Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

A Review on Advanced IoT Cyber-Attack Mitigation Using Hybrid Machine Learning and Deep Learning Frameworks

Palak Jain
Department of Information Technology, Mahakal Institute of Technology, Ujjain, India;

Asso. Prof. Yashovardhan Kelkar (Guide/Supervisor)
Department of Computer Science & Engineering, Mahakal Institute of Technology, Ujjain, India;

***Abstract*- The current review article studies the state-of-the-art approaches to cyber-attack prevention in the Internet of Things (IoT) system, as applied to the hybrid frameworks with machine learning (ML) and deep learning (DL) methodologies. This is aimed at examining existing strategies, determining constraints of traditional security systems, and emphasizing how intelligent, adaptive and scalable systems can be used to deal with the challenges of the emerging threats in heterogeneous IoT networks. Decision trees, random forests, support vector machines, and k-nearest neighbors are ML-based methods that have been reviewed in the study and presented an efficient way to detect anomalies and classify traffic, especially on edge devices that have limited resources. It further looks at the DL architectures, such as convolutional neural networks, recurrent neural networks, and long short-term memory models, which are effective at extracting hierarchical features, detecting zero-day attacks and analyzing modalities of time and sequence in big data of IoT. The paper also examines hybrid ML/DL systems that integrate lightweight ML preprocessing and deep learning-backed advanced detection, which are distributed at edge, fog, and cloud layers to ensure the most optimal computational performance, latency, and scalability. Findings of the literature review have shown that the hybrid methods can greatly enhance the accurate detection rate, minimize false positives, and allow near real-time mitigation via automated responses, including device isolation, filtering of traffic policies, and enforcement of dynamic policies. The review highlights the need of layered, adaptive, and intelligent security to ensure heterogeneous IoT infrastructures and offers a clue to the issues of resource limits, heterogeneity in data, preserving privacy and retraining models. All in all, this work provides an exhaustive overview of the latest literature, paying attention to how hybrid ML- DL systems can be used to improve IoT cybersecurity.**

Keywords-IoT Security, Cyber-Attack Mitigation, Hybrid Machine Learning, Deep Learning, Anomaly Detection, Edge Computing, Fog Computing, Cloud Security, Zero-Day Attack Detection, Intelligent IoT Framework.

I. INTRODUCTION

The high-rate evolution of the Internet of Things (IoT) has transformed how physical and digital worlds interact with each other so that billions of smart devices, sensors, and embedded systems are able to communicate, collaborate, and provide intelligent services across different fields of interest, including healthcare, smart cities, agriculture, transportation, manufacturing, and energy management. IoT infrastructures improve productivity, automation, and end user convenience as well as enable decision making based on data on scales never seen before due to continuous connectivity and real time exchange of data. Alongside these benefits, the open and distributed characteristics of IoT networks considerably increase the attack surface, which opens a lot of entry points to cybercriminals. Lots of IoT devices use low computational capabilities, ineffective authentication protocols, older software, and little encryption, and thus they are easy targets by attackers looking into perpetrating distributed denial of service attacks, spreading malware, spoofing attacks, botnetting attacks, stealing data, and disrupting services. With the ever-expanding list of connected devices, the old-fashioned perimeter-based security models are no longer sufficient, thus the immediate necessity of smart, flexible and scalable defense models with the ability to adapt in response to the quickly changing threats.

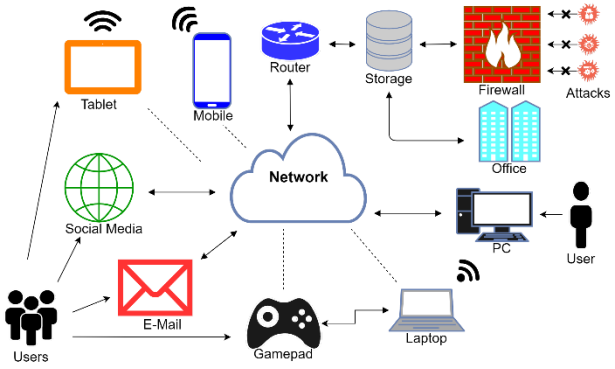

Fig. 1 Cyber Attacks Detection in IoT Systems[1]

Routine intrusion detection and prevention systems are mostly based on fixed rules, misuse signatures, or thresholds determined by an expert to detect malicious activities. Such systems are effective in the event that attacks have been previously known, but they do not fare well with zero-day attacks and multi-vector attacks that constantly change their

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

form to avoid detection. Also, the IoT environments produce large amounts of heterogeneous data which is high velocity and variability and cannot be monitored manually. These constraints have prompted researchers and practitioners to consider artificial intelligence-based solutions that are capable of learning automatically due to the presence of data, identify anomalies, and get better over time. Machine learning methods have demonstrated some potential on this aspect by allowing systems to model normal and abnormal behavioral patterns depending on the past behavioral observations. Decision Trees, Random Forests, Naive Bayes, Support Vector Machines, k-Nearest Neighbors and others are algorithms that are commonly used to classify traffic, detect anomalies and evaluate risk. The benefits of them include relatively low computing complexity, faster training, and interpretability, which is useful in IoT deployments with resource constraints. Their applicability, however, can be strongly determined by precisely crafted features, and can not fully signalize complex nonlinear dependencies between large-scale interactions in networks [2], [3].

Deep learning has become a strong continuation of machine learning that serves as a solution to all these limitations since it automatically derives hierarchical and high-level representations of raw data. Convolutional Neural Networks and Recurrent Neural Networks and Long Short-Term Memory are the most appropriate neural network models to identify spatial relationships and capture temporal variations of sequential traffic flows, respectively. Autoencoders and deep belief networks also increase the capacity of revealing a concealed framework and unseen anomalies. Deep learning models can also conform to a wide range of attack patterns, and their accuracy in detection, particularly in high-dimensional and challenging cases, is higher because they do not need a broad range of manual feature designs. However, they require considerable computing resources, large amounts of labeled data, and extended convergence times, which can pose a challenge to practical implementation on the edge of the IoT network where latency and energy efficiency is a matter of concern To reduce the gap between performance and practicability, hybrid frameworks that combine machine learning and deep learning are becoming more and more popular as an optimal and resilient approach to IoT cybersecurity. These models make use of the efficiency of classical algorithms to perform preprocessing, dimensionality reduction, and initial filtering, and the deep neural networks to do the more advanced representation learning and accurate classification. This interaction of these methods can greatly decrease the false positive rates, improve quicker decision-making and improve the generalization of unseen threats. In addition, distributed intelligence is aided with the help of hybrid strategies, which assign tasks to lightweight devices at the edge and more computationally demanding tasks to either the fog or cloud layers hence allowing scalability and efficient use of resources. This multi-layered control does not only enhance the detection, but also allows a quicker mitigation via automated response controls like the segregation of traffic, dynamic reconfiguration, or threat quarantine.

It is especially important to develop sophisticated mechanisms of mitigating cyber-attacks in terms of mission-critical IoT applications, where the security breach can have disastrous consequences. In healthcare, attacked devices can endanger the lives of patients; in smart grids, attacks can compromise power supply; and in transportation systems, the vulnerability can ensure the endangered safety of the population. Thus, the current security systems should not just utilize a passive mode of monitoring but also integrate active intelligence, lifelong learning, and dynamism. Hybrid ML-DL models allow the systems to adapt to the threat environment by adding feedback loops, retraining processes and real-time analytics that keep the system resilient even in rapidly changing environments.

Against these challenges and opportunities, the current work proposes a state-of-the-art mitigation framework of IoT cyber-attacks that is founded on the combination of the machine learning and deep learning approaches. The framework focuses on total data capture, optimized intelligent features, adaptive multi-stage classification, automatic mitigation policy to secure heterogeneous devices and communication protocols. The proposed solution is aimed at integrating the mutually beneficial forces of both paradigms to achieve greater accuracy, expediency of detection, and robustness than single solutions. Finally, this study is part of the vision of secure, reliable and trustworthy IoT ecosystems that can meet the growing needs of the digital transformation whilst protecting users, infrastructure and other important information assets.

II. Literature Review

Zahid 2025 et al. The high rate of IoT technology adoption has augmented the cybersecurity threats wherein the systems are more susceptible to attacks e.g. DDoS, DoS, R2L, U2R, malware, scanning, and bot attacks raising the risk to the system integrity in various arenas. This paper introduces a hybrid neural network, CNN-BiLSTM, that offers an integration of Convolutional neural network and bidirectional long short-term memory networks, to detect attacks in real-time. The model tested on 3 Data sets (KDDCup99, NSL-KDD and CIC_IDS-2017) had high accuracy of 99.9, 99.8, and 98.0 respectively- with high precision, recall and F1 scores, especially with complex threats. Its superiority has been attested by comparative analysis which provides a scalable, robust solution to the security of IoT infrastructures [4].

Anum 2025 et al. The increasing nature and the sophistication of cyber attacks have revealed the shortcomings of conventional security designs. In the current research, it is suggested to implement an AI-based cybersecurity architecture that combines advanced machine learning algorithms with ANN-ISM paradigm to implement a real-time threat detection process, intelligent risk response, and mitigation that can be scaled. The combination of literature review, empirical surveys, and case-based analysis of insecure coding practices are used as the methodology.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

By use of supervised and unsupervised and reinforcement learning with federated learning as the means of decentralized intelligence, and Explainable AI as the means of transparency, the framework can greatly increase the predictive accuracy, response time, and adaptability which can provide a very strong base of intelligent, sustainable, and scalable cybersecurity system [5].

Deepa 2024 et al. The increase in the sophistication of cyber threats has expedited the implementation of machine learning (ML) methods that ensure successful attack detection and mitigation in other areas such as IoT and Wireless Sensor Networks (WSN). The paper examines such algorithms as Random Forest, Ridge Classifier, and Gaussian Naive Bayes, and their use in improving the detection accuracy and efficiency. The focus on data preprocessing, feature extraction, and hybrid models, as well as, the evidence offered in the study proves that Multi-Agent Reinforcement Learning (MARL) is effective dealing with class imbalance and dynamic threat settings. Results indicate that though traditional ML algorithms are effective, MARL provides a major leap in developing strong, reconfigurable intrusion detection systems [6].

Prabakar 2023 et al. The issue of security on the web is a critical issue within the industries because of the increased rate of attacks especially in the IoT-enabled systems of homes, health, transport, and smart cities. Using the power of fog computing, which brings the processing nearer to the IoT devices than the cloud, allows attacking faster. This study presents a new AI-based framework of sustainable smart city network based on the combination of the kernel quadratic vector discriminant machine as a traffic analyzer and the adversarial Bayesian belief network as a malicious attack detector. Experimental performance shows that it performs well with results of 98 percent throughput, 74 percent traffic analysis, 45 percent end-to-end delay, 92 percent percent packet delivery ratio, 92 percent percent energy efficiency and 79 percent percent QoS respectively, which shows that it is a robust and efficient network security [7].

Salam 2023 et al. With the incorporation of cyber-physical systems, AI, and IoT in Industry 5.0, there is a high risk of cybersecurity breaches endangering production, data, and physical safety. The proposed research will involve a deep learning approach to web-based attack detection in Industry 5.0 settings. Convolutional Neural network (CNNs), Recurrent Neural network (RNNs), and transformer based models were tested on the basis of their effectiveness in attack classification and anomaly detection. The findings of the experiments illustrate that the transformer-based system can excel the traditional machine learning and other more conventional deep learning in accuracy, precision, and recall. The paper notes that deep learning has the potential of delivering robust, scalable, and adaptive intrusion detection, which guarantees the safety of critical industrial infrastructures [8].

TABLE 1: LITERATURE SUMMARY

Authors/Year	Method	Research gap	Findings
Ullah[9]	Hybrid LSTM and GRU deep learning model for attack detection	Real-time, faster algorithm needed for efficient IoV attack detection	Achieved 99.5% DDoS, 99.9% car hack detection accuracy
Alghazzawi/2021[10]	CNN with BiLSTM predicts DDoS attacks using feature selection	Optimal feature selection limits accuracy in existing ML/DL approaches	Achieved 94.52% accuracy on CIC-DDoS2019 dataset
Dehghani/2021[11]	Wavelet Transform, SVD, GWO-based selective ensemble deep learning	CPSs vulnerable to false data injection attacks, need precise detection	Over 95% precision identifying multiple FDIAs robustly
Soe/2020[12]	Sequential ML-based framework with ANN, J48, Naïve Bayes classifiers	IoT devices lack memory, computation for robust rule-based detection	Around 99% accuracy in detecting botnet attacks
Dutta/2020[13]	DSAE for feature extraction, stacked ensemble DNN, LSTM, logistic regression	Traditional ML inefficient for IoT/CPS large-scale anomaly detection	Successfully detects anomalies on IoT-23, LITNET-2020, NetML-2020

III.OVERVIEW OF IOT ARCHITECTURE AND COMMUNICATION

The IoT framework is structured into various collaborative layers which facilitate effective sensing, communication, processing and service delivery. The perception layer comprises of sensors, actuators, RFID tags, and intelligent objects that read the parameters of the environment and translate them into digital format.

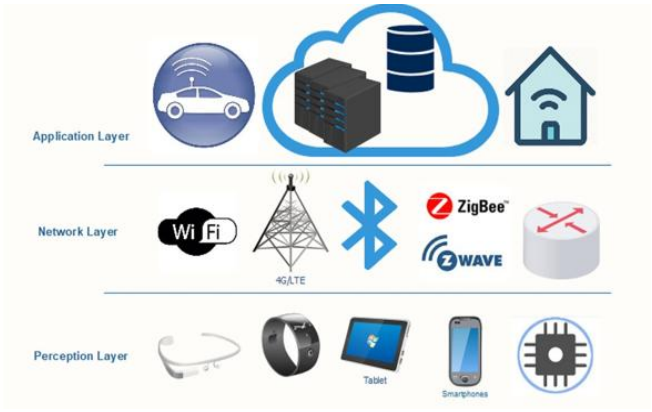

Fig. 2 IOT Layers Architecture [14]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

An edge or a gateway layer is then used to consolidate data and filtering, compression, and protocol translation are used to minimize a latency and bandwidth requirements. The network layer provides a secure channel of transmission through Wi-Fi, cellular, Bluetooth, Zigbee, and LPWAN technologies. Storage, analytics, and authentication are handled in cloud or fog platforms in processing layer [15], [16]. Lastly, the application layer provides user-friendly services, and such protocols as MQTT and CoAP provide scalable communication.

A. Perception (Device) Layer

The device layer is usually known as the perception layer, as it is the cornerstone of any Internet of Things ecosystem since it is where the physical world touches the digital infrastructure. It has an immense range of components such as environmental sensors, actuators, RFID tags, wearables, cameras and embedded smart objects [17]. These aspects constantly monitor real-time data like temperature, humidity, pressure, movement, the intensity of the light, sound, position, or physiological indicators and convert it into organized digital information that may be relayed via the network. This layer also has actuators that allow responding physically to received commands (retaliation), as in switching equipment on or off or making mechanical operations change. The accuracy, calibration and consistency of sensing devices is essential since all advanced analytics and decisions are based on such raw input. The acquisition of poor data may spread the mistakes all over the system, and correct perception guarantees meaningful insights, efficient automation, and reliable IoT activities.

B. Edge / Gateway Layer

The edge or gateway layer is a middle ground intelligence layer between resource limited devices and central computing platforms. It collects the streams of data of a lot of sensors and carries out initial-stage processing like clearance of duplicate data, packet compression, format validation and carrying out lightweight analytics. The edge reduces the amount of traffic that needs to take place across the network as it processes data nearer to the origin. The gateways are also used to convert between different protocols, data models and security requirements to enable a heterogeneous device to interoperate easily. Local coordination lowers latency, bandwidth, improves privacy and allows a system faster and more dependable responses.

C. Network / Transport Layer

The network or transport layer is the means that offers the communication backbone between field devices and gateways and remote processing platforms, data centers, or cloud services. Its main duty is the movement of information efficiently, precisely and safely through infrastructures that may be very large and heterogeneous. This layer may deploy a variety of technologies, including Wi-Fi, cellular networks, Ethernet, LPWAN, Bluetooth, and Zigbee depending on the needs of deployment like range, bandwidth and energy consumption. In addition to mere transmission, it regulates routing policies, addressing of devices, congestion, as well as quality of service, to ensure it has stable connectivity [18]. Systems of encryption, tunneling and authentication are often combined to safeguard data transmission. The transport layer allows higher layers of the IoT architecture to make reliable decisions, engage in automation, and do analytics as it can be used to deliver packets in a reliable manner and ensure reduced losses or delays.

D. Processing / Middleware Layer

Processing or middleware layer is the brain of the IoT ecosystem, the raw data that come through the network are processed to provide usable information. In cloud/mog computing setup, this layer provides scalable storage, high-performance computing and real time analytics. It handles databases, stream processing pipelines and rule engines that are able to extract patterns, identify anomalies and produce actionable insights. Moreover, it implements device authentication, authorization and secure access control to ensure trust throughout the infrastructure. Interfaces and data formats are standardized with middleware services, which allows smooth interoperability of different hardware platforms, software services, and applications to end users.

E. Application Layer

Application layer is the interface on which the end users, administrators and outside systems interrelate with the IoT infrastructure. It converts processed data to useful services specific to specific fields including remote patient monitoring, smart farming, industrial automation, environmental surveillance, or intelligent transportation [19]. Users can internalize trends and obtain system performance alerts and real-time monitoring through dashboards, mobile applications, and web portals. Control commands are also produced by this layer and activate actuators or automated processes depending on the results of the analysis. The application layer is ultimately what dictates the tangible value that is represented by IoT deployments by taking complex data and converting it into information that is understandable and actionable.

F. Communication Models and Protocols

The IoT communication is designed based on diverse models of interaction that are selected based on their latency, power, scalability and management requirements. In device-to-device communication, the devices communicate directly to each other over short-range links, thus providing quick response without intensive reliance on the infrastructure. The device-to-gateway models add a new device, which centralizes the traffic, tracks security policy and is involved in translating protocols prior to relaying information. In device-to-cloud, smart objects are linked directly to remote platforms to store, undertake analytics and made accessible worldwide [20]. In order to make these trends, standardized schemes like MQTT, CoAP, HTTP/HTTPS, and AMQP offer effective messaging, trust, interoperability, and secure and extensive data transmission.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

IV. TAXONOMY OF IOT CYBER-ATTACKS

There are various dimensions of cyber-attacks of IoT networks. Physical attacks refer to the violation of hardware, taking of devices, or even malicious firmware, especially in unattended installations. Attacks that utilize communication channels use network-based attacks based on eavesdropping, spoofing, man-in-the-middle attacks, or DDoS attacks that attack availability. Malware and botnets attacks infect vulnerable nodes enabling the adversary to remotely control devices and organize extensive activities [21]. Weak credentials result in authentication and access control attacks, which create the possibility of impersonation and privilege escalation. The attacks are aimed at application and data vulnerabilities, and such exposure causes information theft, manipulation, and severe privacy invasion.

A. Physical Attacks

Physical attacks are also one of the most basic forms of threats to the IoT infrastructures as they do not use a software vulnerability but instead an attack on the hardware. Sensors and embedded nodes in most deployments are put in a more exposed, unattended, or scattered geography and are therefore easier to access by adversaries. Hackers can seize devices to steal cryptography keys, be able to gain access to stored data, disassemble elements, or impersonate identities [22]. They also have the capability to modify circuits, install debugging interfaces or replace valid firmware with malicious firmware that leaves a backdoor. After being compromised, a single machine with manipulated node can either neutralize the operations, distort the readings or provide broader network intrusions.

B. Network-Based Attacks

Network-related attacks center on the use of vulnerabilities in the communication channels that include IoT devices, gateways, and cloud platforms. Since the data can be delivered across wireless and shared channels, they can be easily intercepted by enemies who can steal the information or understand the traffic patterns. The attackers can impersonate legitimate nodes by using such techniques like spoofing, and man-in-the-middle attacks can be used to modify or inject malicious packets into the communication. Attacks that are routing manipulate routes to cause data to malfunction or discard, which compromises reliability [23]. DDoS attacks consume network bandwidth, slow down, and can put important services out of service to authorized users.

C. Malware and Botnet Attacks

Insecure settings, old software, or loose authentication systems are used to install malicious code in IoT devices by malware and botnets attacks. After being infected, the attackers are able to spy on the operations remotely, modify functionality, or steal sensitive data without the knowledge of their owner. Due to similarities in architecture of many devices, malware can propagate quickly in networks and result in massive pools of infected nodes [24]. Such orchestrated networks, also referred to as botnets, are often used to run distributed denial of service campaigns, spam, cryptocurrency mining or espionage. Such operations are especially difficult to detect and contain, given the scale of such operations and their automation.

D. Authentication and Access Control Attacks

Authentication and access control attacks occur when the IoT systems are based on default passwords, lack identity verification, or permissive permission policies. These vulnerabilities can be used by adversaries to masquerade as a legitimate user, service or devices and pass through security barriers into restricted portions of the network. When inside, attackers can further upgrade privileges, alter configurations, disable safeguards, or alter data flows. This unauthorized control may interfere with the operations, breach confidentiality and lower the trust in automated decision-making [25]. The decentralized and massive character of the IoT environment further complicates the management of credentials, making it vulnerable to identity-based attacks.

E. Application and Data Attacks

Application and data attacks are focused on vulnerabilities found in software services, web interfaces, APIs, and cloud structures underlying IoT ecosystems. Attackers use coding weaknesses, lack of proper input validation or incorrectly set up storage systems to access sensitive resources without having appropriate authorization. The adversaries can modify databases, modify the behavior of the system, or retrieve confidential records with the help of SQL and command injection techniques. Violation can result in the leakage of personal data, business records, or intellectual content to cause financial and reputational losses. Due to the interconnections between most applications, a vulnerability has the potential to propagate across the services, increase privacy risks, and systemic consequences.

V. CONVENTIONAL SECURITY AND MITIGATION TECHNIQUES

A combination of cryptography and encryption, authentication, access control policy, firewalls, IDS/IPS, and patch management creates an overall security system of IoT ecosystems. Encryption protects both data at rest and data in transit, whereas authentication only allows access by legitimate users and devices. Access control prevents overlaying principles of the least privilege and ensures that the user is not exposed to sensitive resources, whereas traffic may be tracked and malicious activities can be identified or prevented by the use of firewalls and IDS/IPS. Patching and Firmware updates are performed on a regular basis to address vulnerabilities, to strengthen encryption and authentication [26]. Collectively, these layers of strategies secure the IoT networks against unauthorized access, tampering, and attacks, data integrity, privacy, accountability and general system reliability of distributed environments.

A. Cryptography and Encryption

Cryptography is one of the basic protection tools in the security of the IoT since it secures the information against the unauthorized exposure and alteration. Encryption algorithms would convert decipherable information into

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

incomprehensible ciphertext, and there is a chance that, even in situations in which the transmissions are intercepted, the adversaries cannot decode the data easily. These safeguards not only apply to data at rest in devices or in the cloud but also to data at motion in the communication networks [27]. The protocols like TLS, SSL, and IPsec provide secure channels, authenticate communicating parties, and integrity of messages provided by hashing and digital signatures. Encryption ensures that the trust and reliability in the IoT ecosystem is reinforced by eliminating eavesdropping and tampering.

B. Authentication Mechanisms

Authentication is a key to making sure that the resources and services of the IoT are accessible only to authentic users and trusted devices. However, traditional methods use usernames and passwords which mean that the credentials are compared to those stored before access is granted. To enhance this process, cryptographic keys and digital certificates are usually employed to form identities among the machines and permit well-founded mutual authentication between the conversing entities. Multi-factor authentication also provides extra protection by demanding supplementary evidences including one-time password, biometrics or hardware tokens [28]. All these methods of layering can considerably minimize the likelihood of unauthorized access, impersonation, and theft of credentials. In extensive IoT setups, sound identity management systems are essential towards accountability, sensitive data, and integrity of automated processes in distributed settings.

C. Access Control Policies

Mechanisms of authorization are used to ascertain the kind of access that is accorded to a user or devices once their identities are properly verified. Role-based access control (RBAC) is the one in which the permissions are granted based on job functions or jobs which are defined and only the tasks required by the role are performed. Attribute-based models build on this concept by including other parameters like location, time, device type or security posture during approval [29]. These strategies restrict unwarranted access to sensitive resources by applying the least privilege principle. Proper authorization can minimize unintended abuse, stem out privilege escalation, and minimize the threats of malicious insiders or compromised accounts.

D. Firewalls and IDS/IPS

The firewalls and intrusion detection or prevention systems are the protection mechanisms in the IoT networks that regulate the flow of data in and out of the trusted and untrusted environment. Firewalls use preset rules to block or allow traffic depending on the parameters of IP addresses, ports, and protocols, and help minimize the exposure to illegal connections. To supplement this role, the IDS and IPS technologies constantly examine traffic patterns and system behavior, in order to identify abnormalities, established attack signatures, or violation of policies. On detection of suspicious activity, warnings are sent or automatic countermeasures are issued to prevent threats. Collectively, these mechanisms enhance perimeter security and enhance situational awareness.

E. Patch Management and Updates

Patch management and timely updates are essential practices towards keeping the IoT ecosystem security posture. The firmware and software usually have vulnerabilities that can be identified later and reported publicly providing attackers with precise knowledge on the manner of exploiting the vulnerable systems. Organizations can ensure that such security gaps are closed before they are widely exploited by applying the patches that are provided by the vendors on a regular basis. New changes can also come along with more robust encryption, superior authentication functions and better monitoring. Due to the regular occurrence of thousands of distributed devices as part of the IoT deployments, there is a need to have automated and centrally controlled update mechanisms. Regular maintenance helps a lot in preventing exposure to the new threats as well as increasing the stability of the system.

VI. MACHINE LEARNING FOR IOT SECURITY

Machine learning enhances the security of the IoT since it allows smart and data-based protection systems in various settings. With anomaly detection, the models are taught normal behavior and raise an alarm when there is anomaly, which might be a zero-day attack or a stealthy attack. Traffic classification methods analyze the packet attributes and flow behavior to differentiate a legitimate communication and malicious activity.

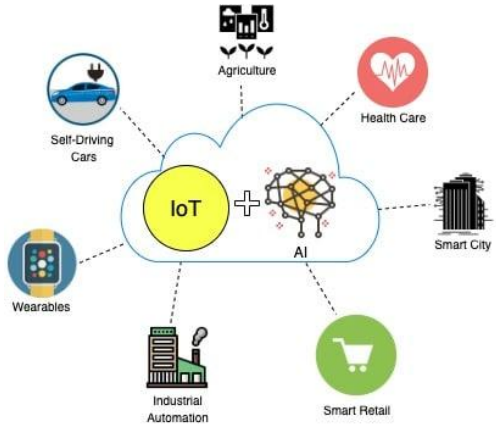

Fig. 3 Machine learning IoT security[30]

Automated feature extraction saves human labor (determining the most informative indicators of large, heterogeneous datasets) and enhances efficiency and accuracy. The adaptive learning enables a constant retraining to ensure that defenses keep up with the emerging threats [31]. Ultralight implementations can be deployed to small edge devices, and risk assessments generated by ML can be used to make fast, automated response and mitigation.

A. Anomaly Detection

One of the strongest applications of machine learning in the IoT security is the anomaly detection since it enables systems to identify threats that they had not encountered before. Using historical data, ML models create a baseline which indicates normal behaviour of devices, users and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

network traffic. This baseline can be in the form of frequency of communications, packet sizes, access times, or pattern of resource utilization [32]. In case the observed real-time data are greatly unusual to these learnt norms, the system indicates them as possible intrusions. This kind of capability can play a very important role in detecting zero-day attacks, insider abuse, or covert operations that have no existing signatures to allow more operations to be investigated and contained in a shorter amount of time.

B. Traffic Classification

Traffic classification methods employ either supervised or unsupervised learning methods to analyze network traffic and classify it as legitimate or malicious. Attributions like source addresses, destination addresses, type of protocol, nature of payload, time delay, and durability of the session are examined to bring out concealed relationships [33]. Through precise labeling of traffic, the ML systems can block malicious communications, quarantine suspicious nodes or priority critical alerts. This type of classification comes in particularly handy when the deployment of IoT is large-scale and manual monitoring is not possible. Quality classification enhances situational awareness and allows automated defense strategies and increases the overall network reliability and performance.

C. Automated Feature Extraction

The scales of IoT environments create large and heterogeneous data, which renders the manual feature engineering process ineffective and susceptible to errors. Machine learning helps in that, it automatically picks up the most informative attributes out of the raw streams of data. The statistical values, correlation trends, and behavioral variables are compared to find out which elements play the greatest role in the successful detection of the threat. The right extraction of features minimizes dimensionality, fastens the training of models, and decreases the computation needs. It also reduces noise and redundancy which otherwise may reduce performance. With meaningful inputs, the security systems developed using ML can have better generalization and remain effective in diverse devices and communication conditions.

D. Adaptive Learning

Hackers keep on changing strategies to evade the current security mechanisms as cyber threats constantly evolve. Adaptive learning helps machine learning models to be active with the addition of new information as time goes by. When it comes to legitimate and malicious behavior, systems become more knowledgeable through retraining or incremental updates. Predictions can be updated by the use of feedback of detected incidents, human analysts, or updated datasets. This dynamic capability will not lead to stagnancy but it will remain relevant even in changing environments. Adaptive mechanisms hence optimize detection accuracy, false alarms and the long term resilience of IoT infrastructures.

E. Lightweight Detection

Several IoT devices have hard limits that pertain to the use of power, memory storage, and processing power. Lightweight machine learning models aim to operate effectively within these constraints and at the same time offer meaningful security monitoring. Such techniques as simplified classifiers, compressed models, or edge analytics provide threat detection in and around the data. This lessens the need to have constant connectivity to the cloud and also lessens the delays in communication [34]. Lightweight detection techniques allow intelligent security to be realized with high-degree of distribution and low-power deployments by balancing the performance with resource efficiency.

F. Decision Support and Response

The machine learning systems can not only identify the threats; they can also help in identifying the appropriate countermeasures. The results can be in the form of probability scores or severity rankings or behavioral classifications, which can be used by the administrators to assess the risk level. In more sophisticated systems, such outputs may automatically lead to mitigation measures, such as blocking the suspect IP addresses, isolating the attack-affected computers, or even forensic recording. ML-based decision support comes in handy by ensuring damage and disruption of operations are minimized because it speeds up the response time. The integration with orchestration platforms also allows organized, real-time protection measures on the IoT ecosystem, improving the overall security governance.

VII.DEEP LEARNING FOR CYBER-ATTACK DETECTION

Deep learning will strengthen IoT cyber-attack detection by hierarchical features through self-directional learning of raw or low-level processed data, obviating feature engineering and training, and detecting hidden malicious behavior. It is very good at detecting sophisticated, multi-stage, and zero-day attacks by learning intricate nonlinear associations between high-dimensional data. Sequential architectures such as LSTM, GRU and RNN can capture the temporal behavior, and identify slow or changing intrusions which snapshot method can ignore [35]. Deep networks are effectively scaled to large data streams of IoT data enhancing generalization and accuracy. They are incorporated with streamlined frameworks giving near real-time alerts and automated mitigation isolating threats and minimizing response time and human input.

A. Automatic Feature Learning

One of the major benefits of deep learning in detecting cyber-attacks is that it can learn informative representations using raw or processed data to the minimal extent. As opposed to more traditional machine learning, which relies heavily on handwritten attributes that are based on the domain expert, deep neural networks automatically learn hierarchical structures over traffic flows, payloads, or device logs [36]. Simpler patterns are also picked up by lower layers and then more abstract messages of harmful activities are made up by the deeper layers. This minimizes problem of human prejudice, wastage of time and in many cases reveals relations that would have otherwise been concealed. Consequently, there will be stronger, more extensively

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

flexible and adaptable detection systems, which can be utilized in a variety of IoT situations.

B. Detection of Sophisticated and Zero-Day Attacks

Contemporary attackers often develop attack strategies that are fast-evolving in nature or those that occur in phases, rendering them hard to detect using fixed signatures. Deep learning is very effective in the process of identifying such threats since it will be able to fit nonlinear dependencies and intricate associations involving a large number of variables at the same time. Neural networks are able to detect the subtle deviations on high dimensional spaces, which can help identify hidden attack footprints where explicit rules do not exist. This is especially useful in the case of zero-day detection where there are no examples [37]. Extrapolation capability out of the trained cases enhances proactive protection and minimises exposure to new cyber threats.

C. Temporal and Sequential Analysis

A lot of cyber-attacks do not occur in an instance but occur through a process of time. Sequential data deep learning models, including the Recurrent Neural Networks, Long Short-Term Memory networks, and Gated Recurrent Units, are optimally adapted to the dynamics. They examine the changing nature of behaviors, and this might be suspicious transitions or repeated patterns or gradual increases in activity [38]. This time consciousness enables the system to identify slow and stealthy attacks that may not be identified by snapshot based monitoring tools. Through event correlation in various time windows, DL models are able to offer richer context and thus they are more accurate in detecting threats and are also able to give better situational awareness.

D. Scalability with Large Data Volumes

IoT systems are producing vast amounts of heterogeneous data on a continuous basis and exponentially in the thousands or millions of devices. Deep learning models can easily support this scale, and they probably perform better the more training data is available to them. Neural networks are now able to effectively process high-dimensional inputs, and learn complex distributions using parallel processing and with state-of-the-art hardware accelerators. This scalability allows organizations to have the same level of security monitoring despite the increase in the size of a network. Moreover, big data can be used to minimize overfitting, boost generalization and increase confidence in forecasts, which makes DL an effective method in high-growth infrastructures.

E. Real-Time Intelligent Response

Deep learning systems can deliver almost real-time threat detection and response when combined with streamlined deployment systems. Once suspicious activity is detected, there are alerts, risk probabilities, or classifications that are generated by the models and can be used to automatically initiate defense mechanisms. These can be the isolation of affected nodes, the barring of malicious connections, or the updating of firewall settings. Cascading failures can occur in an environment where IoT may need rapid action as delays may cause new failures. With high-speed inference and automation, DL-based security platforms reduce human involvement, decrease the speed of response, and prevent the possible effects of cyber attacks.

VIII. HYBRID ML–DL FRAMEWORKS

Hybrid machine learning deep learning (ML–DL) frameworks are a progressive concept of ensuring the safety of IoT ecosystems through the application of the strengths of both approaches in addressing the multifaceted cyber threat. The preprocessing, feature selection and lightweight anomaly detection in these systems are handled by traditional ML methods, such as decision trees, random forests or SVMs, particularly at edge devices which have limited resources. ML prunes and compresses the data, allowing deep learning models, including CNNs, RNNs, and LSTMs, to discover nonlinear connections, temporal, and minor deviations to identify multi-stage attacks, zero-day attacks, and anomalies. This stratified architecture enhances the precision of detection, reduces the number of false alarms and enables response to be adaptive and real time with the use of automated mitigation policies, such as isolating a device or blocking traffic. The scalability of the framework manages huge data streams of IoT, and the ML makes sure that small nodes are efficient. It is used in smart cities, industrial internet of things, medical services, and intelligent transportation. The issues still persist in integrating models, optimizing resources, retraining continuously, and ensuring low-latency protection to ensure reliability and sustainable protection in changing IoT environments [39], [40]

IX. IMPLEMENTATION CHALLENGES AND REAL-TIME DEPLOYMENT

Resource constraints, heterogeneity of data, latency, and model management are also quite problematic to IoT devices. Low processing power, memory and battery present a limitation to the deployment of complex ML/DL models, which requires edge-friendly architectures. Large, multi-modal data of sensors and gateways should be preprocessed, normalized, and feature extracted in an efficient way to ensure model accuracy. Threat detection needs low latency processing with hybrid edge-fog-cloud, optimized, and parallel processing. It is necessary to train and update models in order to match the changing cyber threat, and strategies such as incremental and federated learning are necessary to guarantee consistency, overhead reduction, and reliable and up-to-date detection in resource-constrained, heterogeneous IoT contexts.

A. Resource Constraints on IoT Devices

There are numerous IoT gadgets that are constrained significantly in processing capability, memory and power supply. The use of complex machine learning (ML) or deep learning (DL) models on these devices can exceed its ability, causing slowing of the system, high power consumption, or system failure. Lightweight algorithms, pruning of models, quantization and edge friendly architectures are necessary so that detection tasks in real time do not negatively affect the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

performance of a device. The smart utilization of computational resources enables the IoT devices to carry out analytics on the device, eliminate reliance on cloud computing, decrease latency, and balance performance, accuracy and energy consumption in resource-constrained settings [41], [42].

B. Data Heterogeneity and Volume

Internet of Things (IoT) ecosystems produce vast amounts of data in a variety of sources such as sensors, gateways, and user devices in various formats, frequencies, and qualities. Unless processed effectively, this heterogeneous and large volume data can overwhelm the conventional processing pipelines. There is a need to have scalable architectures that can handle diverse data streams to extract meaningful insights without bottlenecks. Preprocessing methods of data including normalization, filtering, feature extraction, and fusion are important to keep the models of ML and DL accurate. When this diversity is handled appropriately, it would be possible to achieve the ability to aid the continuous monitoring, minimize latency, and enhance the consistency of real-time detection in large-scale IoT networks.

C. Latency and Real-Time Processing

The process of threat detection in IoT networks requires timely and accurate analysis and reaction to possible abnormalities. Slowness in cloud computing processing may lag the decision-making process, which enables cyberattacks to take advantage of the vulnerabilities of the system. Equally, inefficient edge computation cannot process the necessary data at the real time. The issue of assigning computation loads between the edge, fog and cloud layers is important to minimize the delays without losing precision. The latency can be minimized by implementing hybrid processing measures, such as local preprocessing and selective offloading to the cloud. Net Protocols and Parallel Processing - Optimized net protocols and parallel processing also help to enhance the responsiveness of the system, which ensures timely mitigation and solid protection in dynamic IoT systems.

D. Model Training and Updating

Deep learning and machine learning systems must be constantly updated to support new trends of threats and changes in the IoT environment. This is through regular retraining with the newest datasets, version control and safe distribution of the updated models to distributed devices. It is operationally and technically challenging to achieve consistency and integrity of models across heterogeneous nodes. The cost of training, data synchronization and validation can be a significant computational overhead especially to resource-constrained devices. Incremental learning and federated learning, among other strategies are essential to support current and trustworthy detection functions and minimize downtime and communication expenses; as well as eliminate the chances of implementing old or unsafe models.

X. CONCLUSION

Finally, the uncensored expansion of the IoT ecosystems, heterogeneous and resource-deficit due to their characteristics, has posed unprecedented security challenges on cybersecurity, requiring intelligent, adaptive, and multi-layered defensive measures. Perimeter-based security models cannot effectively combat advanced attacks like a zero-day exploit, multi-stage attacks, and botnet attacks particularly in latency-sensitive and large-scale applications. Hybrid machine learning and deep learning systems provide a solution to this issue, as lightweight ML models would be useful at the edge to efficiently perform preprocessing, anomaly detection, and dimensionality reduction, whereas deep learning architectures would have strong representation learning, time- series analysis, and high-dimensional pattern recognition capabilities on both fog and cloud layers. The combination of edge, fog, and cloud computing makes these frameworks optimize the speed of detection, computational efficiency, and scalability to enable real-time responses with intelligent capabilities, automated mitigation, and continuous adaptation to changing threats. Nevertheless, real-life use has been found to encounter issues such as insufficient resources of the device, heterogeneous data volumes, latency issues, continuous model training, compatibility with previous infrastructure, and protection of sensitive information. To overcome these problems, lightweight algorithms have to be carefully designed, preprocessing pipelines have to be scalable, model distribution must remain secure and privacy preserving techniques must be employed. In general, hybrid ML-DL systems are a robust, proactive, and smart method of IoT cybersecurity, which improves situational awareness, decreases false positives, and allows distributed networks wide-ranging protection. They are essential in protection of mission critical applications in healthcare, transportation, industrial automation and smart cities, and eventually allow secure, reliable, and trustful IoT ecosystems that have potential to sustain the requirements of digital transformation.

REFERENCES

[1] “Cyber Attacks Detection in IoT Systems.” Accessed: Feb. 12, 2026. [Online]. Available: https://www.mdpi.com/2079-9292/11/9/1502

[2] B. M. K. Reddy, A. Abdul Azeez Khan, K. Javubar Sathick, and L. Arun Raj, “Cyber Attack Recognition in an Internet of Things-Enabled Environment Using a Hybrid Optimised Deep Learning Approach,” *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 16, no. 1, pp. 49–71, 2025, doi: 10.58346/JOWUA.2025.I1.003.

[3] H. Kamal and M. Mashaly, “Enhanced Hybrid Deep Learning Models-Based Anomaly Detection Method for Two-Stage Binary and Multi-Class Classification of Attacks in Intrusion Detection Systems,” *Algorithms*, vol. 18, no. 2, 2025, doi: 10.3390/a18020069.

[4] M. Zahid and T. S. Bharati, *Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection*, vol. 5, no. 1. Springer International Publishing, 2025. doi: 10.1007/s43926-025-00156-y.

[5] A. Malik, K. Arshid, N. Noonari, and R. Munir, “Artificial Intelligence-Driven Cybersecurity Framework Using Machine Learning for Advanced Threat Detection and Prevention,” *Sch. J.*

Eng. Technol., vol. 13, no. 06, pp. 401–423, 2025, doi: 10.36347/sjet.2025.v13i06.005.

[6] S. Deepa Rajan and A. Manikandan, "Navigating Cybersecurity: a Comprehensive Analysis of Machine Learning in Cyber Attack Detection," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 21, pp. 7658–7669, 2024.

[7] D. Prabakar, M. Sundarrajan, R. Manikandan, N. Z. Jhanjhi, M. Masud, and A. Alqhatani, "Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City," *Sustain.*, vol. 15, no. 7, pp. 1–14, 2023, doi: 10.3390/su15076031.

[8] A. Salam, F. Ullah, F. Amin, and A. Mohammad, "Deep Learning Techniques for Web-Based Attack Detection in," *Mdpi*, pp. 1–18, 2023.

[9] S. Ullah *et al.*, "HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles," *Sensors*, vol. 22, no. 4, pp. 1–20, 2022, doi: 10.3390/s22041340.

[10] D. Alghazzawi, O. Bamasaq, H. Ullah, and M. Z. Asghar, "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection," *Appl. Sci.*, vol. 11, no. 24, 2021, doi: 10.3390/app112411634.

[11] M. Dehghani, T. Niknam, M. Ghiasi, N. Bayati, and M. Savaghebi, "Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach," *Electron.*, vol. 10, no. 16, pp. 1–19, 2021, doi: 10.3390/electronics10161914.

[12] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–15, 2020, doi: 10.3390/s20164372.

[13] V. Dutta, M. Choraś, M. Pawlicki, and R. Kozik, "A deep learning ensemble for network anomaly and cyber-attack detection," *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–20, 2020, doi: 10.3390/s20164583.

[14] "IOT Layers Architecture." Accessed: Feb. 12, 2026. [Online]. Available: https://connectwithiot.wordpress.com/2020/11/01/device-layer/

[15] K. N. Singh, "Automating Cyber Attack Detection through Integrated Deep Learning and Scalable Data Science Pipelines," 2025.

[16] M. K. Al-Anni, R. M. Almuttairi, A. A. Al-Hamadani, K. A. Zidan, H. I. H. Alsaadi, and G. A. Al-Sultany, "Machine learning Algorithms to Detect Cyber-Attack in the Internet of Things Platform," *Iraqi J. Comput. Sci. Math.*, vol. 6, no. 2, pp. 317–333, 2025, doi: 10.52866/2788-7421.1268.

[17] W. Wu, H. Fouzi, B. Benamar, S. Sidi-Mohammed, and S. Ying, "Deep learning-based stacked models for cyber-attack detection in industrial internet of things," *Neural Comput. Appl.*, vol. 37, no. 24, pp. 19617–19651, 2025, doi: 10.1007/s00521-025-11418-9.

[18] A. Abbas *et al.*, "Machine learning-based hybrid technique to enhance cyber-attack perspective," *J. Cloud Comput.*, vol. 14, no. 1, 2025, doi: 10.1186/s13677-025-00782-5.

[19] A. Sharma and S. Rani, "An RF-DNN-Based Approach for Detecting Cyber Attacks in IoT Network," *J. Transform. Technol. Sustain. Dev.*, vol. 9, no. 1, 2025, doi: 10.1007/s41314-025-00077-2.

[20] V. Kandasamy and A. A. Roseline, "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks," *Sci. Rep.*, vol. 15, no. 1, pp. 1–26, 2025, doi: 10.1038/s41598-025-85547-5.

[21] T. H. Kim, A. Srinivasulu, R. Chinthaginjala, J. Dhakshayani, X. Zhao, and S. Obaidur Rab, "Enhancing cybersecurity through script development using machine and deep learning for advanced threat mitigation," *Sci. Rep.*, vol. 15, no. 1, pp. 1–14, 2025, doi: 10.1038/s41598-025-92676-4.

[22] I. Priyadarshini, "Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated Learning and Split Learning," *Big Data Cogn. Comput.*, vol. 8, no. 3, 2024, doi: 10.3390/bdcc8030021.

[23] S. H. Oh, J. Kim, J. H. Nah, and J. Park, "Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity," *Electron.*, vol. 13, no. 3, pp. 1–19, 2024, doi: 10.3390/electronics13030555.

[24] I. Journal and O. F. Science, "System Using Attention based Deep Learning Approach for Cyber Attacks," pp. 3947–3959, 2024.

[25] S. Gaba, I. Budhiraja, V. Kumar, and A. Makkar, "Advancements in enhancing cyber-physical system security: Practical deep learning solutions for network traffic classification and integration with security technologies," *Math. Biosci. Eng.*, vol. 21, no. 1, pp. 1527–1553, 2024, doi: 10.3934/mbe.2024066.

[26] N. U. Bacha, S. Lu, A. Ur Rehman, M. Idrees, Y. Y. Ghadi, and T. J. Alahmadi, "Deploying Hybrid EnsembleMachine Learning Techniques for Effective Cross-Site Scripting (XSS) Attack Detection," *Comput. Mater. Contin.*, vol. 81, no. 1, pp. 707–748, 2024, doi: 10.32604/cmc.2024.054780.

[27] T. S. Delwar *et al.*, "The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection: A Detailed Analysis," *Sensors*, vol. 24, no. 19, 2024, doi: 10.3390/s24196377.

[28] F. Alserhani and A. Aljared, "Evaluating Ensemble Learning Mechanisms for Predicting Advanced Cyber Attacks," *Appl. Sci.*, vol. 13, no. 24, 2023, doi: 10.3390/app132413310.

[29] L. K. Pai, "Deep Neural Network Architectures for Advanced Cyber Attack Identification," vol. 6, no. 2, pp. 9559–9567, 2023, doi: 10.15662/IJSRAT.2023.0602001.

[30] "Machine learning strengthens IoT security ." Accessed: Feb. 12, 2026. [Online]. Available: https://iotworlds.com/what-is-the-role-of-machine-learning-in-iot/

[31] M. S. Andhare, V. S. Kumbhar, and A. A. Tekade, "Detecting Cybersecurity Attacks in Industrial Internet of Things: A Systematic Literature Review," *5th Bienn. Int. Conf. Nascent Technol. Eng. ICNTE 2023*, pp. 1–27, 2023, doi: 10.1109/ICNTE56631.2023.10146705.

[32] A. Judith, G. J. W. Kathrine, S. Silas, and A. J, "Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices †," *Eng. Proc.*, vol. 59, no. 1, 2023, doi: 10.3390/engproc2023059139.

[33] F. Y. Assiri and M. Ragab, "Optimal Deep-Learning-Based Cyberattack Detection in a Blockchain-Assisted IoT Environment," *Mathematics*, vol. 11, no. 19, pp. 1–16, 2023, doi: 10.3390/math11194080.

[34] I. H. Sarker, "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects," *Ann. Data Sci.*, vol. 10, no. 6, pp. 1473–1498, 2023, doi: 10.1007/s40745-022-00444-2.

[35] B. B. Behera, R. K. Mohanty, and B. K. Pattanayak, "A Deep Fusion Model For Automated Industrial Iot Cyber Attack Detection And Mitigation," *Int. J. Electr. Electron. Res.*, vol. 10, no. 3, pp. 604–613, 2022, doi: 10.37391/IJEER.100332.

[36] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review," *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 527–555, 2022, doi: 10.3390/jcp2030027.

[37] A. Almalaq, S. Albadran, and M. A. Mohamed, "Deep Machine Learning Model-Based Cyber-Attacks Detection in Smart Power Systems," *Mathematics*, vol. 10, no. 15, 2022, doi: 10.3390/math10152574.

[38] W. B. Demilie and F. G. Deriba, "Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques," *J. Big Data*, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00678-0.

[39] S. Ren, J. Jin, G. Niu, and Y. Liu, "ARCS: Adaptive Reinforcement Learning Framework for Automated Cybersecurity Incident Response Strategy Optimization," *Appl. Sci.*, vol. 15, no. 2, pp. 1–20, 2025, doi: 10.3390/app15020951.

[40] S. Berrios, D. Leiva, B. Olivares, H. Allende-Cid, and P. Hermosilla,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

"Systematic Review: Malware Detection and Classification in Cybersecurity," *Appl. Sci.*, vol. 15, no. 14, pp. 1–32, 2025, doi: 10.3390/app15147747.

[41] B. A. Agbor, B. U. A. Stephen, P. Asuquo, U. O. Luke, and V. Anaga, "Hybrid CNN–BiLSTM–DNN Approach for Detecting Cybersecurity Threats in IoT Networks," *Computers*, vol. 14, no. 2, pp. 1–27, 2025, doi: 10.3390/computers14020058.

[42] Z. Aydın, "Detecting Cybersecurity Threats in Digital Energy Systems Using Deep Learning for Imbalanced Datasets," *Int. J. Energy Econ. Policy*, vol. 15, no. 3, pp. 614–628, 2025, doi: 10.32479/ijeep.19649.