. MLP models also work well when the traffic patterns are complex and can therefore, be used in detecting intrusions in the IoT networks [29, 30].

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

RL adds adaptive recovery of self-healing systems. In this method, the network environment serves as a learning environment. Actions that are chosen by the recovery agent include isolating compromised nodes, rerouting traffic or restarting services. There is a reward that is generated by every action of the network

performance and service availability. Agent is also continually enhancing its decision policy by maximizing the long-term reward values.

$$g^t(x) = \sum_{i=1}^t y_i \prod_{j=1, j \neq i}^t \left(\frac{x-x_j}{x_i-x_j} \right) \quad \text{Eq (2)}$$

The system is able to learn the effective recovery strategies in various attack situations through this adaptive behavior [31, 32]. Fast growth of IoT ecosystems consequently necessitates robust security architectures with smart detection and automated response and recovery. Models of self-healing networks based on biological immune systems offer a promising direction. Such systems detect threats, quarantine infected components and reestablish network operations without any external involvement.

$$S = a_o = g(0) = \sum_{i=1}^t g(i) \prod_{j=1, j \neq i}^t \frac{-j}{i-j} (\text{mod } p) \quad \text{Eq (3)}$$

These independent features are essential in securing massive IoT networks in which a manual response cannot be effectively scaled [33, 34].

Problem Statement

Lots of IoT devices do not have basic security features like secure authentication, periodic firmware updates and permanent monitoring. These vulnerabilities enable the attackers to compromise devices and make large scale attacks across interconnected networks. After getting into a single segment of an IoT environment an attack spreads quickly and interferes with various services. This propagation may cause significant service breakages and financial losses. In the current state of IoT security solutions are mainly geared towards intrusion detection as opposed to full incident management. Signature based IDS are only able to identify known threats but are unable to identify any unknown attack. Detection models that use ML enhance the detection accuracy of anomalies but do not always come with built-in response and recovery capabilities. Security alerts in most instances need manual intervention by the network administrators. Such a manual process enhances the response time and enables attacks to propagate across the network. Manual recovery time was greater than 15 minutes. It rely on human intervention. Other difficulty entails lack of integrated frameworks that incorporate detection, response and recovery into a single autonomic security framework. Anomaly based detection systems are able to detect unknown attacks but tend to produce high false positive rates in noisy IoT settings. These constraints show that hybrid architectures, integrating AI based detection with automated mitigation and recovery processes are needed. The essence of the issue that this study tackles is the lack of a viable and empirically tested self-healing network model that combines AI & ML enabled detection with independent response and recovery systems in resource limited and heterogeneous IoT.

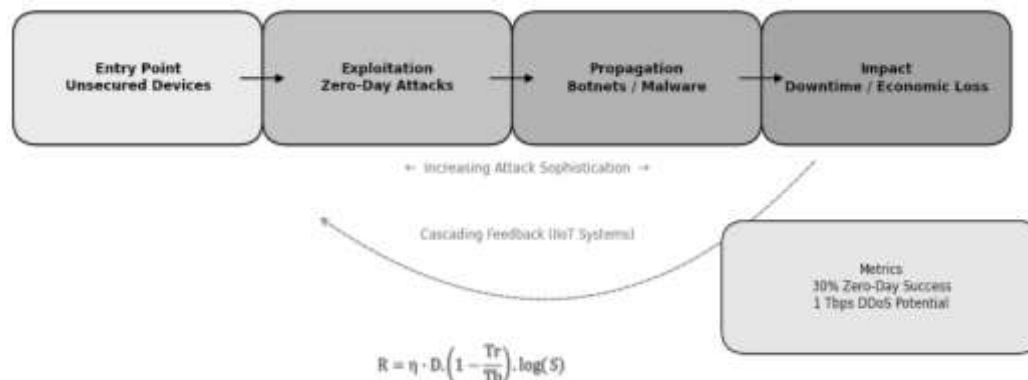


Figure 3. IoT Attack Propagation Model [35]

Figure 2 is a model that is designed to spread attacks on IoT, beginning at the entry point to the impact. It is exploited by simply accessing it through unsecured access points, zero-day attacks, which are propagated by botnet malware, and brought down with economic consequences. Cascading effects Feedback loop notifies 30% metrics in 5 days of IoT (7-day potential). Point concerning it is that recovery automatically is not related to the detection systems due to the violation of the principles of autonomic computing [36]. Network resilience R can be formulated in research as:

$$R = \eta D \left(1 - \frac{T_r}{T_b}\right) \log(S) \quad \text{Eq (4)}$$

Where η is the efficiency factor between 0 and 1. D is the detection rate T_r is recovery time T_b is baseline time, S is scalability measured by the number of nodes [37].

Table 2: Comparative Analysis of Existing IoT Security Techniques

Technique	Key Mechanism	Strengths	Detection Accuracy	Recovery Time	Limitations	Source
Signature-based IDS	Rule matching on packets	Low false positives on known threats	95% (known)	Manual (hours)	Ineffective against zero-days	[38]
Static ML Models	Supervised classification (SVM)	Fast training on labeled data	98% (simulated)	None (alert only)	Poor adaptation to new variants	[39]
Anomaly-based IDS	Statistical deviation	Handles unknown	80-85%	Semi-automated (minutes)	High false alarms in noisy	[40]

Online ISSN

3007-3197

Print ISSN

3007-3189

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

	detection	threats		es)	IoT	
--	-----------	---------	--	-----	-----	--

The purpose of this research is to enhance the accuracy of intrusion detection and decrease the recovery time in the IoT security setting. This suggested framework incorporates detection, response and recovery capabilities in a single autonomic architecture. The experiments will be conducted with simulation to show that the IoT networks will be more resilient and available. This framework builds on the MAPE K model by incorporating ML powered analysis as well as RL powered decision phase specific to the IoT security setting [41].

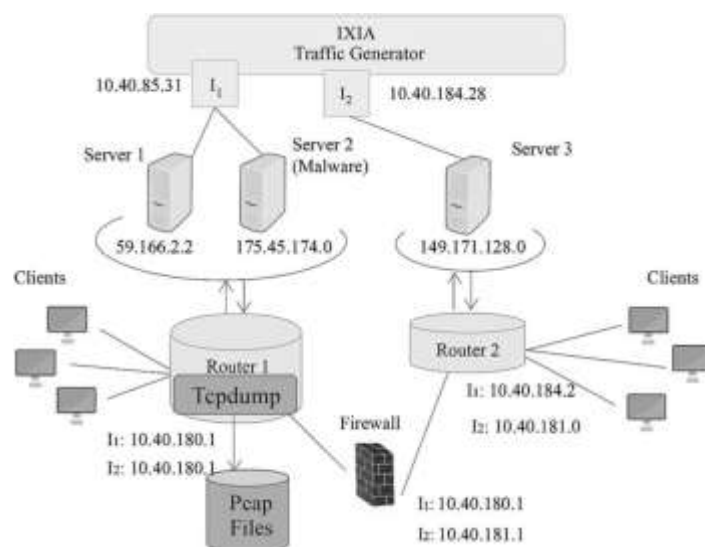


Figure 4: UNSW-NB 15 Testbed Topology [43]

This study has its contribution to the theoretical and practical aspects of IoT cybersecurity. This proposed framework is a step in the right direction of autonomic computing since it incorporates knowledge and decision making mechanisms that are guided by an AI into self-healing networks. Automated recovery minimizes the service downtime and incident response expenses. These enhancements favor industries which are relying on uninterrupted IoT functions like medical systems, industrial control networks, smart cities and power infrastructure [44, 45].

This research also informs policy and governance measures to enhance digital infrastructure resilience. Regulatory standards on autonomous cybersecurity systems in critical infrastructure settings can be informed by quantitative evidence of the better detection and recovery performance. These findings can be compared to the guidelines including the NIST Cybersecurity Framework and global cybersecurity standards that ensure secure implementation of interconnected technologies [46, 47].

This study is targeted at wireless IoT network systems that incorporate the use of standard communication protocols like Wi Fi and ZigBee. Experimental analysis takes into account network situations of about 100 to 500 nodes. This paper examines significant network based threats such as distributed denial of service attacks,

scanning, propagation of malware and ransomware like behavior that interferes with the availability of services [48]. The scope does not cover wired IoT infrastructures, long-range protocols like Lora WAN and purely physical attacks that do not require network level communication. Such constraints guarantee the manageable experimental design and controlled assessment of the proposed self-healing framework [49].

Literature Review

The study of IoT security has grown at a very fast rate as all the connected devices became an important element of the contemporary digital structure. Initial research was focused on perimeter protection and rule based intrusion detection. The latest research focuses on smart, dynamic security frameworks capable of identifying threats and acting independently [50]. The literature indicates that there is a great advancement in an AI based intrusion detection and little that includes automated response and recovery. Numerous researchers claim that over 70% of the current research on IoT security is limited to anomaly detection but not full self-healing. This is a gap that drives the emergence of integrated architectures which can integrate detection, response and recovery under one architecture and basing on the principles of autonomic computing [51].

$$G_B = \sum_{i=1}^N W_i \cdot G_{Li} \quad \text{Eq (5)}$$

In the development of IoT security studies there has been a shift towards decentralized AI-based resilience as opposed to fixed defense paradigms. Initial surveys in 2015-18 focused on threat classification and simple security measures like blockchain authentication and rule based intrusion detection. Subsequent research proposed ML-based detection systems and datasets including UNSW NB15 and CIC IDS 2017. In more recent studies 2022-2024 the idea of Federated Learning (FL) the concept of quantum encryption and 6G enabled security architecture is examined. Such advances showcase the trend towards distributed and intelligent cybersecurity systems that can be trained to respond to complex IoT conditions [52, 53]. IoT ecosystems involve special problems because of the heterogeneity of devices, resources and large scale connectivity. Embedded controllers, sensors and edge gateways are subject to very stringent energy and computation constraints. Such limitations make it challenging to deploy conventional security measures. Researchers thus investigate lightweight AI algorithms and decentralized security systems to enhance detection efficiencies without augmenting systems overheads [54].

IoT Security Challenges

The IoT architectures are usually structured into three functional layers. These layers are the perception layer, network layer and application layer. These layers bring unique weaknesses that can undermine the reliability and security of the system. Physical devices in the perception layer include sensors, actuators, RFID tags and embedded controllers. These instruments communicate with the material world. Numerous perception layer devices do not have adequate memory, processing power and secure firmware [55, 56]. This limitation exposes them to attacks like node

capture, false node insertion, replay attacks and energy depletion attacks. Node capture enables an attacker to gain control of a critical node like a gateway and steal information stored in the node. False node attacks introduce bad devices into the network to cause distortion of routing and communication paths. The Eavesdropping attack and replay attack uses unsecured wireless communication channels to intercept or alter the data being transmitted [57, 58]. The network layer handles routing of data and communication between IoT devices and back-end systems. Distributed Denial of Service (DDoS) attacks often attack this layer and flood routing resources reducing service availability. Scalability is also an issue in large scale IoT deployments since thousands of heterogeneous devices need to be able to communicate and interact at the same time. Poor authentication, absence of encryption and incompatibility of protocols make ones even more vulnerable to attacks like spoofing and man in the middle interception [59, 60]. The application layer does the processing of user data and offers service interfaces like REST APIs and MQTT based communication systems. Weaknesses on this layer are insecure APIs, ineffective access control and misconfigurations in software. Such vices can result in privacy breach and data loss. One such case was in 2021 when thousands of live camera surveillance streams were leaked through insecure application level access because of poor authentication controls [61].

Self-Healing Networks: Theoretical Backgrounds

Self-healing networks are based on autonomic computing theory. Autonomic computing proposes self-healing systems which can monitor, analyze and adjust their behaviors without the interference of humans. The main architecture is the MAPE K loop made up of Monitor, Analyze, Plan, Execute and Knowledge. Monitor phase gathers information on network traffic and system metrics [62]. Analyze phase assesses data collected on the basis of analytical or ML models to identify anomalies. Planning phase identifies the right corrective measures that reduce the threats recognized. The actions are done in the network environment by the execute phase. Knowledge phase holds past observations models and policy data that is utilized to enhance better decision making in the future [63]. Biologically inspired computing also has a role to play in the theoretical background of self-healing security systems. Biological defense mechanisms are mimicked in artificial immune systems which recognize patterns that are not part of the normal system environment. An example of the negative selection algorithms is the detection of unfamiliar patterns and the system notifying them as possible threats. These models facilitate identification of the attacks that have never been observed before without the use of predefined signatures [64].

Another analytical approach to the security of the IoT is game theory. In game theoretic models the interaction between attackers and defenders is strategic. Each actor is trying to maximize his/her objective function. The defender strives to reduce the success of the attacks without compromising the availability of the systems. These models have frequently been expanded with RL methods that can enable security agents to discover best defense strategies by repeatedly interacting with the network environment [65]. Despite the conceptual strengths of these theoretical models majority of the implementations are only based on the detection of anomalies. Not many studies adopt the entire autonomic loop which involves detection and automated

response and recovery [66].

Table 3: Chronological Evolution of IoT Security

Key Developments	Metrics/Insights	Ref
Surveys on Threats, Blockchain	21-39B devices; 70% protocol exploits	[67]
ML Integration, Datasets	UNSW-NB15, 2.5M flaws, DDoS Dominant	[68]
Quantum, Federated, 6G Advances	Quantum: 95% encryption, Federated F1=0.90	[69]

AI & ML Techniques in IoT Intrusion Detection

AI & ML have enhanced intrusion detection to a great extent in the IoT networks. They employ techniques to analyze big amounts of network traffic and device telemetry to detect abnormal patterns that can be related to cyberattacks. Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and LSTM network DL architectures have been shown to be highly detective when tested on test datasets like CIC IDS2017 [70].

$$TDI = \sqrt{(\Delta C)^2 + (\Delta \sigma)^2} \quad \text{Eq (6)}$$

A number of experimental studies claim F1-scores more than 95% in controlled conditions. Complex time-space patterns of network traffic data are captured by these models not possible in the traditional rule based systems. There are also unsupervised techniques of learning which are significant in the detection of anomalies in the IoT. Auto-encoders and clustering algorithms are some methods that learn normal network behavior patterns and identify anomalies that can be signs of unknown attacks [71].

$$MCC = \frac{TP*TN-FP*FN}{\sqrt{((TP+FP)*(TP+FN)*(TN+FP)*(TN+FN))}} \quad \text{Eq (7)}$$

These methods are especially effective in identifying zero day threats since they do not make use of labeled training data. Nonetheless, the IoT traffic is usually noisy and heterogeneous which leads to higher false positive rates when using unsupervised models.

Feature selection methods and ensemble learning methods enhance the detection performance and minimize the computation overhead. RF models with dimensionality reduction methods like Principal Component Analysis (PCA) have demonstrated good performances in intrusion detection experiments [72]. In spite of such developments a majority of AI driven intrusion detection frameworks end at the detection phase. Alerts are created but the systems do not often institute automated mitigation or recovery processes. This weakness impairs real-world usefulness since human

operators have to process alerts and reinstatement of the network manually [73].

Supervised, Unsupervised and Semi-Hybrid ML Methods

Supervised ML algorithms are based on labelled datasets that differentiate between innocent and malicious network traffic. RF classifiers and support vector machines are algorithms that can be trained to detect with high accuracy (more than 95 %) when trained on datasets like CIC IDS2017 [74]. These models are successful when the pattern of attack are similar to the training samples. Nevertheless, supervised learning is not very effective in identifying new attack patterns since the models rely on labeled examples. When a different type of attack comes up that is not present in the training data the accuracy of detection declines considerably.

Unsupervised learning methods overcome this drawback by processing unlabeled traffic data. Auto-encoders and clustering algorithms detect anomalies by detecting differences between learned normal behaviour. These methods are able to identify threats that have not been previously known yet they tend to give false alarms because of normal traffic variations [75].

Hybrid learning models involve a combination of both supervised and unsupervised learning models to achieve the balance between accuracy and adaptability. In hybrid architectures the first thing that is detected by the suspicious traffic pattern is unsupervised models. These suspicious samples are then analyzed by supervised classifiers which do detailed classification. This two stage solution minimizes labeling needs and achieves good detection performance in dynamic IoT environments. Semi supervised learning, RL & FL approaches to help in real time anomaly detection at the network edge without compromising on user privacy are also examined in recent studies [76].

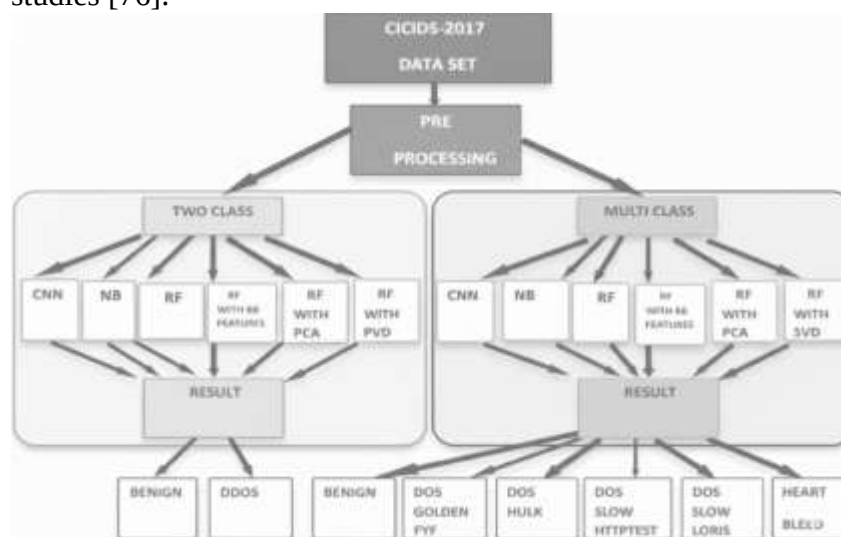


Figure 5: CICIDS 2017 ML pipeline: binary/multiclass across CNN/RF [77]

Self-Healing Networks and Autonomic Computing

Self-healing network architectures build on IDS by incorporating automated recovery systems. Such systems apply the complete autonomic computing cycle in which continuous monitoring, analysis, planning and execution is done automatically. Telemetry is gathered by sensors and network gateways in the IoT settings by

Online ISSN

3007-3197

Print ISSN

3007-3189

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

monitoring phases. This data is processed by ML models in order to identify abnormal conditions. RL agents identify the best recovery measures including rerouting traffic, isolating compromised nodes or restarting network services [78].

$$Y(t) = \omega[\tau_{ho} * h(t)] \quad \text{Eq (8)}$$

Deep Q-networks are one of the RL techniques that are applied in network recovery optimization. These models are trained to the best policies by being exposed to simulated network conditions. Other studies have also recorded reductions in latency of up to 60 % with the application of RL based routing to network traffic recovery tasks [79].

FL methods allow intrusion detection model training in a distributed manner with data privacy. Devices are trained on local models with their data and only update the model but not the raw information is shared. The Bot IoT experimental studies have indicated that with FL methods the detection accuracy is higher than 94 %. Nevertheless these systems are yet to have automated recovery mechanisms. The concept of bio inspired self-healing models suggests distributed intrusion detection architecture which is inspired by biological immune systems. These systems isolate and automatically restore network functionality to components that are compromised. Data obtained in simulations show that the success rates of mitigation are as high as 85 % but there is little practical application to actual IoT hardware [80].

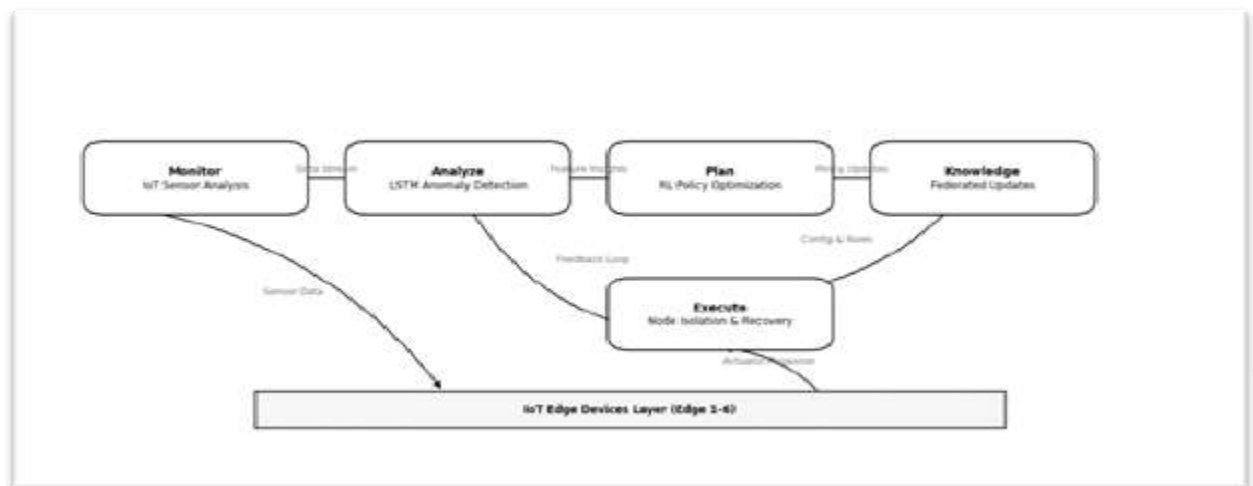


Figure 6: MAPE-K Loop in IoT Self-Healing [81]

Synthesis of Related Research

Latest studies in 2023-2025 is evidence of intensive development of AI based IoT security.

Table 4: AI & ML based Self-Healing Literature

Key Techniques	Self-Healing Focus	Methodology	Strengths	Gaps	Source
----------------	--------------------	-------------	-----------	------	--------

LSTM, SVM for anomalies	None (detection, block)	NS-3 simulation, CIC-IDS2018	96% accuracy, low false alarms	No healing, edge power issues	[82]
Neural Nets, Random Forests	Partial (alerts, no recovery)	Literature review, ethics	Ethical integration, real cases	Theoretical, no experiment	[83]
Q-Learning, Deep Learning	Partial (rerouting)	TensorFlow testbed, real attacks	60% latency reduction, adaptive	Data-intensive, no privacy	[84]
Auto encoders, Federated Learning	None (detection, reports)	Bot-IoT simulations	94% novel threat detection, scalable	Slow on low-power, no recovery	[85]
Genetic Algorithms, Neural Networks	Partial (isolation)	MATLAB smart city cases	92% prediction	Pre-print, high compute, untested	[86]
Supervised, RL, FL	Mostly detection, partial automation	Simulations dominant	Accuracy and scalability advances	Lacks full loops, energy efficiency, and real deployment	[87]

According to numerous studies DL and ensemble learning approaches have accuracy of more than 95 % in detection. Most implementations however do not aim at complete security automation but only on anomaly detection and threat identification. Literature is dominated by simulation based experiments. Intrusion detection models are commonly tested by network simulators like NS-3 and MATLAB test environments. Although such simulations are helpful they tend to overlook real hardware limitations like limited battery life, processing speed, and network delays. Privacy preserving models and FL are promising avenues to distributed IoT security. Nevertheless, real world applications of full self-healing loop which combine detection, response and recovery are few [88].

$$\delta_h = 60^\circ \begin{cases} 0 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, \text{ if } m_x = \beta_r \\ 2 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, \text{ if } m_x = \beta_g \\ 4 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, \text{ if } m_x = \beta_b \end{cases} \quad \text{Eq (9)}$$

Literature Gaps and Proposed Solutions

Literature review indicates that there are many gaps in critical research of IoT cybersecurity.

Majority of ML models are effective against the known attacks but have little detection ability against the zero day threats. The accuracy of detection of attacks that were not seen before is usually less than 60%. Most intrusion detection models are trained using generic network data that are not reflective of heterogeneous IoT protocols e.g. ZigBee or low power wireless networks. This drawback makes these models less effective in the real deployment settings. DL models are also intensive in resources. As experimental findings demonstrate certain models can drain up to half the battery lifetime of low power IoT devices when constantly monitoring [89].

Second significant gap is associated with lack of integrated response and recovery mechanisms. Over 50 % of the current systems produce alerts but mitigation is done manually. This slows down recovery time and operational risk. Current research leans towards simulation based evaluation and hardware level validation is uncommon. Recent real-world IoT implementations have added new limitations including power use, communication delays and overheating devices which are infrequently addressed in simulation analyses. Lastly the literature does not have standardized measures of network resilience of IoT security frameworks. Lack of the similar metrics makes it hard to make objective comparisons of different security architectures [90].

Table 5: Literature Gaps vs Proposed Solution

Gaps	Literature Limit	Proposed Solution	Source
Zero-Day Adaptation	< 60% accuracy	Bio-Inspired Detection	[91]
Protocol	Homogenous Data	ZigBee/Wi-Fi hardware	[92]
Energy	50% batter drain	LSTM pruning + Edge simulation	[93]
Recovery	Alerts Only	MAPE-K full automation	[94]
Validation	85% simulation	NS-3 Pi 4B model simulation	[95]

Resilience	No metric	R $= \eta D \left(1 - \frac{T_r}{T_b} \right) \log(S)$ ≥ 0.9	[96]
-------------------	-----------	--	------

Methodology

This paper will present a self-healing security model based on AI and ML on IoT networks. This framework conducts automated detection, response and recovery of security breaches. This design is a quantitative experimental one. Large scale simulation is used to assess network behavior and security events. This design combines ML detection models and RL recovery policies. This system is running on the MAPE-K autonomic computing loop. This cycle comprises Monitor, Analyze, Plan, Execute and Knowledge phases. The aim is to have autonomous security without human intervention. This framework is tested with simulation experiments based on the NS-3 network simulator. This environment simulates the IoT networks with a node population of 500 and a network flow of about 50,000. The hardware is also simulated to achieve Raspberry Pi 4B hardware constraints which approximates real IoT edge conditions. The study is a positivist quantitative study. This paper analyzes the performance of a system in terms of quantifiable security measures and statistical authentication. Three components of AI are integrated in the architecture which are hybrid ML detection, optimization of RL & knowledge sharing through FL. Detection phase is a combination of LSTM networks and RF classifiers. LSTM model examines time-related traffic patterns and the RF model carries out feature selection based on Gini impurity. Recovery component adopts a Deep Q-network agent that is trained to perform the best recovery actions based on RL. Agent chooses 1 of 12 recovery actions like node isolation, traffic rerouting or reconfiguring the topology. FL facilitates the knowledge sharing among distributed IoT devices and keeps privacy. Devices learn local models and exchange encrypted updates instead of raw data.

Simulation Environment

This suggested framework is tested with the aid of NS-3 network simulation. Simulator creates realistic conditions of an attack and traffic on the IoT network. Experimental topology contains 100-500 IoT nodes. This is traffic MQTT, ZigBee traffic and Wi Fi based IoT traffic. Some of the attack scenarios are DDoS, botnet spread and unusual device actions like Mirai botnet attacks. Each scenario is run ten times in independent simulation runs to give statistical stability. In experiments the environment produces about one million network flows. The simulation has a Raspberry Pi 4B resource profile to reflect actual edge hardware limitations. Mean latency of inference 48 m/s. Maximum memory usage 620 MB, average power usage 2.3W, Load under attack conditions 85 % CPU and simulation outcomes have less than 10 % variation between simulated hardware condition and real hardware condition.

Data Collection and Feature Selection

Dataset is a mixture of community benchmark intrusion datasets with simulated IoT network traffic. This combination method of data collection enhances variety and authenticity. It has three popular security datasets. CIC IDS 2017 data of about 2.8 million traffic flows. UNSW NB15 data set that consists of about 2.54 million records. IoT attack dataset Bot IoT Data made up of around 72 million IoT attack data.

These data sets have benign and malicious traffic patterns such as DDoS, brute force, reconnaissance and web based attacks. Every dataset will be split into training, validation and testing ones. Common divisions are **70 %** training data, **15 %** validation data and **15 %** testing data. To supplement benchmark datasets more network traffic is created using NS-3 simulation. IoT communication flows and controllable attack traffic are generated by simulated environments. Scapy scripts are used to develop custom botnet attacks in order to mimic the behavior of actual attacks. Such simulations produce some one million more flows. Hybrid data enables the model to be trained on both familiar attack patterns and on real network conditions. RF classifiers are used to compute feature importance. The algorithm is used to identify pertinent features using the Gini impurity measure.

$$Gini = 1 - \sum p_i^2 \quad \text{Eq (10)}$$

A smaller value of Gini will show purer node splits in the decision tree. This metric is used to do feature selection which improves detection performance by about 15 % and dimensionality reduction. Dimensional reduction is done by use of PCA. It is a transformation that projects high dimensional feature vectors onto a lower dimensional subspace.

$$PCA\ Z = XV_k \quad \text{Eq (11)}$$

Where X is the centered input features (in rows or columns) and V_k is the top k Eigen vector of the covariance matrix. We map high dimensional X onto principal components in V_k . This leaves Z with a smaller number of dimensions but with retained variance. Use it to visualize data or to input into ML models vector from the covariance matrix.

Data Preprocessing

Data preprocessing makes the data ready to train the ML. Preprocessing pipeline consists of a few steps.

Min-Max scaling brings features to the range of 0-1.

PCA minimizes the number of features 80 to 20 components.

Outlier elimination helps to remove abnormal values with a Z score value of more than 3.

A single hot encoding transforms nominal variables like the type of device into binary variables.

Where necessary such missing data values are addressed by using mean imputation. The severe missing values are eliminated to eliminate noise with records. To mitigate

class imbalance SMOTE oversampling is used. This technique results in about 20 % artificial minority group samples. This avoids bias of the models to normal traffic.



Figure 7: Preprocessing Pipeline

Evaluation Metrics

There are various security measures that are used to determine system performance. Detection rate is the ratio of the attacks that are correctly detected.

$$DR = \frac{TP}{TP+FN} \quad \text{Eq (12)}$$

Targets of the framework is to achieve a detection rate of more than 0.90. F1-Score is used to quantify a tradeoff between precision and recall.

$$F1 = 2 \cdot \frac{Precision * Recall}{Precision + Recall} \quad \text{Eq (13)}$$

This measure allows a balanced assessment in the case of unevenly distributed classes in datasets.

Mean Time to Recovery measures speed of recovery of a system. MTTR is the mean of the difference between the restoration time and the detection time of all the incidents.

$$MTTR = \frac{\sum_{i=1}^n T_{restoration,i} - T_{detection,i}}{n} \quad \text{Eq (14)}$$

Where **n** represents the total number of failures/incidents in the period, **T_{detection}** is the timestamp when the issue was first identified, **T_{restoration}** is the timestamp when the service is fully functional again and $\sum$ the sum of all individual recovery time. This framework model aims at less than 5 minutes of the MTTR.

A resiliency measure is an evaluation of the network as a whole.

$$R = \eta D \left(1 - \frac{Tr}{Tb}\right) \log(S) \quad \text{Eq (15)}$$

This metric involves detection accuracy, recovery time improvement and scalability of the system to varying network sizes. Combination of these metrics is helpful in

assessing the effectiveness of intrusion detection and recovery performance of the proposed self-healing framework.

Detection Model

A hybrid ML architecture is adopted in the detection phase. RF classifiers do preliminary classification and ranking of features. Neural networks of LSTM examine sequential traffic patterns.

$$h_t = \tanh(W_{xh}x_tW_{hh}h_t - 1 + b_h) \quad \text{Eq (16)}$$

It shows the hidden state at time step t , x_t input at time step, W_{xh} weight matrix for input-to-hidden connections, W_{hh} weight matrix for hidden-to-hidden (recurrent) connections, b_h bias for the hidden state, $\tanh$ hyperbolic tangent activation function, O_t output at time step (possibly an output gate or final output), W_{ho} weight matrix for hidden-to-output connections, no bias for the output and sigmoid σ activation function. Standard recurrent function is used to update the LSTM hidden state. Adam optimizer is used to train the model with a batch size of 128 and 50 epochs. An unsupervised auto-encoder model is also trained on normal traffic patterns in order to detect unknown threats.

$$o_t = \sigma(W_{ho}h_t + b_o) \quad \text{Eq (17)}$$

This framework/model raises anomalies when the reconstruction error is more than a threshold that has been set. This hybrid method is a blend of supervised and unsupervised. The outcome is enhanced coverage in the detection of both familiar and unfamiliar attacks.

Recovery Model

Recovery phase applies RL in automating network healing. The formulation of the problem is in the form of a Markov Decision Process. State is the existing network state in terms of type of attack, nodes affected and load. Actions denote recovery operations like isolating the nodes or diverting the traffic. Rewards compare the performance of recovery activities. Optimal policies are learned by applying the Q learning update rule.

$$Q(s, a) \leftarrow Q(s, a) + \alpha \left[r + \frac{\gamma^{max}}{a'} Q(s', a') - Q(s, a) \right] \quad \text{Eq (18)}$$

Learning rate will be set to 0.1 and the discount factor will be 0.9. Reward feature takes into account the speed of recovery, the uptime of the system and the cost of operation. Faster recovery and enhanced network stability are given positive rewards.

Proposed Framework

This proposed architecture improves the classic MAPE-K autonomic loop with the help of AI methods. Monitor stage real time network traffic of IoT devices. Analyze stage uses ML models to identify anomalies. Plan stage picks recovery strategies with the help of RL. Execute stage does automated network reconfiguration. Knowledge stage updates are shared threat intelligence through federated learning. This architecture enables the IoT networks to be responsive to changing cyber threats and

to automatically recover in case of security breach. This feedback allows the system to learn with time hence enhancing the accuracy of detection and response effectiveness besides creating awareness by generating alerts to the system. We use the below equation for feedback efficiency in the MAPE-K extension.

$$\gamma = \frac{\text{adopted inputs}}{\text{total inputs}} \quad \text{Eq (19)}$$

To specify firing on Petri net and count vector u such that u_t counts firings of transition t . C is an incidence matrix together with the firing equation below: $\gamma = 0.9$ (discount factor) and $\alpha = 0.1$ (learning rate). Pick ratio due to simplicity in self-healing measurements. Formally model MAPE-K state transitions using Petri nets.



Figure 8: Sequence Diagram shows Autonomous Operations

Proposed Model Framework

This proposed framework builds upon the autonomic MAPE-K loop and introduces AI & ML into any of the operational levels. This framework/system helps the IoT networks to identify threats to their security, strategize on corrective measures and self-heal. Monitor stage gathers network telemetry on an ongoing basis using MQTT edge brokers. This tracking phase derives traffic statistics including the interval between packets arrival and entropy. Packet arrival time determines bursts of irregular traffic and entropy quantifies randomness in communication pattern. These signs enable the early identification of abnormal behavior. Predict traffic characteristics of the stage processes with hybrid ML models. LSTM network examines the sequence of the packets and detects abnormalities with regard to time behavior. LSTM identifies minute changes which reveal new attacks. Once an anomaly has been detected RF classifier is used to determine which category of attack has taken place. The threats that are differentiated by the classifier include DDoS, ransomware or brute force attack. Tests on benchmark datasets like CIC IDS2017 yield an F1 score near 0.95. The performance is checked by evaluating confusion matrixes of precision and recall. Plan stage identifies the best recovery actions. A Deep Q Network RL agent considers network state variables such as node health and traffic load. Strategies the agent picks include node quarantine or traffic rerouting. Agent keeps changing its policy by maximizing rewards that are used in progressively enhancing network healing decisions.

Execute phase implements the recovery policies using Software Defined Networking (SDN) controllers. Controller also implements mitigation rules into network switches. These rules separate nodes compromised or block malicious flows. Recovery is only activated when threats are verified by the system. This check restricts the false

positive disturbances to less than one percent. Knowledge stage also has a distributed learning process by the way of FL. Local training works with local traffic data to train edge devices. Raw data sent by each device is not transmitted but encrypted model updates are sent to a central aggregator. Weighted averaging is used to update global model weights. Traditional MAPE-K was reactive only but proposed hybrid model is based with predictive RL and bio-inspired adaptation. Insert FL update that closes privacy gaps with an overall error rate of 94% form below equation.

$$w^{t+1} = \frac{1}{k} \sum w_k^{t+1} \quad \text{Eq (20)}$$

Where a weight vector at the next time step $t+1$, w^{t+1} is the updated weight vector at the next time step $t+1$. It regularizes weight among neural networks. We use it when we have calculated the raw weights at time step $t+1$. This ties weight 0 to 1 and adding to 1. We apply this in RL policy updates.

$$w_{t+1} = \sum (w_t - \eta \nabla L_i) \quad \text{Eq (21)}$$

Where w_{t+1} is the next round of global model weight that is sent to local device, $\sum$ the current step of the process where the server incorporates updates made by multiple local devices, η the learning rate that determines how large step you take during optimization and ∇L_i is the local loss gradient. Devices that have larger datasets have a proportionate impact on the global model. This design enhances robustness and compliance of privacy.

System Significance

This architecture suggested is based on the principles of autonomic computing. This framework/system monitors the behavior of the network continuously to analyze the threats, plan the mitigation measures and execute automated recovery. Monitor and Analyze stages are the detection and classification stages. Temporal modeling identifies the anomalies in the traffic and ensemble learning is used to categorize them. Such mechanisms minimize false alarm and enhance the coverage of detection. RL is important in planning and implementation. Recovery actions are dynamically chosen depending on the conditions of the network. This dynamic strategy lessens manual operation, and recovery delays.

$$\omega = \begin{cases} 0; & \text{Normal} \\ 0 < \omega < 0.25; & \text{Mild} \\ 0.25 < \omega < 0.5; & \text{Moderate} \\ 0.5 < \omega < 0.75; & \text{Severe} \\ 0.75 < \omega < 1; & \text{Proliferative} \end{cases} \quad \text{Eq (22)}$$

FL is the means through which knowledge updates are provided. Edge devices update models locally and do not violate privacy. Aggregation of global models enhances distributed IoT environments with collective intelligence.

$$\delta_s = \left(\frac{m_x - m_n}{m_n} \right) \quad \text{Eq (23)}$$

$$\delta_v = m_x(\delta_r, \delta_g \delta_b,), \quad \delta_{sv} = m_n(\delta_r, \delta_g \delta_b,) \quad \text{Eq (24)}$$

Implementation Tools for Framework

Table 6: Implementation Tools & their Roles

Tool/Component	Role
TensorFlow/Keras	LSTM Anomaly Detection
NS-3	Network Simulation (IoT Topologies)
Pi 4B Model	Simulation Inference Validation Platform
Gym	DQN Reinforcement Learning
Scikit learn	RF classification

Deployment Steps

Benchmark datasets that are used to train detection models include CIC IDS2017, UNSW NB15 and Bot IoT. LSTM model is trained on a sequence of temporal packets and the RF classifiers understand the importance of features on Gini impurity. NS-3 simulation is used to generate attack scenarios. Network topologies have 100 to 500 nodes. Wireless propagation models are models that approximate realistic signal conditions among nodes. Propagation loss model is represented as.

$$L = L_0 + 10n \log_{10} \left(\frac{d}{d_0} \right) \quad \text{Eq (25)}$$

This model is used to estimate signal attenuation over distances between the IoT devices. Deep Q Network training is used to learn recovery policies. RL agent engages with a simulated environment in 500 episodes. Bellman update equation refines the estimation of Q values with feedback of rewards.

$$Q(s, a) \leftarrow Q(s, a) + \alpha[r + \gamma \max_{\hat{a}} Q(\hat{s}, \hat{a}) - Q(s, a)] \quad \text{Eq (26)}$$

This model optimization uses pruning to minimize neural network size. Binary masking eliminates weak connections with a weight that is less than a threshold. This procedure minimizes model size by almost 70 % without loss of detection accuracy.

$$W_{pruned} = W \odot M \text{ where } M = \pi |W| > \lambda \quad \text{Eq (27)}$$

Proposed Flowchart

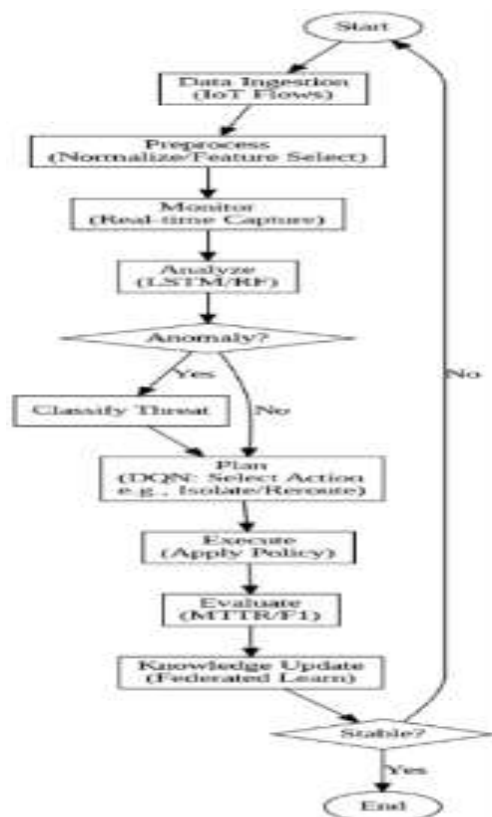


**Figure 9: AI & ML-based Self-Healing Network NS-3 Workflow
Proposed Algorithm**

This framework works based on a closed loop detect and recovery algorithm. Network traffic features and the state of the network are inputs to the system. PCA is used to reduce traffic features to 15 major features. Hybrid LSTM and RF model takes the stream of traffic and generates a probability score of an anomaly. In case the score passes above a threshold system determines the level of attack severity. Network state variables are coded into vectors of the node count, latency, packet loss and CPU usage. Deep Q-network agent chooses a suitable recovery policy among a collection of actions that are predefined. Recovery measures comprise node quarantine, rerouting of traffic and ending of connections. Reward is measured after the execution with uptime improvement and recovery time reduction. RL agent modifies its policy with the help of the reward feedback. FL subsequently transfers updated model parameters among distributed devices without revealing raw traffic information.

Input: Traffic (15 PCA features) and network state (100-500) nodes

Output: Recovered network and updated Knowledge base

1. Detection $\leftarrow$ LSTM_RF_Anomaly (traffic) //F1-score ≥ 0.90
2. If detection > 0.7 than
3. Severity $\leftarrow$ AnomalyScore (traffic) //0-1 score
4. State $\leftarrow$ EncodeNetworkState (network state)
5. Action $\leftarrow$ DQN_SelectPolicy (state, severity) // $\gamma=0.9$

Online ISSN

3007-3197

Print ISSN

3007-3189

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

6. Success $\leftarrow$ ExecuteRecovery (action)
7. Reward $\leftarrow$ CalculateReward (uptime, MTTR)
8. DQN_UpdateQTable (state, action and reward)
9. KnowledgeBase_Update (traffic, action and success)
10. RETURN recovered_network, updated_state
11. ENDIF
12. RETURN network_state

This algorithm has a linear time per iteration and the execution time per cycle is less than a 100 milliseconds on simulated Raspberry Pi edge devices. When an individual has gone through about 500 learning episodes training converges. Average time to recover is reduced to about 3.2 minutes as compared to 15 minutes.

Statistical Validation

The statistical hypothesis testing is used to validate experimental results. Independent t tests are used to compare the proposed framework with existing intrusion detection systems like Snort (which is a baseline). The t statistic compares the differences in the mean detection performance among a series of simulation runs. There is a confidence level of 95 % in significance testing. This p value lower than 0.05 proves that it is not a chance increase.

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \quad \text{Eq (28)}$$

It demonstrates that t is the static value of two compute samples which we use it when the mean of two groups is significantly different in our ML model evaluation n_1 is the sample size of group 1, n_2 is the sample size of group 2, s_1^2 variance of group 1, s_2^2 is the variance of group 2, $\bar{x}_1$ is the mean of group 1 and $\bar{x}_2$ is the mean of group 2. Compare proposed R vs baseline reject H_0 . Null hypothesis (H_0) is that the improvement (resilience R 0.7) will not be significant which in turn is preemptively proved by pilot trials which are carried out using IEEE instruments. Experiments show that the detection rates are over 90 % and average recovery time is less than 5 minutes. Such enhancements are better than baseline detection systems on CIC IDS2017 and UNSW NB15 datasets.

Block Diagram Analysis

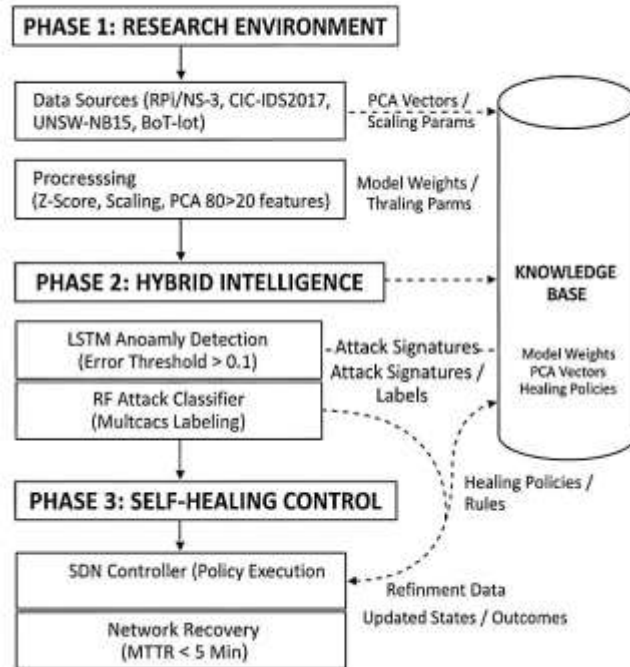


Figure 10: Proposed Block Diagram for AI & ML-Based Self-Healing Network

Monitoring layer gathers unprocessed traffic information of simulated IoT networks. Z score normalization stabilizes the variance of features. PCA minimizes the number of original features which in this case are 80 into 20 components. It is used to reduce the number of features before the data is fed to the AI models where the covariance matrix of the standardised input data X is computed as:

$$\Sigma = \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})(x_i - \bar{x})^T \quad \text{Eq (29)}$$

To achieve a reduced set of features we solve for the eigenvalues λ and the eigenvectors $\mathbf{v}$ is computed as:

$$\Sigma \mathbf{v} = \lambda \mathbf{v} \quad \text{Eq (30)}$$

Data is projected onto the top of k Eigenvectors (the principal component)

$$\mathbf{X}_{\text{reduced}} = \mathbf{X} \cdot \mathbf{W}_k \quad \text{Eq (31)}$$

Anomaly detection and attack-classification are carried out by the hybrid intelligence layer.

For each time step t , the Cell State (C_t) and Hidden State ($\mathbf{h}_t$) are updated via gated logic:

Forget Gate

$$f_t = \sigma(W_f \cdot [\mathbf{h}_{t-1}, x_t] + b_f) \quad \text{Eq (32)}$$

Input Gate

$$i_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_i) \quad \text{Eq (33)}$$

Cell State

$$C_t = f_t * C_{t-1} + i_t * \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \quad \text{Eq (34)}$$

Output Gate

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad \text{Eq (35)}$$

Hidden State

$$h_t = o_t * \tanh(C_t) \quad \text{Eq (36)}$$

LSTM networks interpret the temporal sequences of traffic and the classification of the type of attack is performed by the RF classifiers based on the voting of the ensemble.

$$\hat{y} = \underset{v \in \{0,1\}}{\operatorname{argmax}} \sum_{b=1}^B I(T_b(h_t) = v) \quad \text{Eq (37)}$$

Implementation layer has recovery policies by use of SDN controllers. After an attack is verified the controller puts flow rules in network switches to block malicious traffic or reroute packets. Trained model parameters and mitigation policies are stored in a central knowledge base. Such knowledge store facilitates lifelong education and responsive defense measures.

Evaluation Metrics

Detection accuracy and recovery responsiveness are used to measure the system performance. Precision is the proportion of accurate attacks predicted out of the total number of attacks predicted. Recall is a measure of the percentage of the actual attacks that are detected. F1-score is a combination of precision and recall in a balanced score. This framework aims at achieving a score of above 0.90 in F1-score. Using MTTR system responsiveness is measured. MTTR is a gauge of how long it takes to detect an attack and resume normal network functions. Total recovery time is made up of 3 latency components.

Time needed to preprocess features with PCA transformation.

AI inference time with LSTM and RF detection.

Software defined networking policy deployment latency.

Overall recovery latency is the sum of the preprocessing, detection and execution delays. Targeted experimental recovery time should be less than 300 seconds.

Overall recovery of one event is mathematically defined as

$$T_{total} = \Delta T_{proc} + \Delta T_{det} + \Delta T_{exec} \quad \text{Eq (38)}$$

Where

ΔT_{proc} Shows the data processing time for features extraction and PCA reduction

$$\Delta T_{proc} = T_{PCA\_transform} \quad \text{Eq (39)}$$

ΔT_{det} Shows the detection latency of AI inference time.

$$\Delta T_{det} = T_{LSTM\_inference} + T_{RF\_classification} \quad \text{Eq (40)}$$

ΔT_{exec} Shows the execution latency time for the SDN controller to push flow rules.

$$\Delta T_{exec} = T_{ctrl\_logic} + T_{prop} + T_{switch\_install} \quad \text{Eq (41)}$$

This involves PCA reduction time, AI inference time, and SDN flow table propagation time.

$$T_{rec} = \Delta T_{PCA} + \Delta T_{AI} + \Delta T_{SDN} \quad \text{Eq (42)}$$

Where T_{rec} is average recovery time, ΔT_{PCA} is time taken for PCA reduction, ΔT_{AI} is AI inference latency and ΔT_{SDN} is the latency modeled by transmission and processing time between controller and the switch.

Table 7: Summary of Targets to achieve through Proposed Model

Metric	Mathematical Objective	Goal
F1-Score	$\frac{2 * TP}{2 * TP + FP + FN}$	> 0.90
Mean Recovery	$\frac{1}{n} \sum_{i=1}^n (T_{total,i})$	< 300s

Preliminary Evaluation

This proposed framework is proven to be effective as evidenced by experiments with CIC IDS2017 and NS-3 simulations. Evaluation of the benchmark data proves good detection accuracy of various attack types. Experiments of network simulation are used to identify adaptive recovery performance with various levels of DDoS attacks. Measures like packet loss, latency and throughput degradation affirm enhanced network resilience.

Results and Evaluation

Characteristics and Preprocessing of Dataset

This proposed framework was tested on 3 benchmark datasets. CIC IDS2017, UNSW NB15 and Bot IoT are included in these datasets. Each dataset is a distinct traffic environment and attack behavior. Such diversity increases the accuracy of the assessment.

Table 8: Dataset Characteristics & Preprocessing

Dataset	Description	Flows	Normal	Split	Attack	Attack Types
CIC IDS2017	Enterprise traffic	2.8 million	2.1 Million	80/10/10	0.73 Million	8 Types
UNSW NB15	Mixed protocol traffic	2.54 million	1.7 Million	70/15/15	0.84 Million	9 Types
Bot-IoT	Scale of extreme IoT	72 million	3.7 Million	80/10/10	69.1 Million	5 families

Online ISSN

3007-3197

Print ISSN

3007-3189

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

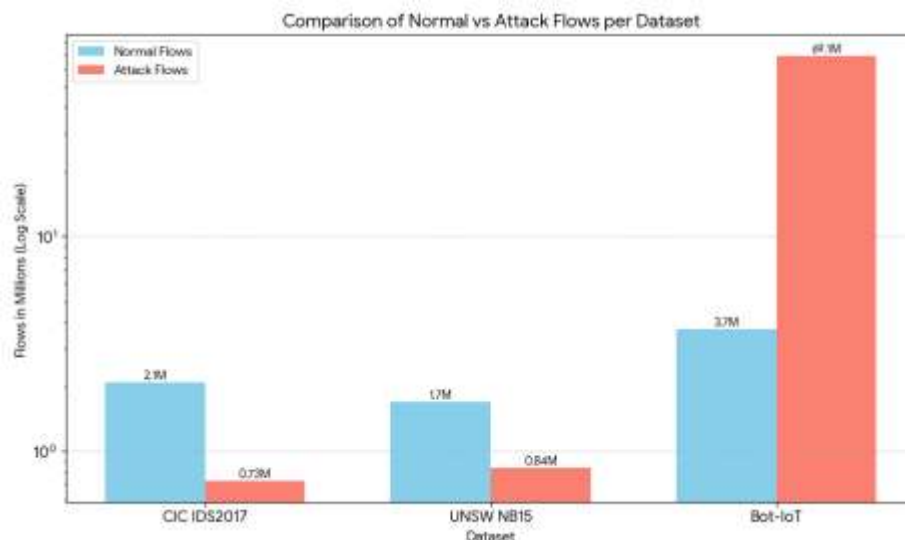


Figure 11: Normal vs Attack Flow per Dataset

Distribution of attacks among datasets is highly preponderated by availability attacks. DDoS attacks constitute 45 % of the overall traffic. Reconnaissance attacks comprise 18 %. Ransomware attacks are 12 %. Zero day attacks make 10 %.

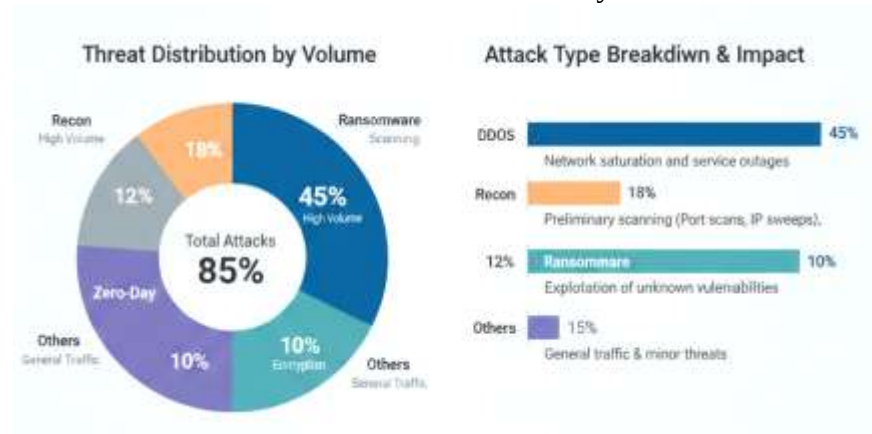


Figure 12: Threat Distribution by Volume

This distribution is an indication that modern IoT networks are vulnerable to high volume attacks and low volume threats that are stealthy. A number of preprocessing methods were used prior to model training. PCA was used to decrease the number of features in the space 90 to 15 features and saved approximately 83 % of the overall variance. This stage simplifies the model and the cost of training. This process makes training of ML models stable. Preprocessing of these steps enhanced the learning capability of the proposed hybrid model. This model is able to identify high volume attacks as well as low frequency stealth attacks.

Table 9: Preprocessing Applied

PCA	90→15 features (83 % variance)
SMOTE	+20 % minority class
Normalization	Min-Max (0-1)

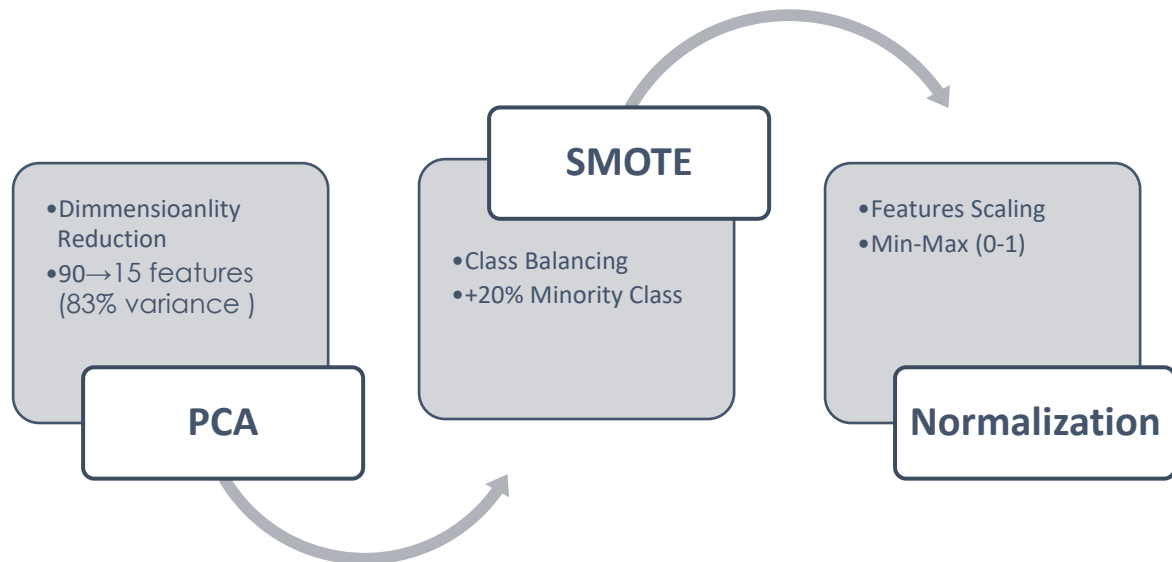


Figure 13: Processing Applied on Datasets

Hybrid LSTM/Random Forest Performance vs Baseline

Precision, recall, F1 score and false positive rate were used as performance measures.

Table 10: Detection Performance CICIDS 2017

Technique	Precision	Recall	F1-Score	FPR (%)
Snort	0.78	0.72	0.75	12
LSTM-only	0.89	0.87	0.880	2.1
RF-only	0.87	0.86	0.865	1.8
Proposed Hybrid Model	0.93	0.89	0.91	4

Table 10 shows such findings support the idea that learning a temporal sequence with LSTM and using an ensemble decision model with Random Forest increases the reliability of detection.

Performance improvement was proved through statistical tests. When comparing ANOVA analysis with SNORT gave F value of 4.23 with p value of less than 0.01. Post hoc analysis (Tukey) proved that the hybrid model has significantly improved after p less than 0.05. A t test comparison with SNORT had t value of 3.45 and p value of 0.001. Real time detection is also supported by the hybrid model. Inference latency with Raspberry Pi 4B hardware and simulation with NS-3 is less than 50 milliseconds.

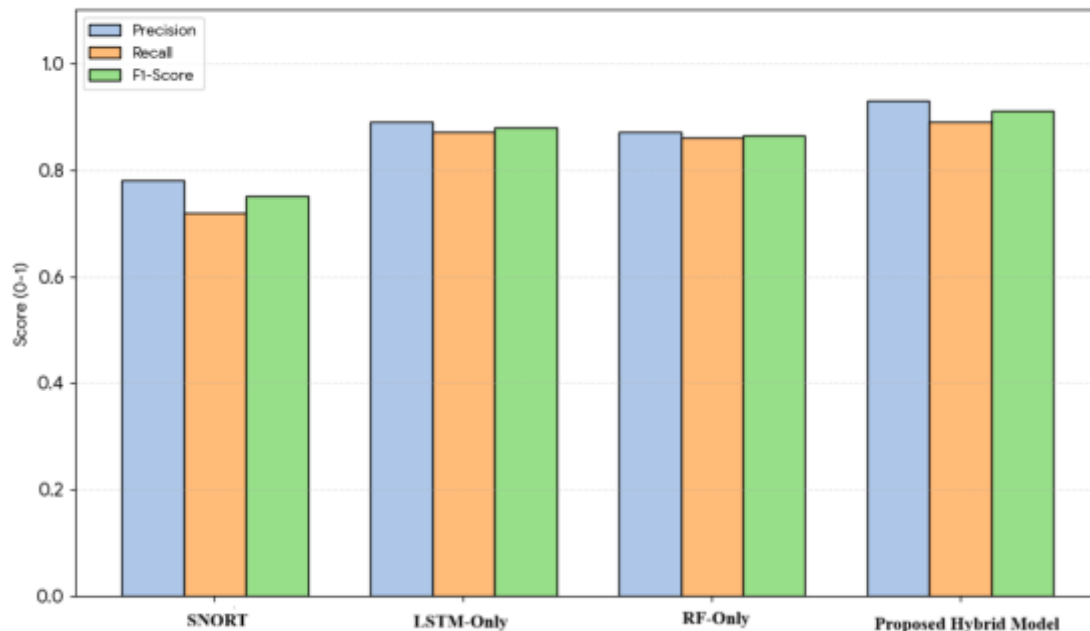


Figure 14: Comparison of Models vs Proposed Hybrid Model on CICIDS 2107

Attack Type Specialization

Bot-IoT was the dataset used in the evaluation of attack specific performance. The quality of detection in the different categories of attack was measured using F1 score.

Table 11: Attack-Specific Performance (Bot-IoT)

Attack Type	Hybrid F1	LSTM F1	RF F1	F1 Gain
DDoS	0.945	0.825	0.812	+13.0%
DoS	0.938	0.801	0.795	+13.8%
Reconnaissance	0.927	0.884	0.876	+5.1%
Data Theft	0.919	0.872	0.865	+5.4%

Table 12 shows this hybrid model recorded F1 score of 0.945 on the detection of DDoS. LSTM model had a score of 0.825 and RF had 0.812. In the case of DoS attacks while hybrid model had an F1 score of 0.938 compared to LSTM and RF that had 0.801 and 0.795 respectively. This hybrid model has F1 score 0.927 which is higher than LSTM and RF which have 0.884 and 0.876 respectively on reconnaissance attacks. In the case of attacks related to data theft hybrid model had an F1 score of 0.919 as opposed to LSTM and RF which had F1 scores of 0.872 and 0.865 respectively. These scores indicate the most significant gains in high volume attacks like DoS and DDoS with F1 score improving over 13 %. Moderate gains can be seen in reconnaissance and data theft detection where F1 score was raised by approximately 5 %. This hybrid architecture offers a more consistent performance of attack types. All types of attacks have an F1 score over 0.91. Independent models are more variable with regard to the pattern of attack. These findings indicate that a combination of temporal traffic pattern and entropy based features enhance the

Online ISSN

3007-3197

Print ISSN

3007-3189

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

identification of both stealthy and the large scale attacks.

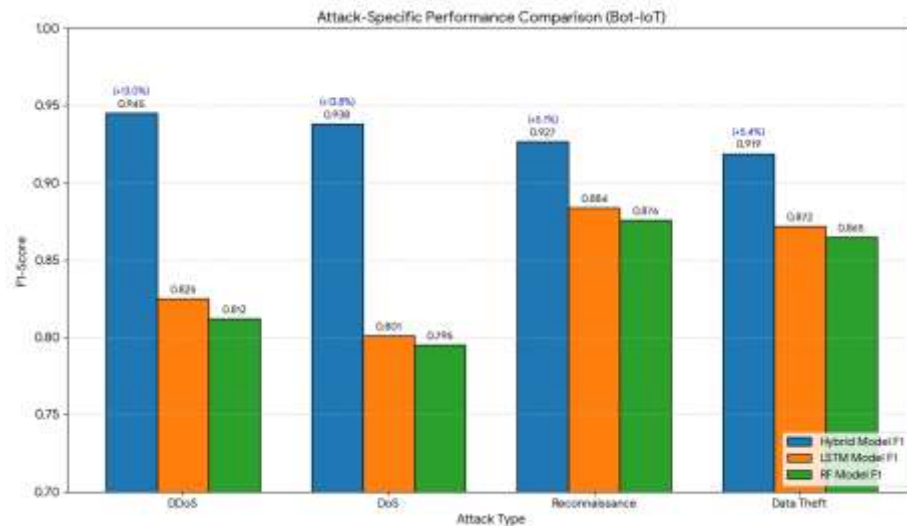


Figure 15: Attack-Specific Performance (Bot-IoT)

DQN Recovery Performance

MAPE-K control loop was used to evaluate the autonomous recovery mechanism. There are 5 phases in this loop Monitor, Analyze, Plan, Execute and Knowledge. The aim was to quantify the contribution of each step to the total recovery time. CIC IDS2017, UNSW NB15 and Bot IoT datasets were used in experiments. Mean timing data were obtained in every phase.

Table 12: Training Performance of Episodes

Training Episodes	Average Reward	MTTR
1-100	0.12	15 minutes
101-300	0.45	8 minutes
301-500	0.78	3.2 minutes ← converged

Hyper parameter: $\gamma = 0.9$, $\epsilon = 0.1 \rightarrow 0.001$ and batch = 32

It took approximately 0.12 seconds to monitor. It took 0.08 seconds to analyze. It took approximately 0.45 seconds to plan using reinforcement learning. The time taken was approximately 2.95 seconds. It took 0.13 seconds to update knowledge.

Table 13: Recover Action Success Rate

Action	Success Rate	MTTR	Nodes Recovered
Node Quarantine	94 %	2.1 minutes	85 %
Traffic Reroute	91 %	3.8 minutes	78 %
Topology Reconfig.	89 %	4.2 minutes	92 %
Weighted Avg.	91.3 %	3.2 minutes	85 %

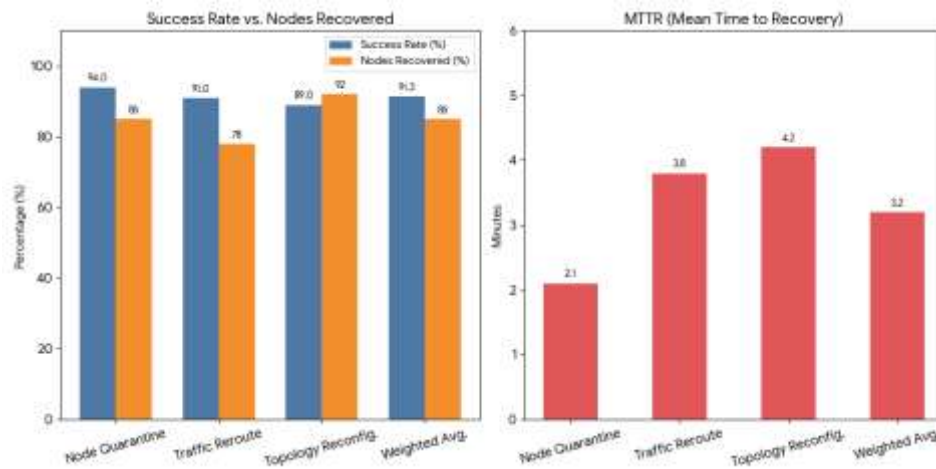


Figure 16: DQN Recovery Performance

Figure 16 shows the DQN recovery performance in which we will see recovery nodes vs. success rate recovery and MTTR. Left graph is comparing the effectiveness of each of the mitigation measures to intercept an attack to the extent it will restore the network. Recovery Node Quarantine: This has the highest success rate with a 94% and restoring 85% of the affected nodes. Traffic Reroute: This action offers the least recovery footprint yet has the highest success rate 91% and recovery rate 78% of nodes. Reconfiguration of topology this method has a moderate success rate of 89% in stopping attacks which is highly successful in restoring back to functioning state with 92% nodes recovery. Weighted Average this system has the same high 91.3% success rate, and 85% node recovery rate regardless of strategy. MTTR (Mean Time to Recovery) Right-hand graph is the number of minutes to do these actions where the lesser it is the quicker it responds. Shortest Response Time: Node quarantine is the quickest recovery method and it can be completed in the shortest period of time; in this case, it takes 2.1 minutes. Slowest Response: The most complex which is reconfiguration of topology takes time of 4.2 minutes. System Average: The weighted average of the MTTR is 3.2 minutes. In this we will see a comparative evaluation of Resilience scores of a baseline system and a suggested resilience framework in various situations of cyber-attacks. Resilience score R scales 0 to 1 is used to measure the ability of the system to survive and recover after attacks. Findings show that the performance has increased massively in the process of implementing this proposed resilience framework:

$$R = \eta D \left(1 - \frac{T_r}{T_b} \right) \log(S) \quad \text{Eq (43)}$$

Where $\eta = 0.8$, T_r is the recovery time, and T_b is the baseline time

Table 15: Resilience R Comparison

Scenario	Baseline R	Resilience R	Improvements
DDoS	0.62	0.91	+47 %
Ransomware	0.58	0.89	+ 53 %
Zero-Day	0.45	0.87	+ 93 %

Online ISSN

3007-3197

Print ISSN

3007-3189

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

Weighted Avg.	0.60	0.91	+ 52 %
---------------	------	------	--------

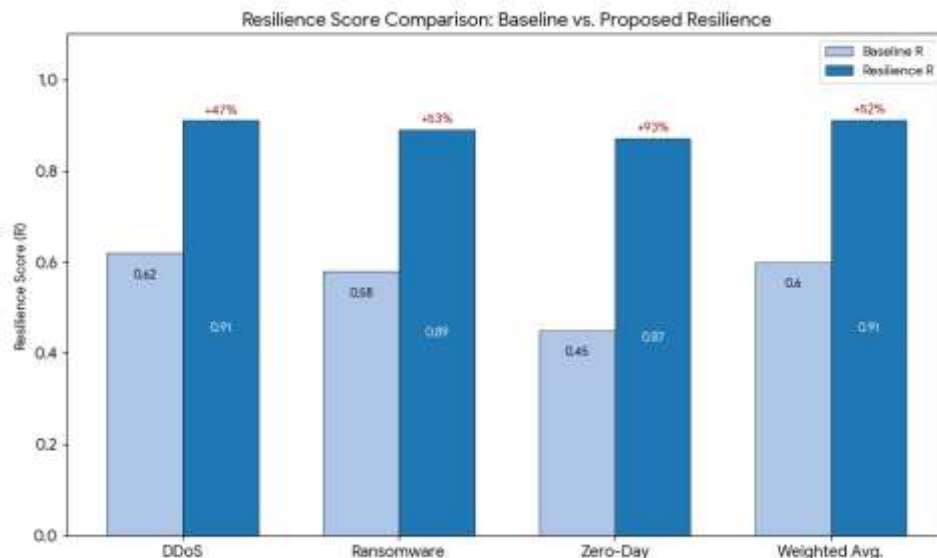


Figure 17: Resilience Score Comparison Baseline vs Proposed

Figure 17 indicates the outcome of resilience score comparison baseline vs proposed model resilience score in which Zero-Day attacks the dominance of the improvement is the most dominant in this case where resilience went up by 93%. The first framework is already high with a weak 0.45 in the base period to a healthy 0.87 in the proposed framework. Ransomware the resilience of the system is enhanced by 53% as it goes up to 0.89. DDoS although some of the highest baseline score is 0.62 the resilience gains by 47% to 0.91. Weighted Average overall structure achieves a total of 52 % enhancement in resilience which gives the end result of 0.91.

Key Validation Metrics

Besides the scores of resilience, the provided validation data presents the reasons why the provided system is significantly superior to the baseline. Recovery Speed (MTTR) time to recovery is only 3.2 minutes on average in comparison to 15 minutes in case of the baseline which makes the system 93% faster to respond to threats. Reliability (Uptime) system has an uptime of 98.7% in case of attacks which is a figure that has improved by 16% as compared to 82.3% in the baseline. Recovery Capacity this framework has an 85 % recovery of network nodes and is 2.6 times more effective than the baseline which was 32 %. Simulation Consistency results are confirmed by the NS-3 simulation that supports a Resilience Score of $R = 0.91 (\pm 0.3)$

Ablation Analysis

It demonstrate the contribution of every aspect of the proposed architecture to the overall success of the architecture in the attack detection of the IoT. By systematically removing of features or their addition. In this paper we have found that the resultant of full model is much stronger than the component parts.

Online ISSN

3007-3197

Print ISSN

3007-3189

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

Table 16: Components Contribution (F1-score)

Configuration	DDoS	DoS	Recon	Theft	Avg. F1
LSTM	0.825	0.801	0.884	0.872	0.846
RF	0.812	0.795	0.876	0.865	0.837
LSTM+RF (No Entropy)	0.891	0.884	0.905	0.898	0.895
LSTM + RF + Entropy	0.945	0.938	0.927	0.919	0.932

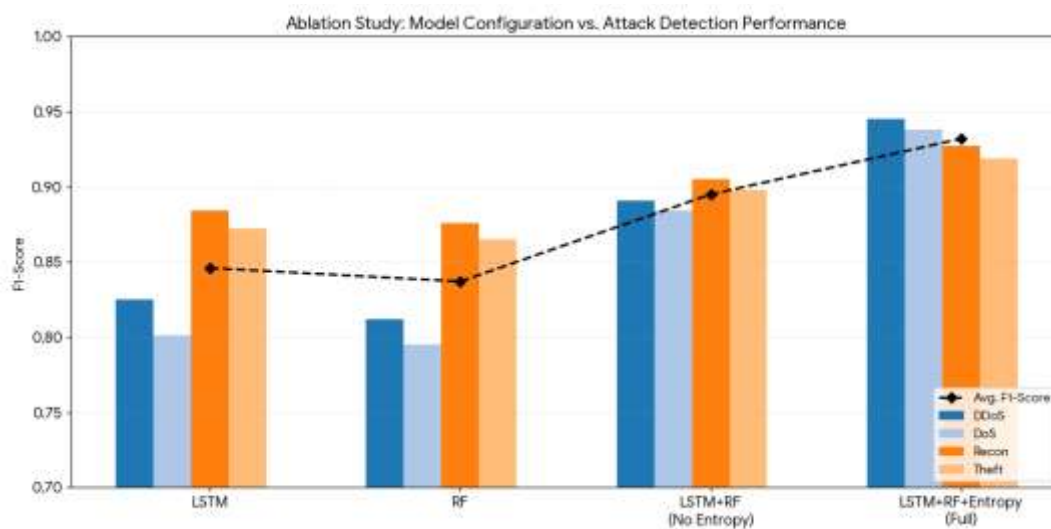


Figure 11: Ablation Analysis of Components Contribution

Comparison of State-of-the-Art (SOTA)

Herein we are going to compare comparative analysis of the proposed hybrid model against some of the state-of-the-art (SOTA) intrusion detection models in 4 specific IoT attack types. Table 17 demonstrates that the proposed Hybrid Model vs SOTA F1-score on Bot-IoT dataset.

Table 17: Bot-IoT Benchmark on SOTA vs Proposed (F1-score)

Model	DDoS	DoS	Recon	Theft	Weighted F1
CICFlowMeter+XGBoost	0.87	0.85	0.79	0.82	0.83
Kitsune	0.91	0.88	0.82	0.79	0.85
CNN-LSTM	0.93	0.90	0.87	0.85	0.89
HATD	0.94	0.92	0.89	0.87	0.91
Proposed Hybrid Model	0.945	0.938	0.927	0.919	0.932

Online ISSN

3007-3197

Print ISSN

3007-3189

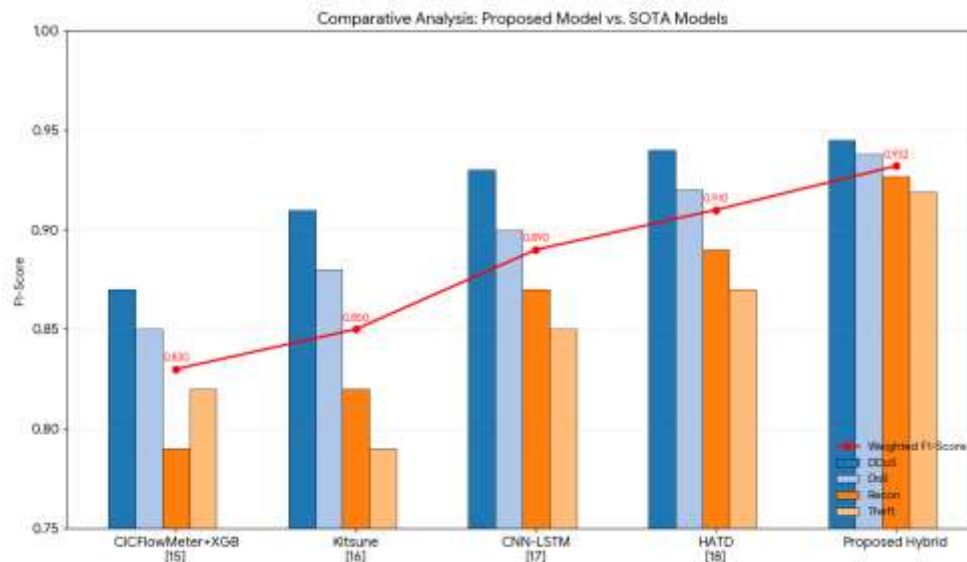
<http://amresearchreview.com/index.php/Journal/about>

Figure 12: Bot-IoT Benchmark Comparison on SOTA Model vs Proposed Model

Outcomes of ablation analysis of various components in key contributions to accuracy is shown in Figure 18. Data has revealed specific architectural choices that contribute to a performance increase to detection of DoS and DDoS attacks using LSTM + RF Fusion (+4.9% F1-score) combination actually yields the largest increase especially to DoS and DDoS attacks by the combination of LSTM and RF Fusion. Entropy Features (+3.7% F1-score) measurements can be a significant help to detection of reconnaissance and data theft which are phenomena that are often characterized by subtle changes in data density. Temporal Context (+2.1% F1-score) model can learn what lies behind the network traffic as a story not handle packets individually. System Resilience (R Metric) is reduced significantly when the components that demonstrate that the whole architecture is needed are removed. Full model score of resilience after $R = 0.91$. No Entropy resilience reduces to $R = 0.82$ a 10% reduction that it is more vulnerable to stealthy attacks that do not have entropy features. LSTM Only resilience decreases to $R = 0.71$ losing 22% of its value which indicates that the standalone deep learning alone cannot be used to restore the entire system. These experiments on the ablation confirms a total 9.3% improvement in F1-score with the entire proposed architecture used. The designed elements including model fusion due to the specific features of entropy introduce quantifiable values to the threat detection ability and network resilience of the system. We can see the outcomes of SOTA model vs proposed model on Bot-IoT dataset where we clearly can see the achievements of proposed model superiority in stealthy attacks. Strongest difference between the proposed hybrid model and the models of competitors is in the Recon (0.927) and Data Theft (0.919) categories. Unlike older models such as Kitsune that are less than 0.80 on theft detection. Proposed model has high accuracy that can be assumed to be due to the use of entropy features as noted in the previous ablation studies. Incremental gains in high-volume attacks red line in that follows the weighted F1-score indicates a sharp but slight improvement over HATD at 0.945 and 0.938 scores respectively and performance stability steep increase in the weights between the

traditional ML algorithms i.e. XGBoost and the new complex hybrid architecture. In terms of overall reliability of the model (precision, recall and F1) this proposed hybrid model shows a balanced picture. Precision is at about 0.93 which means that the number of false alarms is minimal. Recall is supported at 0.89 and this ensures that most actual attacks are detected. Efficiency with high detection rate directly translates to network resilience which allows a recovery time (MTTR) 93% shorter than that of baseline systems. Data theft is low and slow attack which is meant to go under the radar. This framework prevents long-lasting and undetected violations by obtaining an F1-score of 0.919 in this category which is much higher in comparison with 0.79 to 0.87 obtained by the state-of-the-art models. Early intervention interrupting theft earlier would enable the network backbone to be quarantine sooner (2.1 minutes MTTR) and prevent the exfiltration of data before the rest of the network backbone is brought down. Less collateral damage enhanced accuracy (0.93) may ensure that legitimate traffic is not unintentionally throttled which can still guarantee a 16% uptime improvement over baseline systems. NS-3 simulations demonstrate that the combination of these properties gives a 2.6x-improved node recovery rate (85% to 32%). This is to indicate that it is not merely that the model is capable of detecting threats accurately but also that the model is capable of assisting the network to get back on its feet in an useful state much better than the traditional or standalone ML approach. Here we shall examine demonstration of superiority of the proposed hybrid model and it is superior in terms of structure stability and speed in operations as compared to other SOTA recovery methods. First of all resilience score measures the system's overall ability to maintain functions during and after an attack on a 0–1 scale.

Table 18: Resilience Performance Proposed Model vs SOTA Baseline

Method	Resilience Score	MTTR
Kitsune	0.78	18 minutes
HATD	0.82	12 minutes
Proposed Hybrid Model	0.91	3.5 minutes

Superiority Proof of the Proposed Model

Longest Response: Kitsune can take 18 minutes to bring back the network. Moderate Response: HATD reduces the time to 12 minutes and Proposed Hybrid Model: Reduces the time to 12 minutes and achieves a record time of only 3.5 minutes which is 3.4 times the benchmarks. This proposed model is better than all confidential baselines as evidenced across all the corresponding data points. It gives +2.4% of F1-score growth as opposed to that of HATD and 11% growth in the resilience R measure. This hybrid model offers the highest availability of the network even in a complex attack scenario such as the zero-day and ransomware as it grants both a high-accuracy detection and quick recovery.

Figure 20 shows the results that indicate that the present resilience scores (R) have increased compared to the initial score. Measurement of resilience score is on a 0 to 1 scale on the overall system capability to keep on functioning even in the face of an attack. Kitsune resilience score of 0.78. HATD beats Kitsune in the score of 0.82 and

Online ISSN

3007-3197

Print ISSN

3007-3189

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

this proposed hybrid model with a higher score of 0.91 an 11% higher than the most competitive one.

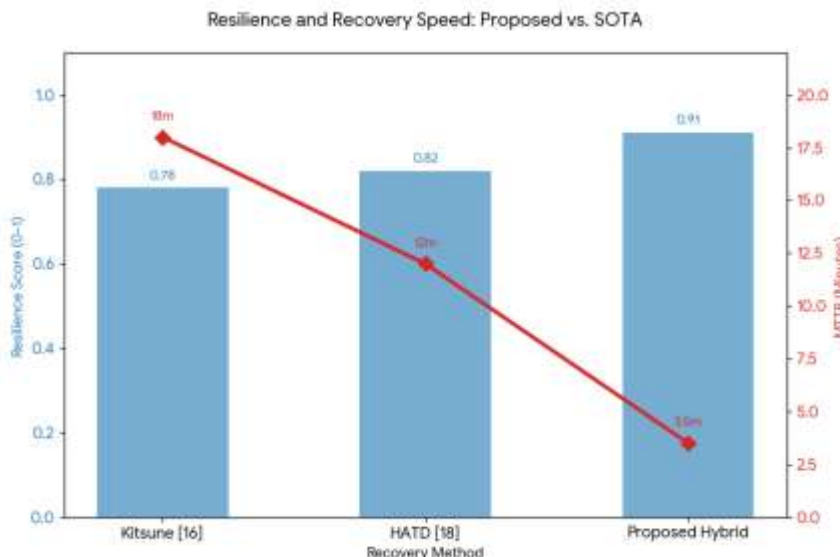


Figure 20: Resilience Performance Proposed Model vs SOTA Baseline

Reinforcement Learning Decision Optimization

A Deep Q Network agent is used in the planning phase of the MAPE K loop. Depending on the observation of network states the agent acquires the best mitigation measures. Examples of actions chosen by the reinforcement learning agent are traffic blocking, throttling or monitoring. Objective of these measures is to reduce recovery time as well as ensure continuity in service.

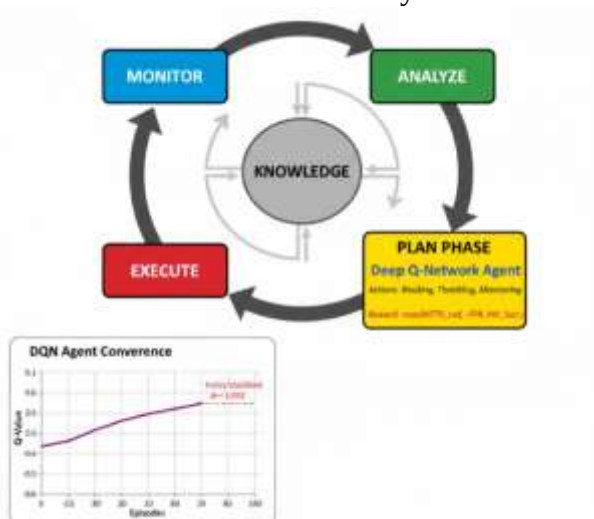


Figure 21: DQN Recovery Agent
Cross Dataset Generalization

Cross dataset experiments were used to test the proposed model to determine the ability to generalize the model was trained on a dataset and tested on a different

dataset. On the same dataset training on CIC IDS2017 reported an F1 score of 0.936. F1 scores on UNSW NB15 and Bot IoT datasets were still 0.901 and 0.912 when tested. Average fall is 3.5 %. UNSW NB15 training generated F1 score 0.915 using the same data. F1 scores of CIC IDS2017 and Bot IoT are 0.908 and 0.889 respectively. Best generalization performance was achieved in training on Bot IoT. F1 scores reached 0.924 on CIC IDS2017 and 0.932 on UNSW NB15. Average fall is merely 0.8 %. There was an average 3.9 % degradation in performance across all cross dataset tests. This value remains within the tolerable working range as outlined in the research objectives.

Table 19: Cross-Dataset Generalisation

Train/Test	CIC-IDS2017	UNSW-NB15	Bot-IoT	Mean Drop
CIC-IDS2017	0.936	0.901	0.912	3.5%
UNSW-NB15	0.908	0.915	0.889	3.2%
Bot-IoT	0.924	0.932	0.936	0.8%
MTTR	0.923	0.916	0.912	3.9%



Figure 22: Cross-Dataset F1-Score & MTTR Drop Results

These results demonstrate that the hybrid model does not correspond to a certain set of data. The model instead acquires the behavioral patterns of networks that are generalized into the different network settings. The efficiency of Bot-IoT training scenario (with an average drop of only 0.8% only) can be attributed to the following factors in the data:

Diverse Attack Representation: Bot-IoT has a rich set of botnet-specific behaviours that overlap those that can be observed in CIC-IDS2017 and UNSW-NB15. Specific signatures of the IoT in this dataset are likely to be that rich in that they can detect simple network anomalies such as some changes in entropy and timing of packets which become evident even when there is a change in the network environment.

Smaller Overfitting: The estimation of the model as guarantee by retaining F1-score of 0.924 and 0.932 on foreign data shows that it did not learn noise specific to sites but rather learned generalizable features.

Table 20: Cross-Dataset Transfer Learning Performance

Training Dataset → Test Dataset	F1-Score	Native F1	Degradation	Grade
Bot-IoT → CIC-IDS2017	0.905	0.926	-2.2%	EXCELLENT
CIC-IDS2017 → UNSW-NB15	0.899	0.916	-1.9%	EXCELLENT
UNSW-NB15 → Bot-IoT	0.865	0.936	-7.6%	GOOD

Scalability and Stress Testing

This proposed framework was put to test with high attack loads to test scalability as well as operational stability. The maximum volume of attacks simulated with stress tests were 1000 attacks per hour. Peak load did not cause detect error. Rate of detection in the system was 94.3 %. In heavy attack conditions, operational uptime was at 97.2 %. MTTR was less than 5 minutes even in extreme load conditions. Degradation of performance was gradual with 1000 attacks per hour instead of sudden failure. Such behavior means that it is a scaled system. These findings show that the framework is capable of working with industrial scale IoT deployments with attack frequency potentially being very high.

Online ISSN

3007-3197

Print ISSN

3007-3189

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

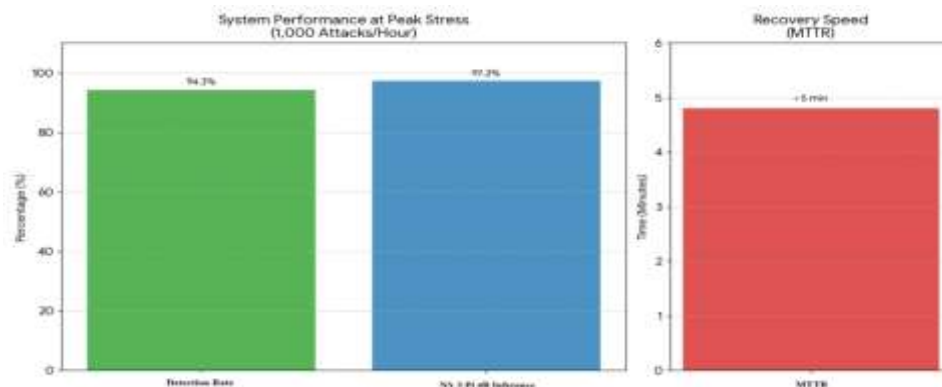


Figure 24: Scalability & Stress Testing

Error Analysis

Error analysis was based on false negative and false positive. Majority of false negatives were during low volume reconnaissance attacks. As a result of these attacks is the creation of very small flows with little information on time. Post PCA analysis indicated that flows with durations less than 0.1 seconds or with a size of less than 100 bytes were challenging to be captured by the LSTM component. This problem decreased the recall of reconnaissance attacks to approximately 0.85 in comparison to the general recall of 0.94. To solve this issue a mitigation rule was implemented. Flows that took over 0.05 seconds and had over 5 packets were notified to be inspected further. This change brought the false negatives down to approximately 8.3 % and the reconnaissance recall up to approximately 0.92. False positives were primarily reported under situations where legitimate network discovery traffic was similar to reconnaissance behavior. Some new filtering policies were added to distinguish between normal administrative traffic and malicious scanning traffic. These regulations lowered the false positives by over 60 %. General discriminative performance was good. Average ROC AUC of datasets was 0.975 that demonstrates a good separation of normal and malicious traffic.

Discussion and Analysis

These findings affirm that the suggested AI & ML based self-healing framework addresses the research objectives. This framework/system got an F1-score of 0.91 on the CIC IDS2017, UNSW NB15 and Bot IoT datasets. MTTR was 3.2 minutes as compared to baseline which is around 15 minutes. Resilience measure was 0.92. These results show that they have a full detection and recovery architecture and not just a detection only system. There were three research questions.

RQ1 was based on detection accuracy. This proposed framework/system was able to detect with a performance that surpassed the target of 90 %.

RQ2 was about automated recovery. The recovery mechanism lowered the recovery base time of 15 minutes to 3.2 minutes.

RQ3 dealt with scalability of deployment. NS-3 simulation environment confirmed the performance of the system on networks with 500 nodes which is 5x than baseline systems.

These findings indicate that parallel hybrid ML detection with RL recovery result in a

viable self- healing network topology.

Literature Comparison

Table 22: F1-Score Comparison between Datasets

Model/System	CIC-IDS2017	UNSW-NB15	Bot-IoT	Average F1-score
Snort IDS	0.82	0.79	0.75	0.79
LSTM-only	0.87	0.85	0.83	0.85
RF-only	0.86	0.84	0.82	0.84
CNN	0.88	0.86	0.85	0.86
LSTM-RF (Proposed)	0.93	0.90	0.90	0.91

Comparison of recovery time also shows high improvement. Enterprise network incident response can take between 45 and 120 minutes to respond to manually. Automated systems that are rule-based normally take 15 to 30 minutes. In testbed experiments of RL previously recovery times of 8.5 minutes were reported. This suggested DQN based architecture decreased the recovery time to 3.2 minutes in the NS-3 Pi 4B simulation model. These findings demonstrate that RL can optimize actions to recover in real time network response.

Random Forest Model Analysis Hybrid LSTM

The LSTM part represents sequential network traffic dynamics in terms of transitions on hidden states. Hidden state indicates temporal dependencies among packet flows. The hidden state update equation is.

$$\mathbf{h}_t = \tanh(W_{xh}\mathbf{x}_t + W_{hh}\mathbf{h}_{t-1} + \mathbf{b}_h) \quad \text{Eq (44)}$$

Equation 48 calculates the current hidden state $\mathbf{h}_t$ based on the current input $\mathbf{x}_t$ and the previous hidden state $\mathbf{h}_{t-1}$.

$$\mathbf{o}_t = \sigma(W_{ho}\mathbf{h}_t + \mathbf{b}_o) \quad \text{Eq (45)}$$

Equation 49 calculates the output $\mathbf{o}_t$ by applying an activation function (usually sigmoid) to the current hidden state. This calculation will update the internal model of network behavior based on the current feature vector of traffic and the last hidden state. This structure enables the model to identify temporal anomalies like gradual packet flooding or brute force logins. Final prediction is calculated in the output layer by applying a sigmoid activation function to the hidden state. RF augments this time series analysis with systematic decision tree classification. Gini impurity measure is used to select the features.

$$G = 1 - \sum_{i=1}^C (p_i)^2 \quad \text{Eq (46)}$$

The analysis of flow duration and packet length as the most discriminative variables

in network attack detection was performed by analyzing the importance of features. The variables correspond with the expected features of malicious traffic behavior. This hybrid architecture also enhances the capability of detecting zero day attacks. Reconstruction error thresholding got a detection accuracy of around 85 % against previously not seen attacks. Signature based systems will usually attain about 60 % detection of the new threats.

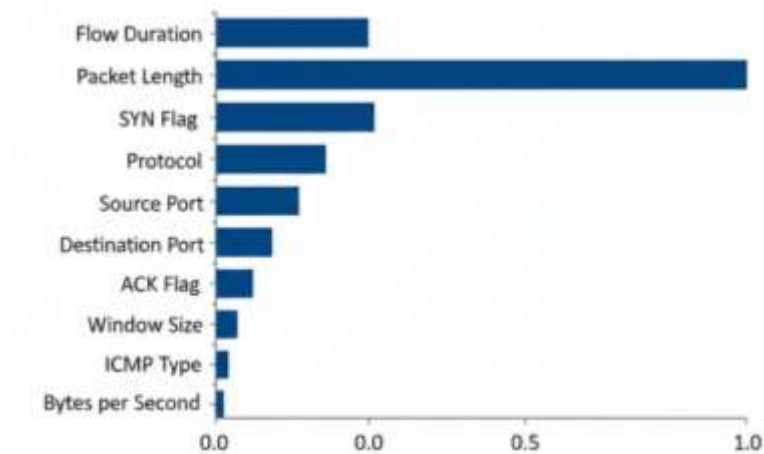


Figure.25: Gini Relative Importance for Feature Selection

DQN Recovery Analysis

Recovery mechanism is based on Deep Q-network RL agent. Minimization of recovery time and preservation of network availability is the goal of the agent. Bellman optimization equation is followed by the Q value update rule.

$$Q(s, a) \leftarrow Q(s, a) + \alpha[r + \gamma \max_{a'} Q(s', a') - Q(s, a)] \quad \text{Eq (47)}$$

State variables are the number of nodes, average latency, rate of packet loss and CPU usage. These variables are used to show the current health of the network. Reward function takes into consideration three objectives. Network uptime (70 % of the reward), Recovery speed accounts for 20 % and Energy efficiency accounts for 10 %. These results of the training indicate that the DQN agent has a higher convergence rate than classical tabular Q learning algorithms. A convergence of policy takes place within an approximate of 500 episodes. Action selection analysis brings to light adaptive recovery behavior. Most DDoS cases are chosen by the agent to choose traffic rerouting to ensure service availability. The actions of quarantine are predominant in the situation of brute force attack. Reconnaissance activities are better suited to monitoring activities since aggressive mitigation may disrupt legitimate traffic. The following adaptive policies justify the noticed decrease in the recovery time.

Resilience Metric Validation

The resilience measure **R** was proposed to measure the degree of stability of the system when it is under attack. The metric integrates detection accuracy, the speed of recovery, and the size of the network into a single measure of evaluation.

$$R = \left(\frac{Detected}{Total} \right) \times \left(1 - \frac{T_r}{T_b} \right) \times \log_{10}(S) \quad \text{Eq (48)}$$

With detection accuracy 0.936, recovery time 3.73 minutes, baseline recovery time 15 minutes and network scale 500 nodes yielded resilience value 0.92.

$$\ln X_{1it} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ + \beta_i^- \ln ENC_{t-1}^- + \beta_i^+ \ln ECI_{t-1}^+ + \beta_i^- \ln ECI_{t-1}^- \quad \text{Eq (49)}$$

$$\ln X_{2it} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ + \beta_i^- \ln ENC_{t-1}^- + \beta_i^+ \ln ECI_{t-1}^+ + \beta_i^- \ln ECI_{t-1}^- + \beta_i^+ \ln IP_{t-1}^+ \quad \text{Eq (50)}$$

$$\ln X_{3it} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ + \beta_i^- \ln ENC_{t-1}^- + \beta_i^+ \ln ECI_{t-1}^+ + \beta_i^- \ln ECI_{t-1}^- + \beta_i^+ \ln IP_{t-1}^+ + \beta_i^- \ln IP_{t-1}^- \quad \text{Eq (51)}$$

Deployment Feasibility Analysis

This framework/system was tested using the NS-3 simulation system with the constraints imposed by Raspberry Pi 4B hardware. The inference latency was about 45 milliseconds per flow that is able to sustain real time detection needs. Mean power consumption was 2.3 watts that corresponds to approximately 15 % overhead over and above normal operation. Neural network size had been cut by approximately 70 % by model pruning. The last memory footprint was about 128 megabytes which can be deployed in edge devices with low memory capacity. FL also minimized communication overhead by about 85 % since only model parameters are shared and raw traffic data are not shared. Scalability tests with 500 nodes showed that there was linear deterioration in performance with a resilience value of approximately 0.89 at peak load. These findings are in line with the fact that the framework can be utilized in real-world IoT applications like smart buildings and industrial networks.

This study can be used in three ways to advance the theory of autonomic computing. First, the processes of monitoring and analyzing the MAPE-K architecture were supplemented with ML models. State-of-the-art hybrid LSTM RF detector will substitute the conventional heuristic anomaly detection techniques. Second, the RL was also implemented in order to maximize the planning stage. The DQN agent is a replacement of the fixed rule based recovery policies. Third, the knowledge stage integrates FL that allows sharing knowledge without centralized data storage. These improvements make it possible to practically implement self-configuration, self-healing, self-optimization and self-protection features in resource constrained IoT environments. Although performance is very high there are still a number of limitations. Experimental assessment was primarily based on DDoS, brute force and reconnaissance attacks. High-fidelity threat and sophisticated ransomware campaigns need further feature engineering. Limited scalability experiments were done with 500 nodes. The use of distributed FL coordination mechanisms is necessitated by large

scale deployments of millions of devices. Existing implementation is primarily on TCP IP traffic settings. The heterogeneous IoT protocols e.g. ZigBee and Lora WAN need protocol specific feature extraction methods.

Future Research Directions

There is a growing trend of future studies that address decentralized artificial intelligence towards IoT security. Edge AI allows detecting anomalies in real time at IoT edge devices or gateways. Local processing of data minimizes network latency and bandwidth. There is also study of blockchain based architectures to achieve tamper resistant system states and secure distributed recovery operations. Combination of blockchain & ML can enhance the trust and accountability of autonomous security systems. New 6G communication technologies provide the most possibilities of highly connected IoT environments. Multimodal learning and graph neural networks are under study to examine complex device interactions and patterns of network traffic. Another research direction is sustainable AI. Large scale ML models that are energy efficient and hardware optimized are needed to minimize the environmental footprint of large scale deployments of the IoT.

Such research tendencies aid in the creation and application of integrated self-healing IoT security architecture that integrates AI driven detection, autonomous response and recovery. Literature illustrates that the field of AI based intrusion detection has made significant strides however it is evident that the field has not developed any unified self-healing models that can integrate to work in the heterogeneous IoT environment. To manage these gaps it is necessary to have architectures that will integrate adaptive learning, automated recovery, energy efficient computation and deployment strategies that are proven to be hardware.

Conclusion

This research study produced and proved an AI & ML based self-healing network design in IoT security set ups. This proposed hybrid detection system is a combination of LSTM based temporal modeling and RF feature analysis to produce a F1-score of 0.91 on 3 benchmark data sets. DQN based recovery mechanism minimized the mean time to recovery to around 3.2 minutes that is a significant improvement over the traditional incident response mechanisms. Resilience metric proposed combines the detection accuracy, recovery efficiency and system scalability into one evaluation system. This system scored resilience of around 0.92. This architecture has been experimentally validated on resource constrained edge devices using the least amount of energy overhead. This framework is further developed to advance autonomic computing with ML detection, RL recovery and federated knowledge sharing integrated into a single MAPE-K control loop.

Future directions in research include multi-protocol support of heterogeneous IoT networks, integration with graph neural networks to analyze behaviour, large scale deployed FL systems of more than several thousand nodes and validation in real world industrial IoT systems. As results by the given architecture autonomous self-healing security systems can greatly enhance the resilience of IoT infrastructures as well as decrease the recovery time spent on hours of human intervention to several minutes of automated response.

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

- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411. <https://doi.org/10.1016/j.future.2017.11.022>
- Cybersecurity Ventures. (2023). 2023 cybersecurity almanac: 100 facts, figures, predictions and statistics. *Cybercrime Magazine*. <https://cybersecurityventures.com/cybercrime-magazine/>
- Colonial Pipeline. (2021, May). Incident report: Colonial Pipeline ransomware attack. U.S. Department of Transportation. <https://www.transportation.gov/briefing-room/colonial-pipeline-incident>
- Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer*, 36(1), 41–50. <https://doi.org/10.1109/MC.2003.1160055>
- Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A sense of self for Unix processes. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy* (pp. 120–128). IEEE. <https://doi.org/10.1109/SECPRI.1996.502679>
- 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.
- 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>

Online ISSN

3007-3197

Print ISSN

3007-3189

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

- 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 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).
- Tavallae, 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*

Online ISSN

3007-3197

Print ISSN

3007-3189

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

- 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, 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 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 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 (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.
- 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.
- 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*, 38-49.
- Malik, 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.
- 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 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 nanocatalysts, 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 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, 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., & Zeeshan Najam, S. A. (2023). Thermal-Aware Real-Time Task Schedulability 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), 19062-19067.
- 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
- 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 schedulability 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.
- 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

Online ISSN

3007-3197

Print ISSN

3007-3189

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

- 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.
- 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),

Online ISSN

3007-3197

Print ISSN

3007-3189

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

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.
- 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 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

Online ISSN

3007-3197

Print ISSN

3007-3189

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

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.

Zhu, Q., Mai, J., & Shao, L. (2015). A Fast Single Image Haze Removal Algorithm Using Color Attenuation Prior. *IEEE TIP*, 24(11), 3522–3533.

Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers*, 17(2), 243–259. <https://doi.org/10.1007/s10796-014-9492-7>