Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

An Intelligent Deep Learning Network based on Internet of Things (IoTs): An Enhanced Approach for Network Threat Mitigations, Techniques, Issues and Opportunities

Majid Ali
AITEEC- AI Technology Exchange and Engineering Consultancy, Lahore, Punjab, Pakistan Email: majidq67@gmail.com **(Corresponding Author)**
Samiullah Aftab
Department of Robotics, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan Email: 2005.m.farhan@gmail.com
Fasiha Ikram
Bahria University, Department of Computer Science, 13 Stadium Road, Karachi, Pakistan Email: fasiha.bukc@bahria.edu.pk & fasia.ikram@gmail.com
Ammar Ahmad
Department of Information Technology, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan Email: ammarahmed9917@gmail.com
Muhammad Saad Hamayoun
Department of Robotics, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan Email: saadhamayoun22@gmail.com
Farhan Zohaib
Department of Robotics, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan Email: 2005.m.farhan@gmail.com
Ali Hassan
Department of Robotics, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan Email: ah0772285@gmail.com
Ukasha Ejaz
Department of Robotics, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan Email: ejazukasha32@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

The Internet of Things (IoT) is among the most commonly utilized technologies nowadays, and it has a substantial impact on our lives in many different ways, including social, commercial, and economic ways. Regarding automation, productivity, as well as the comfort of consumers in diverse application segments, including education and smart cities, the current and future IoT technologies promise significant advancement in the overall human life quality. Nevertheless, cyber-attacks and threats have a significant impact on smart applications in the context of the IoT. The conventional IoT security approaches would not suffice, considering the current security issues in light of the advanced burgeoning of various forms of attacks and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

threats. The solution to providing an updated and dynamic security system to the next-generation IoT system is to deploy the artificial intelligence (AI) expertise and, specifically, machine, and deep learning solutions. In the entire article, we show a comprehensive image of IoT security intelligence that is constructed on machine and deep learning technologies that can extract insights from raw data in order to intelligently defend against numerous cyber-attacks on the Internet of Things. Lastly, in line with our research, we bring out the research issues and future directions based on our research. On the whole, the article aims to become a reference point and guide, especially on the technical level, to cybersecurity experts and researchers operating in the field of IoT.

Keywords

Internet of Things (IoT), Deep learning, Convolutional neural network, Recurrent neural network, Long short-term memory

INTRODUCTION:

The Internet of Things (IoT) stands among the most popular technologies nowadays and is commonly referred to as a network of heterogeneous elements that are capable of creating smart systems and services detecting, acquiring, disseminating, and analyzing data [1]. Things in the IoT devices are those smart devices, which are sensors, smart watches, smart refrigerators, smoke readers, radio frequency identification (RFID), heartbeat, accelerometers, smart phones, etc, which gather and send data [2]. IoT systems are growing daily in the number of interrelated things. As an example, the number of connected things in the world will reach approximately 20.4 billion in 2022, as compared to 8.4 billion connected things in 2020 [3, 4]. The IoT has a profound impact on our lives in a diversity of ways, such as social, commercial and economic. The IoT market is expected to expand its revenues by 892 billion in 2018 and reach 4 trillion in 2025 in terms of the development of the digital economy [5, 6].

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

The IoT facilitates massive technological development and value-added services across many sectors of our lives, such as smart homes, smart cities, transportation, logistics, smart health, retail, agriculture, and business, smart metering, remote monitoring, and automation of processes [7, 8]. Currently and in the future, IoT applications and services have enormous potential in changing the consumer quality of life in terms of automation, performance, and comfort. Nonetheless, when considering IoT, various types of cyber-attacks and threats are considered problematic to the growth of the IoT [9, 10].

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

This paper is thus based on IoT security intelligence to ensure that systems and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

applications are well safeguarded against various cyber-attacks and threats in the IoT [11, 12]. The simplest requirement in the IoT network is the security of all the systems, applications, and devices connected to the system. The huge scale of IoT networks presents a host of issues in numerous domains such as device management, data management, computing, security, and privacy, among others [13, 14]. With the expansion of the IoT, different security issues are being raised as potential threats. The new IoT applications, including the above-mentioned, will not be in a position to fulfill the needs of people and society and they will not get all the potential when there is no trusted system in place [15, 16]. The IoT systems are usually based on multiple layers, such as the perception or sensing layer, the networking and data communication layer, the middleware or support layer, and the application layer [17, 18]. Section 3 gives a very fleeting discussion of these layers. To every layer, there is a certain set of tasks and applicable technologies to do in an IoT application, and with each layer comes new issues and security concerns [19, 20]. ELU – E- Linear Unit with $0 < \alpha$ is

$$f(x) = \begin{cases} \alpha(\exp(x) - 1) & \text{for } x < 0 \\ x \text{ for} & x \geq 0 \end{cases} \quad \text{Eq (3)}$$

Latest Statistics About IoT and Denial of Service (DoS) Attacks

To illustrate, the most prevalent IoT attacks are denial of service (DoS) attacks, spoofing attacks, jamming, eavesdropping, data tampering, man in the center attacks, malicious, and others [21]. Therefore, based on the type of security concerns, possible IoT security measures, including authentication, access control, threat and risk forecasting, malware analysis, anomaly or intrusion detection, prevention, etc, would be applicable [22, 23]. The traditional methods of addressing security incidents have ceased to work due to the development of high levels of boom in security threats and attacks, and the complexity in security incidents. As such, a smart security system that is grounded on the latest technologies and can deal with these security issues is highly demanded to ensure the security of the next-generation IoT system [24, 25].

One of the most crucial technologies is Artificial Intelligence (AI) in creating intelligent systems, and it is deemed as a component of the Fourth Industrial Revolution (4IR) [27, 28] as well. Therefore, with the use of AI expertise, especially machine and deep learning, we will be able to identify anomalies or unwanted malicious behavior in the IoT, and, consequently, provide a dynamic security solution, which is continuously enhanced and updated [29, 30]. Usually, machine or deep-learning models are a collection of rules or techniques or intricate transfer functions that derive valuable knowledge or interesting data patterns out of the security data [31, 32].

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

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

In this way, one can use the ensuing security models to condition the machines to anticipate threats or risks early on, or detect the abnormality in the IoT to create a required defensive policy [33].

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

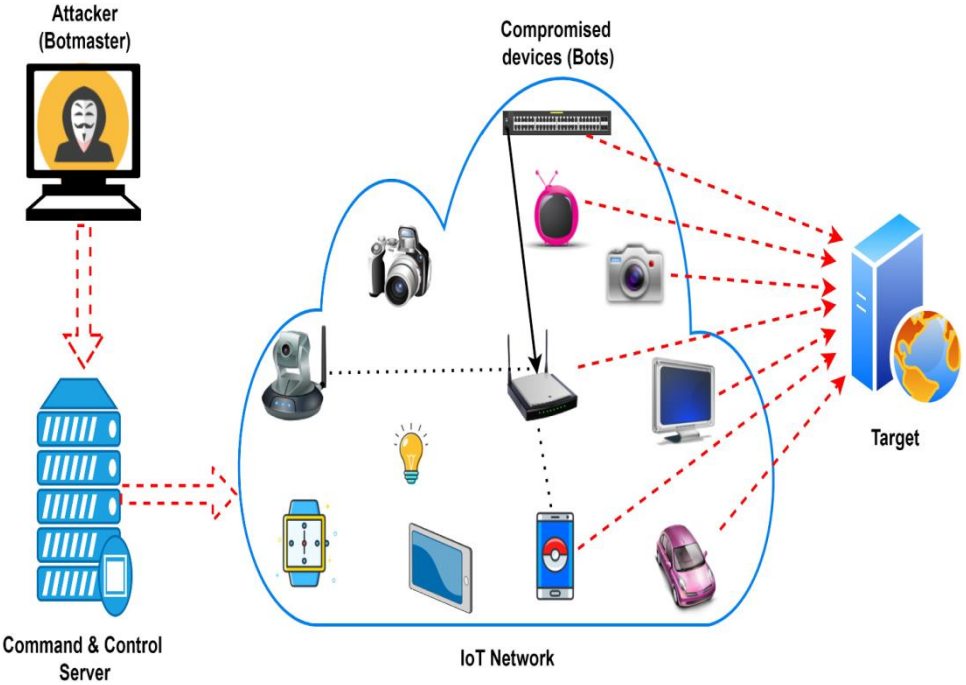


Figure 1: Configuration Hierarchy for Mitigating Attacks using IoT Devices [34]

Internet of Things (IoTs) and M2M Standards

One of the recent smart technologies in the Fourth Industrial Revolution (or Industry 4.0), indicating the continuation of the automation of traditional manufacturing and industrial practices, is the Internet of Things (IoT) [34, 35]. In M2M standards cybersecurityhas many renowned techniques UNSW-NB15 [36, 37], CAIDA [38, 39], ISOT10 [40, 41], ISCX12 [42, 43], CTU-13 [44, 45], CIC-IDS [46, 47], CIC-DDoS2019 [48, 49]. The IoT is a collection of internet-connected and interconnected devices that can gather and transmit data on a wireless network without the involvement of human operators. Several organizations and research groups define IoT and smart environment in several different ways and perspectives. As an example, [50, 51] describe the IoT as an item of hardware and a digital information stream grounded on RFID tags. According to the Institute of Electrical and Electronics Engineers (IEEE), the IoT is something that is described as a mixture of things that have sensors and make a network linked to the Internet [52, 53]. European Telecommunications Standards Institute (ETSI) defines machine-to-machine (M2M) communications as a type of automated system of communications performing

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

decisions and data operations without the direct involvement of human operators [54, 55]. Cisco, as the global leader in IT, networking, and cybersecurity solutions, has simplified the concept of the IoE (Internet-of-everything) as a network of people, data, things, and processes [56].

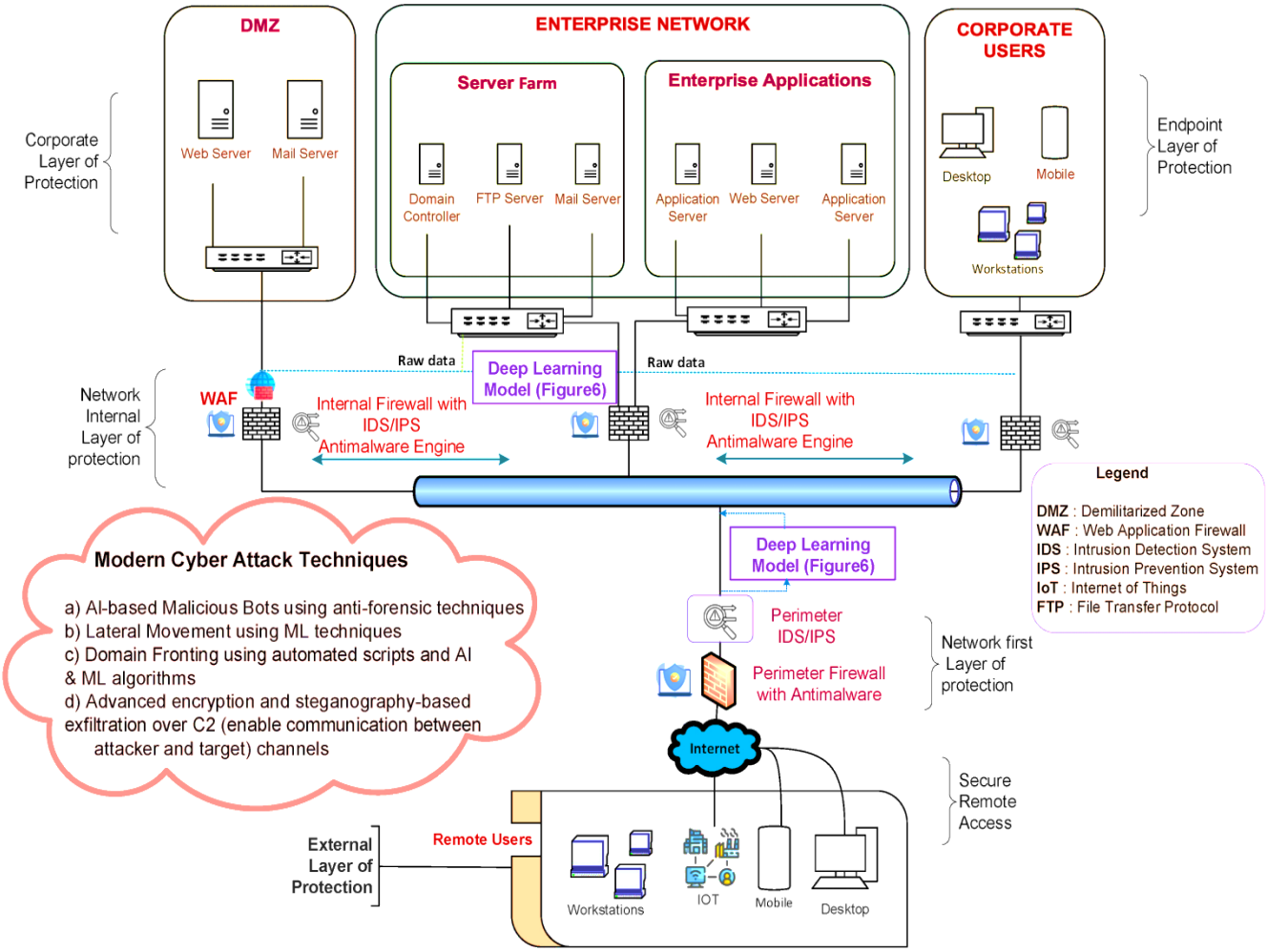


Figure 2: Generic Network Architecture Mitigating Attacks using Deep Learning Architecture [57]

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

According to the RFID (Radio Frequency Identification) group, the IoT is the global cyberspace of interconnected objects that can be addressed uniquely in accordance with standard communication protocols [57, 58]. As stated by Cluster of European research projects on the IoT [59] - Things are active participants in business, information and social processes in which they are facilitated to interact and communicate with each other and with the environment by exchanging data and information sensed about the environment and by responding autonomously to the real/physical world events and influencing it by running processes that cause actions

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

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

and create services with or without human intervention [60, 61].

Authors in [62] refer to the interconnection of actuating and sensing devices as IoT, which offers the capability to exchange information across platforms using a single framework, creating a common operating picture to facilitate novel applications. According to [63], IoT is described in three paradigms, including internet-oriented (middleware), things-oriented (sensors), and semantic-oriented (knowledge).

$$R^2 = 1 - \frac{\sum_{i=1}^{n}\left(Y_i - \widehat{Y}_i\right)^2}{\sum_{i=1}^{n}(Y_1 - \overline{Y})^2} \qquad \text{Eq (7)}$$

In [64], the authors introduce a number of research challenges and opportunities associated with IoT security, and in that case, they have taken into account the overall security background of the IoT. In [65], the current situation in the field of IoT security studies, including the related tools, such as IoT modelers and simulators, was outlined. The authors in [66, 67] give a summary of the concept of security, technological issues, security issues, practical solutions, and future research that can be done to protect the IoT. In their survey, they provide their analysis of the current state and the problems of IoT security, considering three layers of architecture, which include the perception layer, the network layer, and the application layer. The survey on IoT security provided by the authors of [68] considers the domain of applications, security threats, and solution architecture. It has introduced a taxonomy on IoT vulnerabilities, attack vectors, attacks that take advantage of these vulnerabilities and methodologies to address them in [69, 70]. The authors in [71] provide a study on IoT security, and their particular study concentrates on the latest threats and vulnerabilities of IoT security as discovered through an extensive evaluation of the existing IoT security research.

Table 1: Comparative Analysis of Renowned Public Datasets for IoT Security

Dataset	**No. of features**	**No. of instances**	**Name of attacks**	**Separate train- test set**	Ref
BoTNet-IoT-L01	23	1,111,864	UDP, Scan, Syn, Ack, TCP, UDP plain, Combo, and Junk	Yes	[72]
NSL-KDD	42	148,517	DoS, Probe, R2L,and U2R	Yes	[73]
KDD99	42	4,886,431	DoS, Probe, R2L,and U2R	Yes	[74]
UNSW-NB15	49	1,540,044	DoS, Fuzzers, Backdoors, Worms, Reconnaissance, Analysis, Exploits,	Yes	[75]

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

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

			Generic, and Shellcode		
BoTNet-IoT-L01	23	1,111,864	UDP, Scan, Syn, Ack, TCP, UDP plain, Combo, and Junk	Yes	[76]

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2} \quad \text{Eq (8)}$$

$$Y(t) = \omega[\tau_{ho} * h(t)] \quad \text{Eq (9)}$$

In [74], the authors consider the security requirements, the attack vectors and other discussions related to computer learning in IoT networks. A survey of computer and deep learning methods of IoT security was introduced. The influence of IoT's new capabilities on protection and privacy in the light of emerging threats, the solutions and challenges that exist were discussed in [77].

$$\text{MCC} = \frac{\text{TP} * \text{TN} - \text{FP} * \text{FN})}{\sqrt{((\text{TP} + \text{FP}) * (\text{TP} + \text{FN}) * (\text{TN} + \text{FP}) * (\text{TN} + \text{FN}))}} \quad \text{Eq (10)}$$

To build data-driven security systems based on machine and deep learning methods, it is worth knowing the nature of data, as well as diverse types of cyber threats and characteristics associated with them. A number of these datasets are available in the field of cybersecurity. Therefore, we have summarized as NSL-KDD [78], UNSW-NB15 [79], DARPA [80, 81], CAIDA [82], ISOT10 [83, 84], ISCX12 [85, 86], CTU-13 [87, 88], CIC-IDS [89], CIC-DDoS2019 [90, 91], MAWI [92], ADFA IDS [93], CERT [94,] Depending on the domain of the problem, it is possible to construct the machine and deep learning based model using these datasets. As an example, a deep learning model of a neural network is employed to construct a model on intrusion detection using NSL-KDD [95]. The authors apply such NSL-KDD [96], UNSW-NB15 [97] and CIC-IDS [98] in [99] when testing their network intrusion detection model based on machine learning when applied to the IoT environment. Robotics is a very Emerging Field in the past few year's and it is now a part of almost every field, like Healthcare, Manufacturing, Warfare. Countries like China, Japan, US are very advanced in this field and global leaders in this field. So, every day we hear something new has been invented. So, this shows how fast the field of Robotics is growing and this growth is much higher in the coming future [98]. The Internet is also growing well and people use the Internet in different ways to solve their issues or problems like (Playing heavy games on the cloud) so people use internet in different ways. So, what if we also use it with robotics, means we operate a Robot with internet it can solve many problems of Humans. This is not just a thought it is really happening like (Doctor doing a remote surgery from one country to in another country) [99]. But controlling or operating a Robot with the internet or on a network

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

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

is not that easy it has some problems is well. Its biggest issues are Delay, Data Loss and Security Issues, which make this type of technology Unstable and Unsafe [100].

$$\omega = E_f * \frac{1}{1 + e^{-\theta t_f}} \quad \text{Eq (11)}$$

Intelligent Machines in the Network

This paper discusses and explains three control models and also has real-life examples is well. In this review paper, we will discuss those issues that people face when they operate a robot with internet and we will also discuss the method and technologies used in this research paper. We also discuss the Strengths and Weaknesses of the research. And what problems we face in this and how can we operate a robot on a network easily [101, 102]. This paper discusses problems and also explains how other researchers try to solve these problems and issues in the past. This paper also shows some real-world examples, which is give very clarity [103]. Those robots which are operate on the internet mainly have these four parts: Intelligent Mobile Robot, Server for a Robot, Web Server and End-devices (Computer/Laptops/Phones).

The user gives commands form an End-device and then the web server receives these commands and web server sends them to the Robot server, which give commands to the intelligent robot and the robot follows these commands and performs a given task. In this we have two servers because one deals with robot side and the other deals internet side, which is also the user side.

$$\omega = \left\{ \begin{array}{ll} 0; & normal \\ 0 < \omega < 0.25; & Mild \\ 0.25 < \omega, 05; & Moderate \\ 0.5 < \omega < 0.75; & Severe \\ 0.75 < \omega < 1; & Proliferative \end{array} \right\} \quad \text{Eq (12)}$$

Control Architectures and Time Delay

Time Delay is a very important issue that is discussed in this research paper. When we operate a robot on the internet, we face one big problem, which is a Time delay in simple words, this is called a lag. This lag and delay cause some big issues in this type of technology [104]. There are four types of different delay's which are discussed in this research paper. Delay in sensor Data, Delay in user decision, Delay in commands Transmission and Delay in Robot Actions.

Suppose a user needs a camera or sensor data from a robot to send next command but this will take time to reach data from the robot to user which cause a delay. When a user receives camera or sensor data and user will take some time, which will also cause a delay. Now the user sends a command to the robot but we all know that the network always takes some time to send a packet, which will again cause a delay.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

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

Eq (13)

Table 2: Analysis of renowned techniques used for network-based IoT

Ref	Aspect	Dataset	Network Architecture	Algorithm/Model Used
[105]	Response Time Reduction	Decreased from hours to seconds for incident response	Fast Decision Network	Twin Model
[106]	False Positive Rate Reduction	Reduction of 40-60% in false positives	Multi-Area Microgrid	QoS Model
[107]	Monitoring Availability	24/7 continuous monitoring of IoT devices and networks	Strategy Network	Auto-Regressive Moving Average with Exogenous Input Model

Delay in Robot Actions

Now the robot receives a command from the user but it also needs some time to perform an action so this will also cause a delay. Autonomy is a very important topic in robotics, which is discussed in this research paper. Autonomy means a smart robot means how much work a robot can done by itself, autonomy [108]. If a robot can do more work on it than this robot is smart and has high autonomy. A smart robot can think on its own and user only need to give command in simple English and rest is done my robot-like user say move 10m East so robot take this command and them its robot calculate 10m distance and find it's East on it on no more user interaction is need but on the other side a robot with low autonomy always relay on user it can't anything on its own [107, 108]. Now the question autonomy can do in a Networked Intelligent Robotic system so high autonomy can reduce the delay because when a robot can do a task on its own, then it is not always relay on user commands. Yes, this will not fully solve the problem but it will surely reduce the delay in Networked Intelligent Robotic systems [109, 110]. Now we have an idea how big a problem delays in Networked Intelligent Robotic systems but this delay becomes worse because the internet is unstable. Data that travels on the internet doesn't have a constant speed sometimes user commands reach the robot fast, sometimes slow so this make it more difficult to operate a robot on the internet [111, 112].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

$$\delta_s = \left(\frac{m_x - m_n}{m_n} \right)$$ Eq (14)

Data Loss in Networked-Based Intelligent Systems

Another problem which we faced in Networked Intelligent Robotic systems is Data loss the is also a very important and big issues just think you send a command to robot to move in your left for 2 meter but in its way some of its packets may loss for some reason and the command which reach to robot in move in your left just and the other part of a command which is distance is not reach to a robot due to a data loss just think how big issue is this just think a doctor which is currently is in UAE and he is performing a online surgery with Networked Intelligent Robot in some other country or city and he send command to a robot but due to data loss some data can't reach to robot and robot just receive a half command so just think what will happen next. So, this is a very big problem and also discuss in this research paper is well [113].

$$\delta_v = m_x(\beta_r, \beta_g \beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g \beta_b,)$$ Eq (15)

Discussed different types of problems like delay, data loss, security, user interface, and scalability but we get some main problems in all sections where they face Delay problem. Mainly, these delays authors discussed in the search paper. Total of delay time takes up to 11seconds and these delays increase the chance of data loss or data missing [114].

$$R(t) = \sum_{i=1}^{n} FI_i(t) * \tau_{ih} + [\tau_h * r_{i-1}]$$ Eq (16)

Servers that create a virtual channel between user and machine are smart systems that compensate for both delay and data loss automatically. It performs several solutions which solve the problem of delay and missing packets. Receive operator command through web server. Robot server help to process commands. VC (virtual channel). Store command when network slow or predict movement. Its fixed delay problem. Resend loss data packet using TCP/IP. In reality case, Ball-catching system [123]. The robot server predicts the ball position even if some camera packets are lost, allowing the robot to catch successfully. Because TCP /Ip protocol check if every packet arrives or not. If not then it resends the missing packets until successfully arrived. And it shows predicted video instead of delay video which also help to solve the problem of delay [124].

$$Y(t) = \omega[\tau_{ho} * h(t)]$$ Eq (17)

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Table 3: Analysis of renowned Model Networks based on IOTs Mitigating delays

Ref	Aspect	Dataset	Network Architecture	Algorithm/Model Used
[115]	Compromised Device Quarantine Time	Quarantine of compromised devices (e.g., smart thermostat) within seconds	Intrusion Detection System	Convolutional Neural Network
[116]	Resource Constraints	Limited processing power, memory, and energy in IoT devices	Agent Architecture	Artificial Neural Network
[117]	Update Mechanisms	Insecure and varied update mechanisms for IoT devices	Host Intrusion Detection System	Supervised Knowledge Base Algorithm
[118]	Encrypted Update Channels	Secure and encrypted channels for firmware updates	Fast Decision Network	Monte Carlo Tree Search
[119]	Self-Healing Capabilities	Autonomous quarantine and recovery of compromised devices	Fast Decision Network	Naive Bayes
[120]	Anomaly Detection	Identification of suspicious command patterns and anomalous traffic	Multi-Area Microgrid	DBSCAN Algorithm
[121]	Micro-segmentation	Isolation of devices to prevent lateral movement of threats	Strategy Network	Long Short-Term Memory (LSTM)
[122]	Firmware Integrity	Use of digital signatures to ensure firmware integrity and prevent attacks	Valuation Network	Auto-Regressive Moving Average (ARMA)

Uncertain Time-Delay Problem Robotic Network:
Teleoperation is one of the earliest and complex challenges parts of robotics. When

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

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

robots are controlled from very far away, like try to control from another city or country, underwater, or in space, the signals take time to travel. This delay can cause problems and make the robot system unstable. Researchers tried to add force feedback into remote robot control [125, 126]. But this robot shakes or behaves unpredictably because of a network delay. Because the network delay keeps changing, the system also keeps changing with time. So, many current control methods cannot be used directly. [127].

$$\omega = E_f * \frac{1}{1 + e^{-\theta t_f}} \quad \text{Eq (18)}$$

They modified the normal sliding-mode controller to make it work even when the network delay keeps changing. In simple word that system stays stable even when the internet is slow or unstable. Even that system really useful because if the time delay becomes long or unpredictable, then the Robot continues working without any mistake [128]. How communication delays happen in networks and How these delays change over time and How this affects robot control even they built a state-space model it is mathematical way to describe robot motion, behavior and communication delay Even why it is important Because you can't control a remote robot correctly unless you can't understand how delay affects robot movement and how delay change [129]. They made a controller that automatically adjusts itself based on the amount of network delay And Park [130].

$$\ln fl_{it}^{+} = \sum_{j=0}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \sum_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it} \quad \text{Eq (19)}$$

$$\ln fl_{it}^{+} = \sum_{j=1}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \sum_{j=1}^{t} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it} \quad \text{Eq (20)}$$

Communication is also key feature in networked intelligent robots because the robot, the robot server, and the web server must all talk to each other smoothly.

Role of Machine Learning in Internet of Things (IoTs)

The use of ML algorithms is a very versatile concept used in image and speech recognition, natural language processing (NLP), and anomaly detection. The quality of the input data representation is used to traditionally determine the efficacy of these algorithms. Weak representation may lead to poor performance as opposed to an excellent one. Moreover, ML can be ineffective when working with large scopes of data and needs to be enhanced by human intervention to be trained. The development of big data, the increase in computational power, and the improvements in the algorithms allowed the development of the state-of-the-art ML models, including Deep Learning (DL), capable of addressing the complex tasks [131].

Deep Learning utilizes deep neural networks, also known as multi-layered neural networks. These networks are designed based on the information processing of the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

human brain and they are effective specifically in recognizing images and speech, natural language processing and decision making. DL models are able to be trained with large data and they are able to learn features and representations out of the data. The first advantage of the DL models is that they can make predictions or decisions using data without requiring any human intervention or hand-coded feature engineering. DL models are mainly applied in computer vision, NLP, speech recognition, recommendation systems and prediction. They are trainable using supervised, unsupervised and reinforcement learning, which enables them to perform image/speech recognition, NLP, and decision-making tasks [132].

Deep Learning Models in Internet of Things (IoTs)

DL models are the basis of many innovative techniques and are used in different sectors such as finance, healthcare, transportation, retail, etc. The field is under a fast-developing state, and scientists work all the time on new methods to enhance the effectiveness of these models with the help of new architectures and techniques. DL algorithms enable computers to learn by experience and acquire a vision of the world in a hierarchy of concepts, which are defined in terms of their connection to the most fundamental logic. These techniques have introduced radical transformations in the spheres of speech recognition, visual object recognition, object detection and most other fields, including genomics and drug discovery. The Internet of Things (IoT) is emerging as the next revolution in the computing sensor era or networks [133]. The capability of accessing data of sensors and actuators mounted in our local environment. The IoT technology enables the devices to interact with each other and a central system, which allows automation of diverse processes and data collection to analyze it. This may result in efficiency, cost reductions, and decision-making in a very broad spectrum of businesses like manufacturing, transportation, healthcare, and home automation. IoT devices may be interconnected by wired or wireless networks, whereby a broad spectrum of devices may include smart thermostats, security cameras, industrial machines, and wearable devices. Internet of Things (IoT) is considered as of the most popular technologies currently, and it influences our lives in numerous ways, such as social, business, and economic ones. The future and current IoT technologies have a lot of potential in enhancing the overall quality of human life in terms of automation, productivity, and comfort in a large variety of applications, including education and smart cities. Nevertheless, the IoT is highly impacted by cyber-attacks and threats on smart applications [134]. The conventional IoT security methods are no longer enough, given the new security tasks, given the advanced booming of various forms of attacks and threats. The solution is to employ the expertise of artificial intelligence (AI), particularly machine and deep learning in order to provide a dynamically upgraded and modern security system to the next-generation internet of things (IoT) system [135, 136]. In this article, we provide an overall image of IoT security intelligence, which is based on machine and deep learning technologies that can derive insights on raw data and intelligently defend against a number of cyber-attacks on the Internet of things devices [137]. Lastly, we point out the issues of research and future directions of our study as per our study. Altogether, the article has the potential to act as a reference point and a guide, both technically speaking, to cybersecurity experts and researchers operating in the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

framework of IoT [138].

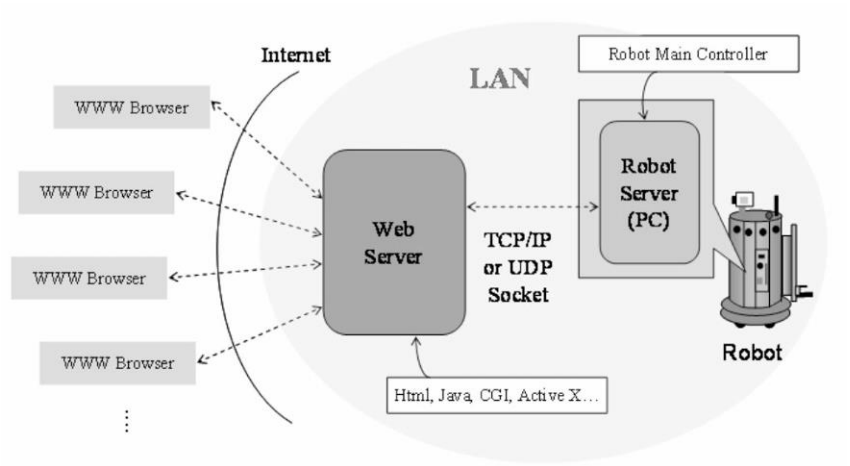


Figure 4: Automated Response from Robotic Server based on DL

In above fig. 4 show a one-robot system, that control the web server receives commands from the user then sends these commands to the robot server. The robot server sends the instructions to the robot and also receives images, sensor values, and status data from the robot. This communication happens because of virtual channel. A virtual channel is like a private tunnel used to send images, commands, and data safely between the servers and the robot

Intelligent services are a part and parcel of the present day life. The example is that disabled individuals might be able to control things with the help of IoT, specially-abled children might be able to communicate with each other by using the Autism Glass and remote health tracking help in curing [139]. In addition, IoT sensors in cooperation with warning system notifications on environmental disasters. The utility of the IoT in controlling natural resources may even be achieved based on the number of applications mentioned in the literature [140]. This is achievable with the smart grids and smart meters where the daily power-consumption would be adjusted and the ratio of supply and demand would be effectively maintained to the increasing demands. Similarly, intelligent transportation systems give useful information on various services [141]. As an illustration, on the basis of the real-time traffic conditions, traffic lights consequently adjust their timer to prevent traffic jam and in consequence, environmental pollution [142]. The agricultural crop yield could be anticipated, the fertilizers required, the areas that were susceptible to diseases could be isolated and identified using smart agriculture. Together with these services, it introduces ground level security issues since these IoT nodes are overwhelmed to the market with natural flaws [143].

The uncontrolled and rapid expansion and adoption of IoT with other technologies have brought about an expanded attack surface to explore. Additionally, due to the nature of an IoT node, which consists of limited resources and unattended environments, the security requirements of the system are difficult to maintain [144]. It is also not possible to utilize the available security measures like encryption,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

authentication and access control measures in order to ensure the security of systems with a high number of connected devices with natural vulnerabilities. Also, the end-users and developers are unaware of the security threats to supplement the comprehensive smart applications. IoT devices also have loopholes, which are used to execute a cyber-attack [145]. Moreover, this carelessness in safeguarding the IoT devices has been established to be life threatening. Indicatively, the hacked sensors of the self-driving vehicles may result in human tragedy and destruction of buildings too. These cyber-attacks now became another means of sabotaging the economy of the developed nations. Therefore, the security issue as one of the aspects inherent in such useful IoT services should not be disregarded and should be given precedence [146].
The learning techniques are the suitable means of distinguishing between the common and uncommon behavior of the IoT components and how they interrelate to one another to ensure delivery of services. The data sent to various elements of an IoT system is evaluated to identify the common patterns of the interaction process, to diagnose the malicious activity in a system in its initial phases. Not only could zero-day attacks be predicted with the help of learning methods [147] (machine learning and deep learning) since they are typically the mutations of the previous attacks. Further, the peculiarities of deep learning that include automatic feature extraction, compression abilities, etc., can support resource constrained IoT systems more. It is all attributed to its self-learning, speedy processing, and precision that has made deep learning a widely accepted technology. As a result, the IoT systems should undergo a shift of just providing safe communication between the gadgets to systems that are based on security facilitated by DL/ML techniques [148, 149].

TCP/IP and UDP in Internet of Things (IoTs) Using Intelligent Robotics Machine

In the fig. 5 multi-robot system, that control communication between many robots through two virtual channels. The first virtual channel sends commands and receives sensor data between the robot and the robot server, and the second one sends camera images and environment information from the robot to the web server for keeps data organized and avoids collisions [150, 151]. Robot treat as an intelligent agent, and the PC control center becomes the main controller for all agents. Communication between computers uses TCP/IP or UDP. TCP/IP is slow but reliable and ensures the data reaches correctly, so it is used for important commands. UDP is fast but may lose some packets, so it is used for streaming images and sensor data where speed is more important than accuracy. Overall, the communication system makes sure robots, servers, and users stay connected and work smoothly even over long distances [152, 153].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

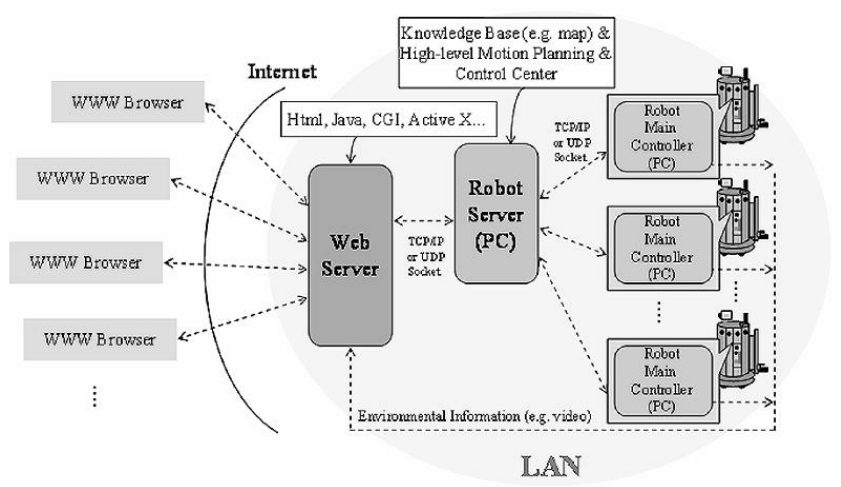


Figure 5: Architecture based on Multi robotic Network

Method and Materials

The different ways of IoT Networks Implementation through control architectures in the internet direct control, supervisory control and learning control. The major issues are addressed at conception, stability problem, task performance and learning capability.

Proposed Network Model

The proposed Deep Learning based secure Network is an innovative and automatic system that is learnt on the data produced by the host IoT network and identifies the intrusion of the network when properly trained. The proposed Intrusion Detection System (IDS) has a dynamic connector that is used to create the bond between emulated network and requests originating within the IoT network. An interface module of the feature extractor and network classifier communicates with the emulated network. The feature extractor takes out the feature of the network packets, which are the input of the deep neural network of the proposed methodology. The proposed IDS is a dynamic one and is updated on a regular basis depending on the new features that have been discovered using the classifier Updated module. After the intrusion has been detected, the network classifier forwards it to the mitigation step. This stage mitigates the effects of the intrusion. The proposed intrusion detection system has been designed with the consideration of simplicity and easy deployment. This is the reason why the detection system was created in a modular way. The proposed Deep Intrusion Detection (DID) will be made of three major modules. They include Communication Module (CM), Intrusion Detection Module (IDM) and Mitigation Module (MM). These three modules collaborate with each other. Communication module handles the entire communication between the receiver and the sender which is two-way. Communication of any kind goes through the IDM module. In case of any intrusion detection, the packets are sent to the mitigation module by this module. The communication module is operationalized by the use of Dynamic Connection, Network Emulator, and Interface module. Among the fundamental contributions of the proposed system is the system that is not tied to any

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

communication protocol. The protocol used as the background of communication between IoT devices is not a limitation to the DID system. It has been achieved by innovative design in the communication module. This subsection has addressed the working principle of the communication module.

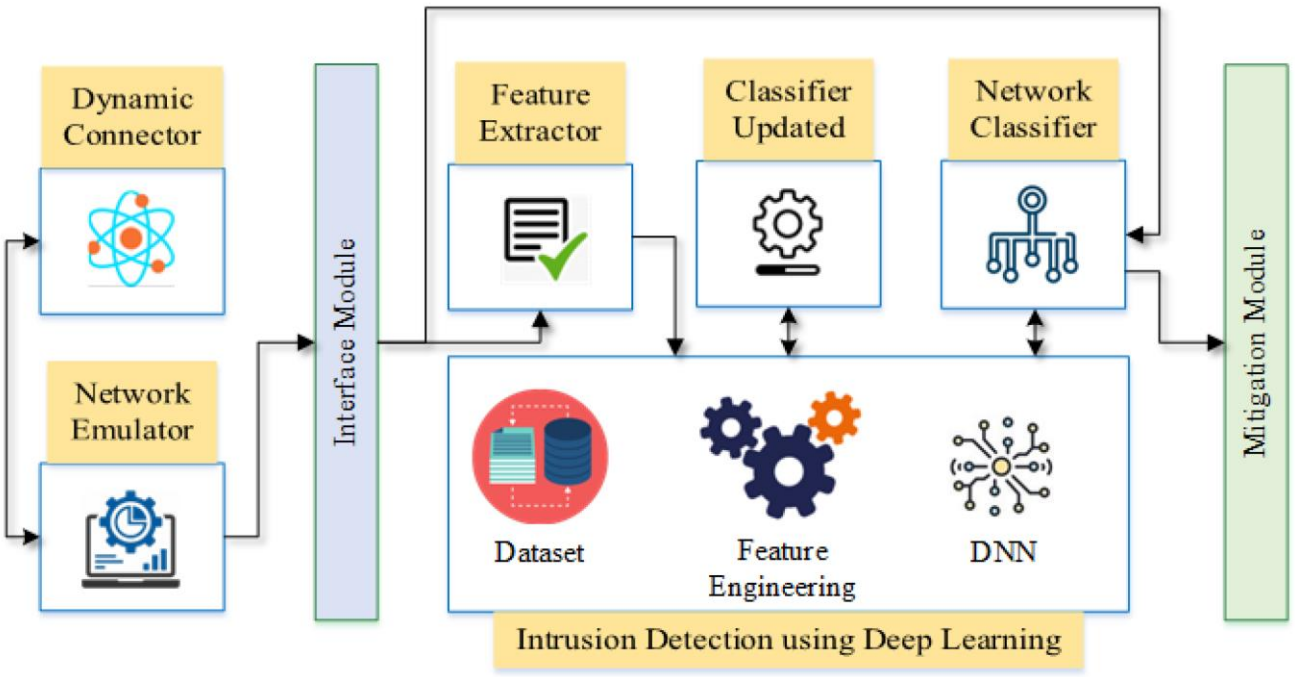


Figure 6: Secure Network Model to Mitigate Intrusion Detection

The Classifier Updated is one of the novel methods of this proposed intrusion detection system. This module has been developed to minimise the need of humans to update the network classifier. This module has tasks. The initial one is to monitor the network signals that do not belong to the training set. And the second step is to check the correctness of the SVM at all times. The Classifier Updated sounds the alarm when the accuracy of the SVM is less than 90% several times. Once it is fed will the labeled dataset, it will update the SVM on the dataset that resulted in performance degradation together with the former dataset.

The intrusion detection system proposed recognizes the intrusion with the help of a deep neural network, and it prevents the attack. Simultaneously, it will create a system response to produce an alert. This whole process involves two activities. The initial step is sensing the nature of the attack and the second step triggers a scheme that is relevant to reduce the effects of the intrusion. These two activities have two elements. The first part is the proposed deep neural network to classify the attack and the second part is the controller to select an appropriate option among a set of options to reduce the consequences of the attack.

Dataset Preprocessing and Utilization

This experiment has prepared a dataset of 25,000 instances that has been used. The ratio of Regular and Malicious instance of the dataset is 82:18. It implies that 82 percent of 25,000 cases are normal cases, and 18 percent are malicious cases. The

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

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

haphazard blend and there is no willful arrangement. The dataset has been split into the training, testing, and validation dataset in the ratio of 70:15:15. The training and validation data has been involved in the training stage. The testing data is not manipulated in the process of training and validating and is only utilized during the experimentation. Two critical steps in the automatic intrusion detection systems include proper feature selection and feature reduction [154, 155]. The IoT system is secure when the ratio between the transmission and reception is near unity. Nonetheless, a large variation in unity implies that the sender of the data is not transmitting to the right recipient or the receiver is not receiving the data to the right source. It signifies spoofing. It is possible that there exists some intermediate device, which is not listed in the network, that violated the network security and has manipulated the sender and the receiver. The mode of transmission is what defines the communication protocol, the present condition of the communication cycle and the next stage of the communication cycle. A Deep Neural Network that has been trained on the nature of communication in the various modes of transmission determines an intrusion when one of the devices behaves differently when it is under a specific mode of transmission. The result of the quantitative analysis is the qualitative results employing which the intrusion in an IoT network is identified.

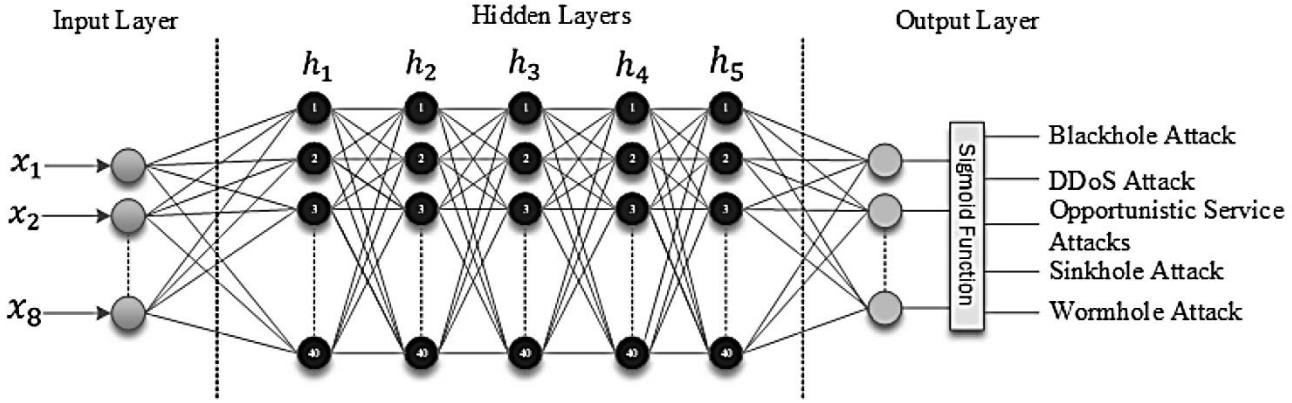


Figure 7: Deep learning Architecture based on Neural Network

In this experiment, a six layer deep neural network is optimized and designed to identify intrusion. Our initial network architecture was a 2-hidden layers network. Nonetheless, the experimental observation demonstrates that the network performance cannot be good using 2 hidden layers. This is the reason as to why we tried various number of hidden layers, and the 6-layer deep neural network produces the most appropriate outcome. Fully Connected Feed Forward Neural Network (FCFFN) architecture [156], shown in Figure 7, was used. Each neuron of a layer is linked to all the other neurons of the other layer in FCFFN architecture. The emphasis and omission of connections is not an extra complexity of implementation. The FCFFN architect was employed to make the implementation of the architect simple and easy.

Issues and Opportunities: Dynamic Network Connection and Emulator

The probe signals are sent by the dynamic connector. It also sends beacons to all the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

IoT equipment in the specified network. It also scans through the broadcast beacons, sniffs the handshake packets and scans the session requests to determine the communication protocols. It has a table of protocols that are in operation in the IoT space. The dynamic connector dynamically keeps functional network interfaces that intercept communication signals of various devices. The dynamic connector converts the packets that it receives on the various network interfaces. It stores the translation packets in the secondary storage as the cache storage. It then transforms the bit stream into network packets through the relevant protocol based on the protocol protocols it has stored in the protocol table when it receives the bit stream of the IoT devices. The protocol table contains the underlying network protocols of the networks in the IoT. All the related information about the network is contained in it. The proposed approach connects with the network using a creative mechanism of staying in touch rather than directly through the network. And that is via a network emulator. It has Virtual Network Client (VNC) module that retrieves the packets stored in the cache memory of the dynamic connector, selects the necessary network protocol within the protocol table, processes the packets based on the protocols, and lastly sends them to the targeted IoT device.

Discussion and Analysis

Human beings have long fantasized about the invention of a machine that would be able to activate the human brain. The most important solution is Artificial Intelligence (AI), which simulates the working of the human brain and introduces all the capabilities of the human brain into machines to enable them to think and behave like humans. AI is a branch of computer science that aims at creating computers or systems that are capable of performing tasks that would otherwise require human intelligence such as speech recognition, decision making, language translation and visual perception. Artificial intelligence is capable of causing a fundamental change in many spheres and can change our lifestyle and labor. Nevertheless, it also has such moral and social challenges as privacy issues and the displacement of jobs. Machine learning (ML) is a subfield of AI, in which algorithms and statistical models are generated that can help machines to learn through information and make decisions or predictions without being programmed explicitly. Images, text, or sensor readings can serve a wide range of data sources, and these algorithms can be trained to spot patterns and relationships in the data. The overall aim of ML is to design models capable of making predictions or decisions that would extrapolate to unseen and new data. ML algorithms can be of three main types: supervised, unsupervised and reinforcement. In supervised learning, the machine is given a dataset that is labelled and can also learn how to predict the output when given a new input, depending on the examples that have been given to it in the dataset. Even in unsupervised learning, the machine is provided with unlabeled data and it is left to identify patterns or structures in the data. Clustering or anomaly detection are common tasks to which this form of learning is applied, in which one is interested in determining the existence of groups or anomalies in the data. Finally, reinforcement learning is also the process in which the ML interacts with an environment and is rewarded (or punished) to provide feedback. These are the three categories of ML algorithms that are important in ensuring that machines can learn, adapt, and enhance their decision-making skills. As

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

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

the availability of data and computing resources grows, ML is becoming one of the most important parts of various industries, healthcare, finance, transportation, etc. With its ability to make machines learn based on the data, ML can change the way we treat technology and how we solve complicated issues.

Network Threat and Intrusions

Blackhole Attack, Distributed Denial-of-Service (DDoS) Attack, Opportunistic Service Attacks, Sinkhole Attack, and Wormhole Attack are the most common and harmful attacks of the IoT networks. This is because of the nature of the data, which has changed. The speed of the data flow, the character of the attack, and the target of the attackers have varied. Consequently, conventional systems that are based on rules are no longer as effective as before the IoT revolution. This is why deep neural networks suggested in this paper are the most recent methods of big data processing, pattern identification, and making relevant predictions [157, 158].

Distributed Denial-of-Service (DDoS) and (OSA)Attack

A distributed denial-of-service attack or DDoS attack is an ill-intentioned effort to interrupt normal traffic of a particular server, service, or network with large quantities of Internet traffic to hamper or cripple the target or the infrastructure it relies on. This kind of attack is referred to as a distributed denial-of-service attack (DDoS). In an opportunistic service attack, the malicious device gains the trustworthiness gradually by initially giving out services of great trustworthiness but later changing to offer services of lesser quality to the effect of making more profit for itself [159].

Sinkhole Attack (SHA) and Wormhole Attack (WHA)

One type of attack is a sinkhole attack in which a compromised node tries to lure network traffic by advertising its own fictitious routing update. Among the adverse impacts of sinkhole attacks, one can mention the fact that they can be employed to carry out additional attacks, including selective forwarding attacks, acknowledgment spoofing attacks, drops, or routing information modifying attacks [160]. In a wormhole tunnel attack, two attacking devices also use a virtual private connection to communicate with one other in order to execute an attack. The packets sent to the victim device are received and first forwarded through the wormhole and it is replayed later on.

Table 4: Analysis of Intrusion Detection-based Models Using DL

Classifier	Delay	Attack	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	IDR
RNN	t= 5ms	Blackhole	52.34	59.89	23.48	62.19	59.89
DT		DDoS	54.32	54.32	17.45	57.34	54.32
NBB		Sinkhole	57.92	57.92	16.74	57.78	57.92
RF		Wormhole	60.21	60.21	24.64	61.28	60.21
SVM		Average	53.68	53.68	19.42	55.79	92.41
CNN		Opportunistic	54.32	91.07	57.97	17.16	54.72

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

		Service					

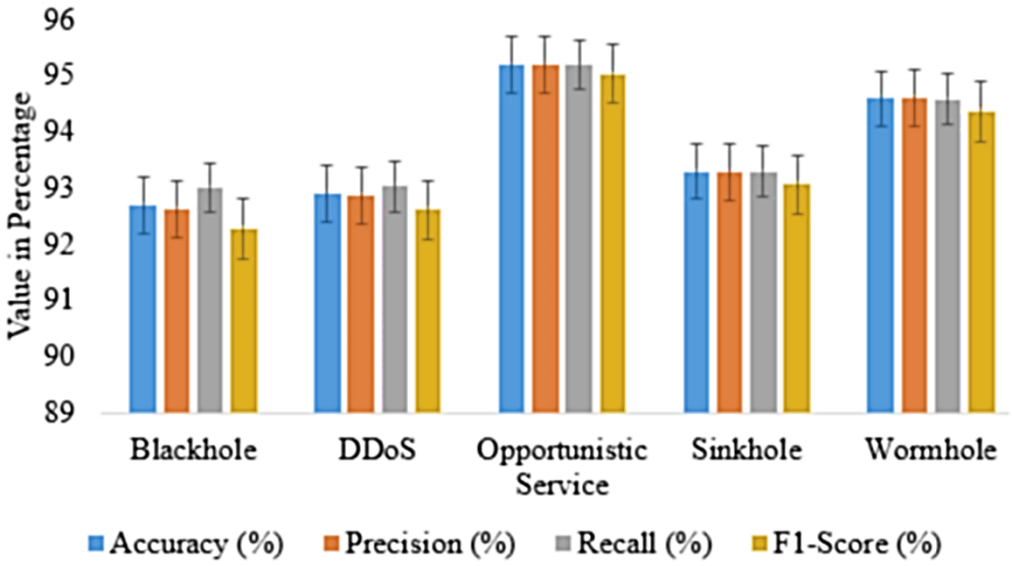


Figure 8: Performance Analysis of Intrusion Detection based Models Using DL

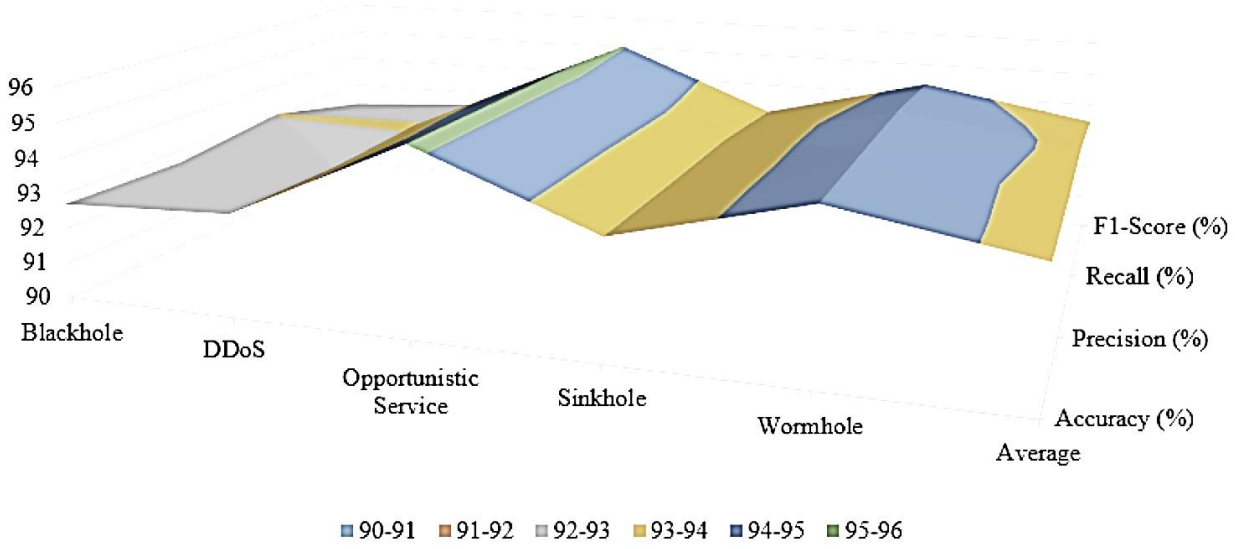


Figure 9: Variation in Performance based on Intrusion Detection Models Using DL

Conclusion and Future Directions

This article examined how intelligent machines can be controlled through the Internet, and what challenges and opportunities come with this technology. Because Internet access is now available almost everywhere, people can operate robots from far away,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

creating new possibilities in factories, hospitals, homes, security, and even entertainment. However, controlling robots through the Internet is not always smooth—problems like delays, lost data, slow connections, and security risks can affect how well these systems work. Researchers have developed several methods to reduce these problems. These include predicting the robot's movements ahead of time, using special control signals that stay stable even when the network is slow, and using mathematical techniques to keep the robot steady despite delays. Although these methods help, relying only on low-level, real-time user control is still difficult when the network is unreliable. This is why improving the robot's own intelligence is important. By giving robots more autonomy such as the ability to avoid network intrusion mitigation, plan routes, understand their surroundings, and make simple decisions—they can continue working even when network communication is slow or interrupted. High-level control methods let users give simple instructions like "go to this location" instead of controlling every movement. At the same time, better user interfaces, including mobile apps and web platforms, make operating these robots much easier.

Many real-world examples show how useful networked robots can be: robots that help with surgery, wheelchairs that assist disabled users, museum tour-guide robots, security robots, and robots used for space or scientific missions. These applications demonstrate how robots can safely support humans in places that are dangerous, difficult, or far away. Looking to the future, progress in this field will depend on improving robot intelligence, making communication more reliable, adding better learning abilities, and ensuring stronger security. Trends such as cloud robotics, mobile control interfaces, and human-friendly interaction will help robots become more connected to everyday life. As these technologies develop, robots will not only follow remote commands but also act as smart partners that help humans in many tasks. Overall, although challenges still exist, the development of networked intelligent robots is moving quickly. Enhancing robot autonomy, stabilizing communication, and improving how humans interact with robots will be key to unlocking their full potential. This paper's findings help support continued research in this important and growing field.

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.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

REFERENCES

Islam, M. K., Rahman, M. M., Ali, M. S., Mahim, S. & Miah, M. S. Enhancing lung abnormalities diagnosis using hybrid dcnnvit- gru model with explainable ai: A deep learning approach. Image Vis. Comput. 142, 104918 (2024).

Amanullah, M.A.; Habeeb, R.A.A.; Nasaruddin, F.H.; Gani, A.; Ahmed, E.; Nainar, A.S.M.; Akim, N.M.; Imran, M. Deep learning and big data technologies for IoT security. Comput. Commun. 2020, 151, 495–517.

Li, Y.; Zuo, Y.; Song, H.; Lv, Z. Deep learning in security of internet of things. IEEE Internet Things J. 2021, 9, 22133–22146.

Alferidah, D.K.; Jhanjhi, N. Cybersecurity impact over bigdata and iot growth. In Proceedings of the 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 8–9 October 2020; IEEE: New York, NY, USA, 2020; pp. 103–108. [Google Scholar]

Yılmaz, H.E.; Sirel, A.; Esen, M.F. The impact of internet of things self-security on daily business and business continuity. In Research Anthology on Business Continuity and Navigating Times of Crisis; IGI Global: Hershey, PA, USA, 2022; pp. 695–712. [Google Scholar]

Harada, R.; Shibata, N.; Kaneko, S.; Honda, K.; Terada, J.; Ishida, Y.; Akashi, K.; Miyachi, T. Quick Suppression of DDoS Attacks by Frame Priority Control in IoT Backhaul with Construction of Mirai-based Attacks. IEEE Access 2022, 10, 22392–22399.

Batten, L.M.; Moonsamy, V.; Alazab, M. Smartphone applications, malware and data theft. In Computational Intelligence, Cyber Security and Computational Models; Springer: New York, NY, USA, 2016; pp. 15–24. [Google Scholar]

Tariq U, Ahmed I, Bashir AK, et al. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023;23(8):4117.

Kaspersky. IT threat evolution Q3 2023[R/OL]. (2023–12–01)[2024–05–11]. https:// secur elist. com/ ksb-2023-stati stics/ 111156/.

Ma B, Zhang Z, Chen Y, Wu JX. The defense method for code-injection attacks based on instruction set randomization. J Cyber secur. 2020;5(4):30–43.

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

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

Xiao-Meng F, Qiu-Ye S, Bing-Yu W, Jia-Wen G. The coordinated cyber physical power attack strategy based on worm propagation and false data injection. Acta Automatica Sinica. 2022;48(10):2429–41.

Yadav B, Tokekar S. Recent innovations and comparison of deep learning techniques in malware classification: a review. Int J Inf Secur Sci. 2021;9(4):230–47.

Shaukat K, Alam T M, Luo S, et al. 2021 A review of time-series anomaly detection techniques: a step to future perspectives//Advances in Information and Communication: proceedings of the 2021 future of information and communication conference (FICC), Volume 1. Springer International Publishing, 865–77.

Online ISSN 3007-3197
Print ISSN 3007-3189

Sung A H, Xu J, Chavez P, et al. 2004 Static analyzer of vicious executables (save)[C]//20th annual computer security applications conference. IEEE, 326–34.

Nataraj L, Karthikeyan S, Jacob G, et al. 2011 Malware images: visualization and automatic classification[C]//Proceedings of the 8th international symposium on visualization for cyber security. 1–7.

Smmarwar SK, Gupta GP, Kumar S. Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: a comprehensive review. Telemat Inf Rep. 2024;12:100130

Gao, J., Wang, H., & Shen, H. (2020). Task failure prediction in cloud data centers using deep learning. IEEE Transactions on Services Computing, 1111–1116. https:// doi.org/10.1109/BigData47090.2019.9006011 ...

Guo, X., Aviles, G., Liu, Y., Tian, R., Unger, B. A., Lin, Y. H. T., & Kampmann, M. (2020). Mitochondrial stress is relayed to the cytosol by an OMA1–DELE1–HRI pathway. Nature, 579(7799), 427–432.

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

Lin, K., Li, Y., Sun, J., Zhou, D., & Zhang, Q. (2020). Multi-sensor fusion for a body sensor network in a medical human-Network interaction scenario. Information Fusion, 57, 15–26. Manogaran, G., Baskar, S., Hsu, C. H., Kadry, S. N., Sundarasekar, R., Kumar, P. M., & Muthu, B. A. (2021).

FDM: Fuzzy-optimized Data Management Technique for Improving Big Data Analytics. IEEE Transactions on Fuzzy Systems, 29(1), 177–185. Manogaran, G., Shakeel, P. M., Priyan, R. V., Chilamkurti, N., & Srivastava, A. (2019). Ant colony optimization-induced route optimization for enhancing the driving range of electric vehicles. International Journal of Communication Systems, e3964. https://doi.org/10.1002/dac.3964

Gesture-based human-Network interaction for human assistance in manufacturing. The International Journal of Advanced Manufacturing Technology, 101(1), 119–135. Nguyen, N. T., Liu, B. H., Pham, V. T., & Huang, C. Y. (2016). Network under limited mobile devices: A new technique for mobile charging scheduling with multiple sinks. IEEE Systems Journal, 12(3), 2186–2196.

Preeth, S. S. L., Dhanalakshmi, R., & Shakeel, P. M. (2020). An intelligent approach for energy efficient trajectory design for mobile sink based IoT supported wireless sensor networks. Peer-to-Peer Networking and Applications, 13(6), 2011–2022.

Priyan, M. K., & Devi, G. U. (2018). Energy-efficient node selection algorithm based on node performance index and random waypoint mobility model on the Internet of vehicles. Cluster Computing, 21(1), 213–227.

Ramprasad, L., & Amudha, G. (2014, February). Spammer detection and tagging based user generated video search system—A survey. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1–5).

Online ISSN 3007-3197
Print ISSN 3007-3189

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).

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.

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.

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.

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

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.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

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.

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

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

Online ISSN 3007-3197
Print ISSN 3007-3189

Shukla, P., Krishna, C. R., & Patil, N. V. (2025). Distributed ensemble method using deep learning to detect DDoS attacks in IoT networks. Arabian Journal for Science and Engineering, 50(2), 1143-1168.

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

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.

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

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

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

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability",

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

Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

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

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

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H.

Online ISSN 3007-3197
Print ISSN 3007-3189

(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.

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

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.

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).

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

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.

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos, G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of

Online ISSN 3007-3197
Print ISSN 3007-3189

Business and Economics (BBE), 13(2), 136-141.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

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

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

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

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.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

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.

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.

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.

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.

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

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

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Ali, 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.

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.

Online ISSN 3007-3197
Print ISSN 3007-3189

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

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

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

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.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An

Online ISSN 3007-3197
Print ISSN 3007-3189

insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

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.

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

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.

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.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

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., 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.

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.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber

Online ISSN 3007-3197
Print ISSN 3007-3189

security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

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.

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., 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.

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.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

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.

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.

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.

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.

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

Online ISSN 3007-3197
Print ISSN 3007-3189

Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

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.

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.

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.

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.

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

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

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.

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.

Ismaeel, S., Saleemi, H., Amir, U., Ashraf, S., & Hamza, A. (2024). A Detailed Review of latest Trends, Technologies Applications

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

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.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An

Online ISSN 3007-3197
Print ISSN 3007-3189

Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.

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.

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

Faruqui, N.; Yousuf, M.A.; Whaiduzzaman, M.; Azad, A.; Barros, A.; Moni, M.A. LungNet: A hybrid deep-CNN model for lung cancer diagnosis using CT and wearable sensor-based medical IoT data. Comput. Biol. Med. 2021, 139, 104961.

Wójcicki, K.; Biegańska, M.; Paliwoda, B.; Górna, J. Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review. Energies 2022, 15, 1806.

Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of industry and blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161.

Zhao, Y.; Lian, Y. Event-driven Circuits and Systems: A Promising Low Power Technique for Intelligent Sensors in AIoT Era. IEEE Trans. Circuits Syst. II Express Briefs 2022, 69, 3122–3128.

Soldatos, J.; Gusmeroli, S.; Malo, P.; Di Orio, G. Internet of things applications in future manufacturing. In Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds; River Publishers: Delft, The Netherlands, 2022; pp. 153–183. [Google Scholar]

Sharma, R.; Arya, R. Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Trans. Emerg. Telecommun. Technol. 2022, 1, e4571.

Rondon, L.P.; Babun, L.; Aris, A.; Akkaya, K.; Uluagac, A.S. Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. Ad Hoc Netw. 2022, 125, 102728.

Williams, R.; McMahon, E.; Samtani, S.; Patton, M.; Chen, H. Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; IEEE: New York, NY, USA, 2017; pp. 179–181. [Google Scholar]

Hilton, S. Dyn Analysis Summary of Friday October 21 Attack. Dyn Blog. 2016. Available online: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack (accessed on 1 January 2023).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Nayak, J.; Meher, S.K.; Souri, A.; Naik, B.; Vimal, S. Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. J. Supercomput. 2022, 78, 14866–14891.

Husnain, M.; Hayat, K.; Cambiaso, E.; Fayyaz, U.U.; Mongelli, M.; Akram, H.; Ghazanfar Abbas, S.; Shah, G.A. Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System. Sensors 2022, 22, 567.

Zheng, Y.; Li, Z.; Xu, X.; Zhao, Q. Dynamic defenses in cyber security: Techniques, methods and challenges. Digit. Commun. Netw. 2022, 8, 422–435.

Nimbalkar, P.; Kshirsagar, D. Analysis of rule-based classifiers for IDS in IoT. In Data Science and Security; Springer: New York, NY, USA, 2021; pp. 461–467. [Google Scholar]

Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun. Surv. Tutor. 2020, 22, 1646–1685.