Design and Implementation of an Intelligent IoT Security Framework for Real-Time Cyberattack Detection Using ML and Web Technologies

Apurva Iraskar[1], Dr.Sudhir Mohod[2]
[1]*Student, Department of computer science & Engineering Bapurao Deshmukh College of Engineering Wardha, Maharashtra, India 442104*
[2]*HOD Professor, Department of computer science & Engineering Bapurao Deshmukh College of Engineering Wardha, Maharashtra, India 442104*

***Abstract*—Industry4.0isfundamentallybased on networked systems. Real-time communication between machines, sensors, devices, and people makes it easier to transmit the data needed to make decisions. Informed decision-making is empowered by the comprehensive insights and analytics made possible by this connectedness in conjunction with information transparency. Healthcare IoT, a fast-growing field, could revolutionize patient monitoring and intervention. This interconnection raises new security concerns, requiring real-time anomaly detection to protect patient data and device integrity. This study presents a novel security framework that uses combination of Hidden Markov Models (HMM) and Support Vector Machine (SVM) to detect anomalies in real-time healthcare IoT environments with high accuracy. The framework prioritizes real-time strength and efficiency. Sensor data from wearables, medical devices, and other IoT devices is carefully segmented into time intervals. Features are carefully derived from each segment, including statistical summaries, patterns, and frequency domain characteristics. The system integrates Random Forest, XGBoost, Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) models within an optimized ensemble architecture to improve detection accuracy and robustness. A structured preprocessing pipeline extracts key features from network traffic, enabling real-time classification of attacks such as DDoS, botnets, malware, intrusion attempts, and port scanning. An intelligent risk assessment mechanism categorizes detected threats into CRITICAL, HIGH, MEDIUM, and LOW levels based on confidence scores and severity, supporting effective response prioritization. Unlike traditional threshold-based approaches, the proposed architecture is capable of autonomously distinguishing between benign operational anomalies and adversarial cyber-attacks, thereby reducing false alarms and improving detection accuracy. The framework adopts a multi-layer design that combines data acquisition, feature learning, anomaly detection, and response.Furthermore, a scalable web-based dashboard provides real-time monitoring, attack visualization, and system performance insights through interactive data streaming. The proposed framework delivers accurate, scalable, and efficient IoT cybersecurity protection suitable for dynamic network environments.**

***Index Terms*—IoT Cybersecurity, Machine Learning, Real-Time Cyberattack Detection, Intrusion Detection System, Anomaly Detection, Network Traffic Analysis, Web-Based Application, Deep Learning, DDoS Detection, Ensemble Learning.**

I. INTRODUCTION

The implementation and development of IoT has transformed a vast number of sectors by enabling connectivity and ensuring high automation. At the same time, those applications have interconnected IoT-enabled infrastructures more thoroughly, making them vulnerable to various cybersecurity risks. The explicitly mentioned cyber threats include DoS, Brute Force, and Trojan Horse cyber threats are more frequent and sophisticated; these threats compromise the integrity, confidentiality, and availability of IoT networks. Basically, the IDS is conventional that uses only the signature-based technology and therefore it can only work as planned provided the signature of the attack is already standardized. However, as seen, attackers are always devising new ways to attack systems, and therefore the signature-based approach

cannot detect such new or different attacks. Therefore, creating sophisticated, evolutional, and immediate means for detecting intrusions becomes strategically crucial. The effectiveness of IoT networks has not been investigated by researchers due to the following challenges; Dynamicity, heterogeneity of nodes presents in the IoT networks, and the fact that IoT devices are resource limited. To address these factors, the technologies which can handle a mass of complicated and different types of data and perfectly detect the exception must be incorporated. This study responds to these challenges by developing a deep learning model using GANs to detect most of the malicious activities happening in IoT networks suitably. The major advantage of GANs in cybersecurity lies in the fact that they are capable of moving beyond being specific to a certain pattern and be able to mimic other datasets of a similar nature to the actual one. This is in contrast to conventional models which employ specific attack signatures or patterns to distinguish between different attack variants which may be completely new. The framework comprises two key components: The other is a Generator that generates data that have the distributions of the original dataset and a Discriminator that determines if the data is normal or has been generated to be malicious. This technique enables the system to detect all types of attack signatures, including those not learned in its dataset.

The rapid advancement of the Internet of Things (IoT) has revolutionized the way devices communicate, interact, and operate in modern digital ecosystems. IoT enables seamless connectivity between physical devices such as sensors, smart appliances, industrial machines, and healthcare systems, thereby improving efficiency, automation, and decision-making across various domains. From smart homes and smart cities to healthcare monitoring and industrial automation, IoT plays a crucial role in transforming traditional systems into intelligent and interconnected environments. However, this massive expansion of interconnected devices has also introduced significant cybersecurity challenges, making IoT networks highly vulnerable to cyberattacks.

One of the primary concerns in IoT environments is the lack of robust security mechanisms. Many IoT devices are resource-constrained, with limited processing power, memory, and energy capacity, which makes the implementation of traditional security solutions difficult. Additionally, IoT systems often operate in heterogeneous and distributed environments, where devices from different manufacturers communicate over various protocols. This diversity increases the attack surface and creates multiple entry points for malicious actors. As a result, IoT networks are increasingly targeted by cyber threats such as Distributed Denial of Service (DDoS) attacks, malware injection, botnets, data breaches, and unauthorized access.

Traditional cybersecurity approaches, including signature-based detection systems, are often insufficient to address the dynamic and evolving nature of modern cyber threats. These methods rely on predefined attack patterns and fail to detect new or unknown attacks, also known as zero-day attacks. Furthermore, conventional systems are not designed to handle the high volume and velocity of data generated by IoT devices in real time. This limitation necessitates the development of advanced, intelligent, and adaptive security solutions capable of detecting and mitigating cyber threats as they occur.

In this context, Machine Learning (ML) has emerged as a powerful tool for enhancing cybersecurity in IoT environments. ML algorithms can analyze large volumes of network traffic data, identify hidden patterns, and distinguish between normal and malicious behavior. Techniques such as supervised learning, unsupervised learning, and ensemble methods enable the development of efficient intrusion detection systems (IDS) that can detect both known and unknown threats. Algorithms like Support Vector Machine (SVM), Random Forest, Decision Trees, and Gradient Boosting are widely used for classification and anomaly detection tasks in cybersecurity applications. Moreover, deep learning models further improve detection accuracy by capturing complex, non-linear relationships in data.

Real-time cyberattack detection is critical in IoT systems, as delays in identifying threats can lead to severe consequences, including data loss, system failure, and financial damage. Therefore, integrating ML-based detection models with real-time monitoring systems is essential for ensuring timely response and mitigation. The use of streaming data processing techniques allows continuous analysis of network traffic, enabling immediate identification of suspicious activities. This real-time capability

enhances the overall resilience and reliability of IoT networks.

In addition to detection, visualization and accessibility of security insights are equally important. Web-based applications provide an effective platform for monitoring, analyzing, and managing cybersecurity systems. By integrating ML models with web technologies, users can interact with the system through intuitive dashboards, visualize network activity, receive alerts, and take appropriate actions. Such applications improve usability and enable both technical and non-technical users to understand and respond to cyber threats efficiently. The combination of backend ML processing and frontend web interfaces creates a comprehensive cybersecurity solution that is both powerful and user-friendly.

Despite significant advancements, several challenges remain in developing effective IoT cybersecurity frameworks. These include handling imbalanced datasets, ensuring data privacy, reducing false positives and false negatives, and maintaining scalability in large-scale IoT deployments. Additionally, the interpretability of ML models is becoming increasingly important, as users need to understand the reasoning behind detection decisions. This has led to the integration of Explainable Artificial Intelligence (XAI) techniques, which enhance transparency and trust in ML-based systems. To address these challenges, this research proposes an intelligent IoT cybersecurity framework that leverages machine learning techniques for real-time cyberattack detection and integrates a web-based application for monitoring and control. The framework focuses on efficient data preprocessing, feature extraction, and the implementation of hybrid or ensemble ML models to improve detection accuracy and performance. Furthermore, the system is designed to provide real-time alerts and visual insights through a user-friendly web interface, enabling proactive threat management.

Many monitoring and diagnostic systems for the cutting process have been developed to deal with this problem, in which the cutting signals have been used for chatter identification, but most of them are offline systems. Traditionally, the chatter monitoring process consists of data collection, processing of cutting signals, and applying statistical methods and model training for chatter detec tion. Recently, machine learning approaches have been recognized to be an effective method for classification and recognition problems. Many studies also applied these techniques for monitoring machining stability successfully. Traditionally, machine learning-based chatter detection consists of signal collection, data acquisition, feature extraction, feature selection, and classification. This approach usually relies on how to determine the set of features that are relevant to cutting stability. Feature extraction and feature selection are therefore required to f ind out the most important features within the dataset. The irrelevant and redundant features will reduce classification accuracy and increase the computation time, it is expected to remove those features from the data set.

Security experts highlight the substantial risks posed by IoT devices across multiple domains. Various types of attacks and anomalies, including DDoS, Denial of Service (DoS), probing, Root to Local (R2L), User to Root (U2R), port scanning, malware, and unauthorized access, can lead to system failure. As a result, attack and anomaly detection has become a major concern in IoT environments. Timely identification of such attacks is critically important. Recent approaches have explored Machine Learning (ML) techniques such as Naive Bayes, Support Vector Machines (SVM), Logistic Regression, and Decision Trees. While these traditional methods offer certain advantages, they also have notable limitations. Extracting meaningful insights often requires significant human intervention, making the process costly and less practical. Additionally, rule-based and supervised learning models are effective in detecting known attacks but struggle to identify new or zero-day attacks, particularly in dynamic IoT environments. To overcome these limitations, Network Intrusion Detection Systems (NIDS) have incorporated deep learning techniques, showing promising results. Advanced methods such as Deep Restricted Boltzmann Machines (RBM) and Deep Convolutional Neural Networks (DCNN) have been used to enhance feature extraction and improve classification accuracy. Similarly, techniques like stacked denoising autoencoders (SDAE) have strengthened the ability of deep learning models to detect cyber threats in IoT environments. However, existing models often rely on single network architectures, which may limit their ability to capture complex relationships among diverse features. Furthermore, challenges such as incorrect labeling in training datasets and the availability of

small datasets continue to affect model performance. Deep learning models require careful tuning to achieve optimal results, and advanced techniques are necessary for accurate real-time attack detection. Key challenges include managing feature correlations, handling noisy or mislabeled data, and overcoming limitations in network architectures. Despite these challenges, deep learning continues to play a vital role in improving security mechanisms for classification and prediction in IoT systems.

II. RELETED WORK

The implementation of advanced monitoring and diagnostic systems has been made easier as a result of the incorporation of Internet of Things (IoT) technology in the healthcare industry. Because of the growing volume of real-time health data generated by Internet of Things devices, it is imperative that a significant emphasis be placed on preserving the dependability and quality of the data. When it comes to identifying abnormal patterns or deviations from the norm in health-related data, anomaly detection techniques are absolutely necessary. The purpose of this literature review is to investigate a variety of studies and methodologies pertaining to anomaly detection for health monitoring that is based on the Internet of Things (IoT). The authors, [10] proposed a method to evaluate the quality of photoplethysmography in real time health monitoring by utilizing Internet of Things technology. This approach is intended to be efficient and unobtrusive. Additionally, in order to gain insights into the accuracy of health-related data collected from Internet of Things devices, their methodology makes use of unsupervised anomaly detection. Syndrome is a spectral analysis technique that was developed by.[11] for the purpose of identifying anomalies on medical Internet of Things and embedded devices. A reliable solution for anomaly detection is provided by this methodology, which focuses on identifying abnormalities in the spectral characteristics of data related to health. Specifically, the development of efficient methods for detecting anomalies in Internet of Things (IoT) systems that are utilized in smart hospitals was the focus of a study that was carried out.[12]. The purpose of their work is to enhance the dependability of health data in Internet of Things environments by identifying anomalies in a timely manner in order to facilitate timely intervention. As part of their research,[13] focused on identifying irregularities in wireless sensor networks that are utilized in the medical field. The findings of this study highlight the significance of identifying abnormalities in sensor data, particularly in the context of applications applicable to the healthcare industry. In the field of Internet of Things (IoT) healthcare analytics, 14] emphasized the significance of anomaly detection. The findings of their research shed light on the significance of anomaly detection in maintaining the accuracy and reliability of The establishment of large hospitals where hundreds to thousands of patients are treated , it has created a serious problem of biomedical waste management. The seriousness of improper biomedical waste management was brought to the light during summer 1998. In India studies have been carried out at local / regional levels in various hospitals, indicate that roughly about 1-5 kg/bed/day to waste is generated. Among all health care personnel, ward boys , sweepers, operation theatre & laboratory attendants have come into contact with biomedical waste during the process of segregation, collection, transport, storage & final disposal. The knowledge of medical, paramedical staff & ward boys, sweepers about the biomedical waste management is important to improve the biomedical waste management practices. The biomedical waste requiring special attention includes those that are potentially infectious , sharps, example needle , scalpels, objects capable of puncturing the skin , also plastic, pharmaceutical & chemically hazardous substances used in laboratories etc.

A framework was presented by.[16] for the purpose of identifying irregularities in network traffic within the Healthcare Internet of Things platform. By identifying and analyzing abnormal patterns in network traffic, the primary purpose of this research is to improve the safety of Internet of Things (IoT) systems that are used in the healthcare industry. Within the realm of the Internet of Things (IoT), developed an intrusion detection system that was tailored to meet specific requirements. With a particular emphasis on protecting the integrity and confidentiality of health-related data, the primary objective of this system is to identify and prevent unauthorized access in Internet of Things (IoT) systems. In order to better understand how to identify irregularities in time-series data for the

Internet of Things (IoT).[18] carried out a comprehensive investigation. The research that they conducted provides a comprehensive analysis of the methodologies and frameworks that are currently being utilized to identify anomalies in time-series data that is generated by Internet of Things (IoT) devices. Through the use of a comprehensive literature review, [19] conducted an in-depth investigation into the methods of anomaly detection, analysis, and prediction that are utilized in Internet of Things environments. Through their research, they have provided valuable insights into the various methodologies that are utilized for anomaly detection in environments that are associated with the Internet of Things (IoT). A neural network called ANNet was developed by Sivapalan et al.[20] with the purpose of identifying irregularities in electrocardiogram (ECG) signals obtained from Internet of Things (IoT) edge sensors. ANNet was developed with the express purpose of being exceptionally lightweight, which makes it suitable for use in environments with limited resources. Their strategy revolves around the utilization of neural networks in order to accomplish the goal of achieving efficient and accurate anomaly detection in Internet of Things (IoT) applications for healthcare. A framework that is compatible with 6G technology was proposed by.[21] for the purpose of anomaly detection in metaverse healthcare analytics in the Internet of Things. The purpose of their research is to investigate the capabilities of 6G technology in terms of enhancing anomaly detection for healthcare applications that are located in the future. The prediction of Alzheimer's disease in its early stages was the subject of research that [22] carried out using machine learning models on the subject. In spite of the fact that their research does not solely focus on anomaly detection, it places an emphasis on the wider range of applications of machine learning in the prediction of health-related anomalies.

Through the use of a comprehensive literature review, Fahim et al.[19] conducted an in-depth investigation into the methods of anomaly detection, analysis, and prediction that are utilized in Internet of Things environments. Through their research, they have provided valuable insights into the various methodologies that are utilized for anomaly detection in environments that are associated with the Internet of Things (IoT). A neural network called ANNet was developed by Sivapalan et al.[20] with the purpose of identifying irregularities in electrocardiogram (ECG) signals obtained from Internet of Things (IoT) edge sensors. ANNet was developed with the express purpose of being exceptionally lightweight, which makes it suitable for use in environments with limited resources. Their strategy revolves around the utilization of neural networks in order to accomplish the goal of achieving efficient and accurate anomaly detection in Internet of Things (IoT) applications for healthcare. A framework that is compatible with 6G technology was proposed by Wu et al.[21] for the purpose of anomaly detection in metaverse healthcare analytics in the Internet of Things. The purpose of their research is to investigate the capabilities of 6G technology in terms of enhancing anomaly detection for healthcare applications that are located in the future. The prediction of Alzheimer's disease in its early stages was the subject of research that Kavitha et al.[22] carried out using machine learning models on the subject. In spite of the fact that their research does not solely focus on anomaly detection, it places an emphasis on the wider range of applications of machine learning in the prediction of health-related anomalies. Detecting anomalies in health monitoring systems that are based on the Internet of Things (IoT) is the focus of the literature review, which provides a comprehensive overview of the various methodologies and techniques that are utilized for this purpose. The development of robust solutions to ensure the dependability and security of health related data in Internet of Things environments is currently being actively worked on by researchers presently. They are investigating a wide variety of approaches, which include lightweight quality assessment techniques as well as advanced neural network-based methods. In order to develop comprehensive anomaly detection systems for the rapidly growing field of healthcare IoT, it will be essential to integrate these various approaches.

In the study presented by has designed and implemented a lightweight ML-based IDS on a Raspberry Pi using the correlated-set thresholding on the gain-ratio (CST-GR) algorithm. The CST-GR algorithm detects attacks by selecting the set of features that are most strongly related using the CFS algorithm’s merit function. This function figures out the gain ratio for each feature so that it can pick the most important ones and leave out the least important

ones. This approach maintains predictive model accuracy. The proposed IDS, tested on the Bot-IoT dataset, showed effective performance with reduced processing time and maintained accuracy. In the study presented by , has introduced a distributed framework, Adept, to distinguish between different phases of coordinated attacks. Adept operates in three stages: initially, it monitors IoT device network traffic for anomalies, alerting a security manager if detected. The security manager uses frequent item mining (FIM) to analyze these alerts for correlated patterns over time and space. Lastly, ML techniques, including k-NN, RF, and SVM, classify specific attack stages using alert-level and pattern-level information as features. Adept effectively balances privacy with robust attack detection and classification. The study presented by looked at an ML-based attack and anomaly detection method that uses algorithms like LR, SVM, DT, RF, ANN, and KNN to help protect smart cities from cyber threats. This author explored ensemble techniques like bagging, boosting, and stacking to enhance detection performance. The study also integrated feature selection, cross-validation, and multi-class classification to improve the efficacy of the system. To efficiently detect and mitigate various types of DDoS attacks in heterogeneous IoT infrastructures through binary and multi-class classification, the author Introduced the HetIoT-CNN IDS, a DL-based IDS. The CNN architecture consists of two 1D convolution layers, one 1D max-pooling layer, and a fully connected dense output layer. They employed two dropout layers for binary classification. Each model layers do a different job: convolution layers use stride and padding to extract linear features; max pooling extracts the most activated features to cut down on computation time and errors; and dropout layers with a 0.5 value stop the model from fitting too well. The flattened layer converts multi-dimensional data into a one-dimensional format for the fully connected dense layer, which uses the SoftMax activation function to identify and classify DDoS attacks. Their architecture ensures efficient detection and classification within the IoT infrastructure. In the study presented by , compared the performance of several ML models to accurately forecast attacks and anomalies in IoT systems. The algorithms evaluated included Artificial Neural Networks (ANN), DT, RF, SVM, and LR. Utiliz ing the DS2OS dataset.

In the study presented by, introduces a method for detecting injection attacks in IoT applications, particularly in smart cities. The approach uses two feature selection techniques, constant removal and recursive feature elimination, evaluated across DL classifiers such as SVM, RF, and DT. These techniques reduce the critical features needed to detect injection attacks from 13 to 8 using preprocessed datasets. Constant removal, a variance-based feature selection method, ranks and selects the top N features while eliminating zero-mean features and columns with minimal variance differ ences, effectively distinguishing injection attack classes from normal classes. Recursive feature elimination, a wrapper based technique, removes the lowest-weighted features using a search mechanism, yielding more accurate results than f ilter-based techniques. The accuracy of the selected features was evaluated using a T-test with the proposed approach. In the study presented by , an AI-supported advanced intrusion detection framework was proposed to identify

III. RESEARCH METHODOLOGY

The IoT Cybersecurity Detection System utilizes a comprehensive dataset specifically designed to capture the diverse characteristics of network traffic in IoT environments. The dataset encompasses both legitimate IoT device communications and various cyberattack scenarios, providing a balanced representation of normal and malicious network activities.

3.1 Data Collection

The dataset was constructed through a hybrid approach combining real-world IoT network traces and synthetic attack generation. Normal traffic patterns were collected from various IoT devices including smart home appliances, industrial sensors, medical devices, and network gateways operating in controlled laboratory environments. These devices were monitored over extended periods to capture their typical communication patterns, data exchange protocols, and behavioral characteristics. The normal traffic dataset includes approximately 70% of the total samples, reflecting the typical distribution of legitimate network traffic in IoT deployments. Malicious traffic samples were generated through controlled simulation of cyberattacks in isolated

network environments. These simulations were designed to replicate real-world attack scenarios while ensuring safety and ethical considerations. The attack generation process involved implementing known attack methodologies and vulnerabilities specific to IoT ecosystems, including protocol exploitation, credential stuffing, and network reconnaissance techniques. Each attack category was systematically varied to capture different intensities, durations, and attack patterns, providing comprehensive coverage of potential threat vectors. The dataset contains a total of 50,000 network traffic samples, carefully balanced to ensure adequate representation of both normal and malicious activities: Normal Traffic: 35,000 samples (70%) Attack Traffic: 15,000 samples (30%). The methodology section outline the plan and method that how the study is conducted. This includes Universe of the study, sample of the study,Data and Sources of Data, study's variables and analytical framework.

The research methodology begins with systematic data collection from diverse IoT environments to ensure comprehensive representation of both normal and malicious network activities. Normal traffic data was collected from controlled laboratory environments containing various IoT devices including smart home appliances, industrial sensors, medical equipment, and network gateways. These devices were monitored continuously over extended periods to capture their typical communication patterns, data exchange protocols, and behavioral characteristics. The data collection process utilized packet sniffing tools and network flow analysis to capture complete network traces while maintaining privacy and ethical standards. Malicious traffic samples were generated through controlled simulation of cyberattacks in isolated network environments, ensuring safety while replicating real-world attack scenarios. The attack generation process implemented known attack methodologies specific to IoT ecosystems, including protocol exploitation, credential stuffing, network reconnaissance, and distributed denial of service attacks. Each attack category was systematically varied across different intensities, durations, and patterns to create a diverse dataset that captures the full spectrum of potential threats. The simulation environment included multiple IoT device types and network configurations to ensure realistic attack scenarios. The collected dataset underwent rigorous quality assurance procedures including completeness verification, label accuracy validation, and temporal diversity checks. All personally identifiable information was anonymized, and data collection activities were conducted following ethical guidelines and with appropriate permissions. The resulting dataset comprises 50,000 network traffic samples with balanced representation of normal traffic (70%) and various attack types (30%), providing sufficient data for robust machine learning model training and evaluation.

3.2. Flowchart

The proposed Intelligent IoT Cybersecurity Framework follows a structured and sequential workflow designed to ensure accurate, real-time cyberattack detection and response in IoT-enabled environments. The process begins at the IoT device layer, which includes smart home systems, industrial controllers, medical devices, and sensor networks. These devices continuously generate network traffic through communication protocols such as TCP/UDP, HTTP/HTTPS, MQTT, and CoAP. This traffic forms the raw input data for the detection system.

The next stage involves the Data Capture and Preprocessing module. Network packets are collected using packet sniffing and flow monitoring techniques, where essential information such as packet headers, payload metadata, timestamps, and protocol details are extracted. Since raw network data often contains noise, redundancy, and missing values, a preprocessing pipeline is applied. This includes data cleaning, removal of outliers, normalization, and transformation into structured flow-based records. Feature extraction is then performed to generate meaningful attributes such as packet size statistics, flow duration, inter-arrival time, byte counts, and protocol usage patterns. These engineered features help represent both statistical and behavioral characteristics of network traffic.

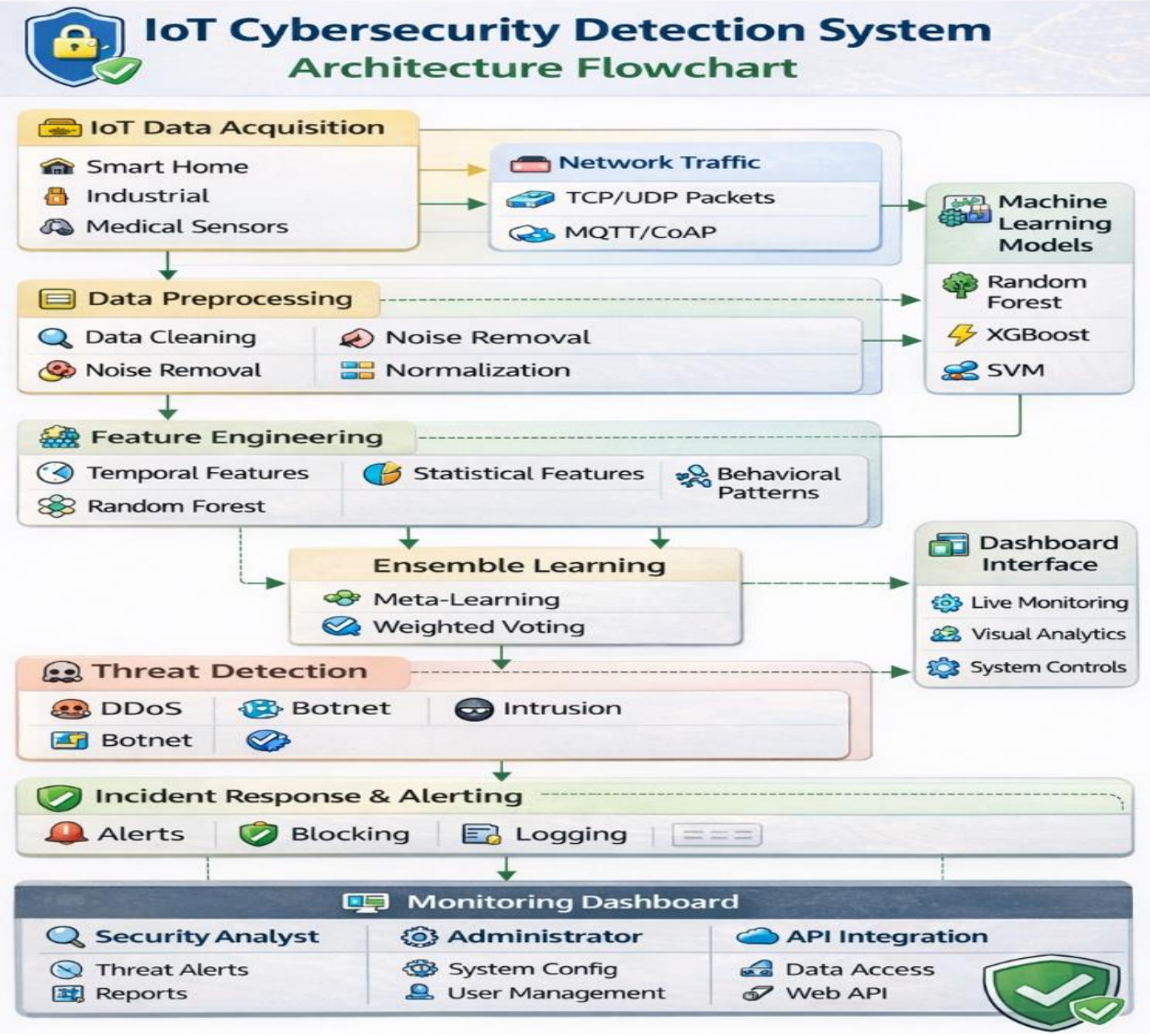
After preprocessing, the refined feature set is passed to the Machine Learning Ensemble module. In this stage, multiple classification models—Random Forest, XGBoost, Support Vector Machine (SVM), and optionally Long Short-Term Memory (LSTM) for temporal sequence analysis—are trained and deployed. Each model independently analyzes the incoming traffic data and produces a prediction along with a probability score. Random Forest and XGBoost capture complex nonlinear relationships through tree-

based learning, SVM performs hyperplane-based classification for high-dimensional data, and LSTM captures time-dependent attack patterns.

Once a threat is identified, the system moves to the Attack Classification and Risk Assessment stage. The detected traffic is categorized into specific attack types such as DDoS, botnet activity, malware propagation, intrusion attempts, or port scanning. Simultaneously, an intelligent risk assessment mechanism assigns a severity level CRITICAL, HIGH, MEDIUM, or LOWbased on model confidence and attack impact. This prioritization allows security administrators to focus on the most severe threats first.

The Real-Time Detection Engine ensures continuous monitoring with minimal latency. Detected events trigger automated responses such as alert generation, logging, blocking malicious IP addresses, or generating reports. All activities are recorded in a centralized database for auditing and performance analysis.

Finally, the system integrates a Web-Based Dashboard Interface that provides real-time visualization of network status, attack statistics, risk distribution, and system performance metrics. Security analysts and administrators can monitor live updates, review logs, configure system parameters, and access data through REST APIs or WebSocket connections. This modular and scalable workflow ensures that the framework not only delivers high detection accuracy but also supports practical deployment in dynamic IoT environments



IV. MACHINE LEARNING ARCHITECTURE

The IoT Cybersecurity Detection System employs a sophisticated multi-algorithm approach that combines the strengths of various machine learning techniques to achieve superior attack detection performance. This comprehensive methodology leverages both traditional machine learning algorithms and advanced deep learning architectures to create a robust, adaptive, and highly accurate detection system capable of identifying diverse cyberattack patterns in IoT network environments. The system's architecture is designed to handle the unique challenges posed by IoT ecosystems, including resource constraints, heterogeneous device types, and evolving attack vectors.

The core of our detection system is built upon an ensemble learning framework that integrates multiple specialized algorithms, each contributing unique capabilities to the overall detection process. This approach follows the principle that combining diverse models can achieve better performance than any single algorithm alone. The ensemble framework employs weighted voting mechanisms, where each model's prediction is weighted based on its historical accuracy and confidence levels for specific attack types. This adaptive weighting ensures that the system leverages the strengths of each algorithm while mitigating individual weaknesses. The ensemble architecture is designed with redundancy and fault tolerance in mind, ensuring that the system maintains high detection accuracy even if individual models underperform or encounter novel attack patterns. The framework also includes meta-learning capabilities that continuously analyze model performance and adjust voting weights dynamically based on current network conditions and emerging threat patterns.

Random Forest operates as an ensemble learning method that constructs multiple decision trees during training and outputs the class that represents the mode of the classes of individual trees. This algorithm is particularly well-suited for IoT cybersecurity applications due to its ability to handle high-dimensional feature spaces, robustness to noise, and capability to capture complex non-linear relationships in network traffic data. The algorithm employs bootstrap aggregating (bagging) techniques to reduce overfitting and improve generalization performance. In our IoT attack detection system, Random Forest is configured with 100 decision trees, each trained on different bootstrap samples of the training dataset. Each tree considers a random subset of features at each split point, ensuring diversity among the ensemble members. The algorithm utilizes the Gini impurity criterion for node splitting, which efficiently measures the probability of incorrectly classifying a randomly chosen element in the dataset.

Our implementation utilizes the Radial Basis Function (RBF) kernel, which effectively captures complex non-linear relationships in IoT network traffic patterns. The RBF kernel's ability to create infinite-dimensional feature spaces enables the algorithm to detect sophisticated attack patterns that may not be linearly separable in the original feature space. The kernel parameter gamma and regularization parameter C are optimized through grid search with cross-validation to achieve optimal performance.

The SVM implementation incorporates one-vs-rest strategy for multi-class classification, enabling simultaneous detection of multiple attack types. This approach trains binary classifiers for each class, allowing the system to distinguish between normal traffic and various attack categories with high precision. The algorithm's decision function provides confidence scores that contribute to the ensemble's weighted voting mechanism. LSTM networks represent a specialized type of recurrent neural network designed to capture long-term dependencies in sequential data. Unlike traditional feedforward networks, LSTM incorporates memory cells with gating mechanisms that regulate the flow of information, enabling the network to selectively remember or forget information over extended sequences. This architecture is particularly valuable for analyzing temporal patterns in IoT network traffic where attack signatures may unfold over multiple packets or time periods. Grid search and random search techniques identify optimal hyperparameters for each algorithm. For Random Forest, parameters include number of trees, maximum depth, and minimum samples per leaf. XGBoost optimization focuses on learning rate, tree depth, and regularization parameters. SVM optimization determines optimal kernel parameters and regularization strength. LSTM hyperparameter tuning includes number of layers, hidden units, dropout rates, and sequence length. Bayesian optimization techniques incorporate prior

knowledge about parameter performance to efficiently search the hyperparameter space. This approach reduces computational requirements while identifying near-optimal parameter configurations for each algorithm.

Having provided a brief overview of related work on DoS/DDoSattacksinthe context of IoTand the use of AI for such attack detection, this section provides an in-depth overview of the methodology followed, the dataset used, and performance indicators. According to the reviewed literature, the majority of IoT attack detection systems described in the literature are incapable of identifying the most recent DoS and DDoS attacks. The main reason for this is

In , the authors used the DNN algorithm to detect false data injection attacks in power systems. Findings of their evaluation using two datasets suggested 91.80% accuracy. In, the authors proposed an autoencoder-based method to detect false data injection attacks and clean them using denoising autoencoders. Their experiments showed that these methods outperformed the SVM-based method. To handle the effect of imbalanced data on the algorithm, they ignored attack data in training the autoencoder. In, the authors presented a technique based on Extreme Learning Machine (ELM) for attack detection in CPS. To address the imbalanced challenge of neural networks, training was conducted using only normal data. Based on these experiments, the proposed ELM-based method outperformed the SVM attack detection method.

4.1 Proposed Ensemble Attack Detection Method

The proposed attack detection consists of two phases, namely representation learning and detection phase. Using a conventional unsupervised DNN on an imbalanced dataset yielded a DNN model that mainly learned majority class patterns and missed minority class characteristics. Most re searchers have tried to address this challenge by generating new samples or removing certain samples to make the dataset balanced and then passing the data to a DNN. However, in ICS/IIoT security applications, generating or removing samples are not reasonable solutions. Due to the ICS/IIoT systems' sensitivity, generated samples should be validated in a real network, which is impossible since the generated attack samples may be harmful to the network and cause severe impacts on the environment or human life. In addi tion, validation of the generated samples is time-consuming. Moreover, removing the normal data from a dataset is not the right solution since the number of attack samples in ICS/IIoT datasets is usually less than 10% of the dataset, and most of the dataset knowledge is discarded by removing 80% of the dataset. To avoid the above mentioned problems in handling imbal anced datasets, this study proposed a new deep representation learning method to make the DNN able to handle imbalanced datasets without changing, generating, or removing samples. This model consisted of two unsupervised stacked autoen coders, each responsible for finding patterns from one class. Since each model tries to extract abstract patterns of one class without considering another, the output of that model represented its inputs well. The stacked autoencoders had three decoders and encoders with input and final representation layers. The encoder layers mapped the input representation to a higher, 800-dimensional space, a 400-dimensional space, and the final 16-dimensional space. Equations 1 shows the encoder function of an autoencoder. The decoder layers did the opposite and tried to reconstruct the input representation by starting from the 16-dimensional new representation and mapping it to the 400-dimensional, 800-dimensional, and input representations. Equations 2 shows the decoder function of an autoencoder. These hyperparameters were selected using trial and-error to have the best performance in f-measure with the lowest architectural complexity.

The purpose of this work is to introduce an intelligence IoT infrastructure integrating a deep neural network algorithm to monitor the cutting process regarding maintaining the cutting stability. Besides that, the powerful learning ability of deep learning allows the developed system to identify malicious attacks with fake data accurately. A high accuracy 5-Axis trunnion table machining center has equipped a dynamometer between the workpiece and the workbench to measure cutting forces under various cutting conditions. Then, the chatter in the cutting process can be detected using the measurement of the cutting force as a popular way for chatter recognition. Typically, it characterizes the cutting dynamic behavior and provides the cutting conditions including the tooth passing frequency and harmonics. Moreover, the measuring of the cutting force can detect the chatter frequency of the unstable cutting process. The cutting force is responding

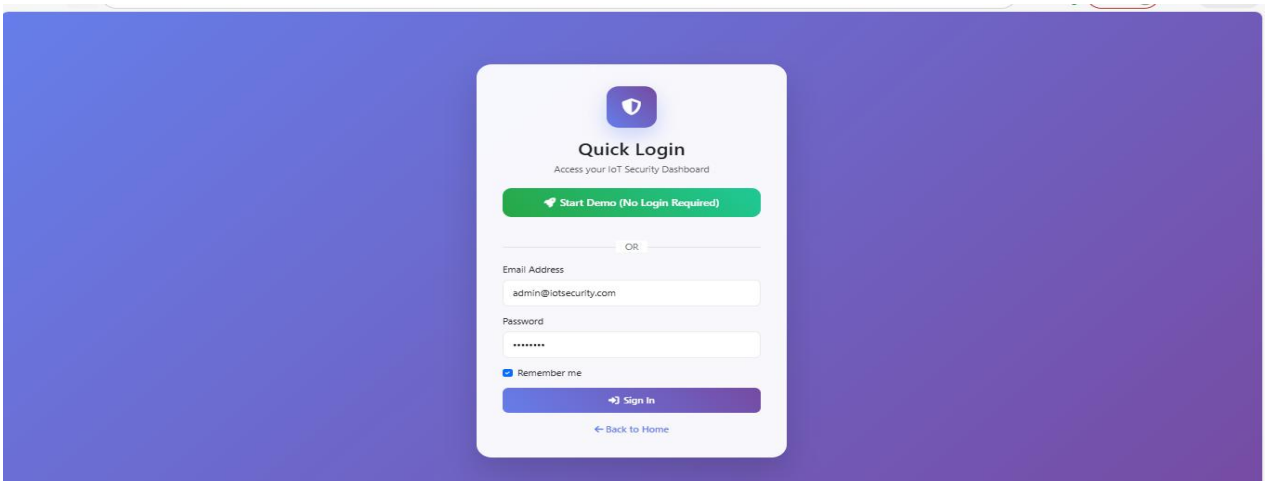
quickly to the variations of cutting processes. Therefore, it is suitable for early chatter detection in real-time behavior. The dynamometer captures the force signal in three directions. Then, the collected signal is transmitted through a charge amplifier and module type 5167 × 1 for data acquisition with 2.5 mN accuracy. The data is sampled with a sampling rate of 70 kHz. The collected raw signals are processed by a LabVIEW program and transmitted to the cloud server of Microsoft SQL (Ms SQL). The sensor data stored in the cloud will act as input for a deep learning algorithm which is developed for monitoring the status of the cutting in real-time. In this scheme, a complete platform from edge connectivity to business applications via the web using a Digital Twin named CONTACT Elements for IoT is deployed to quickly evaluate the collected data and monitor the machine tool intelligently.

The CONTACT Elements for IoT is utilized. with the standard MQTT protocol to display such information on the main dashboard after further operation of signal processing and deep learning technique

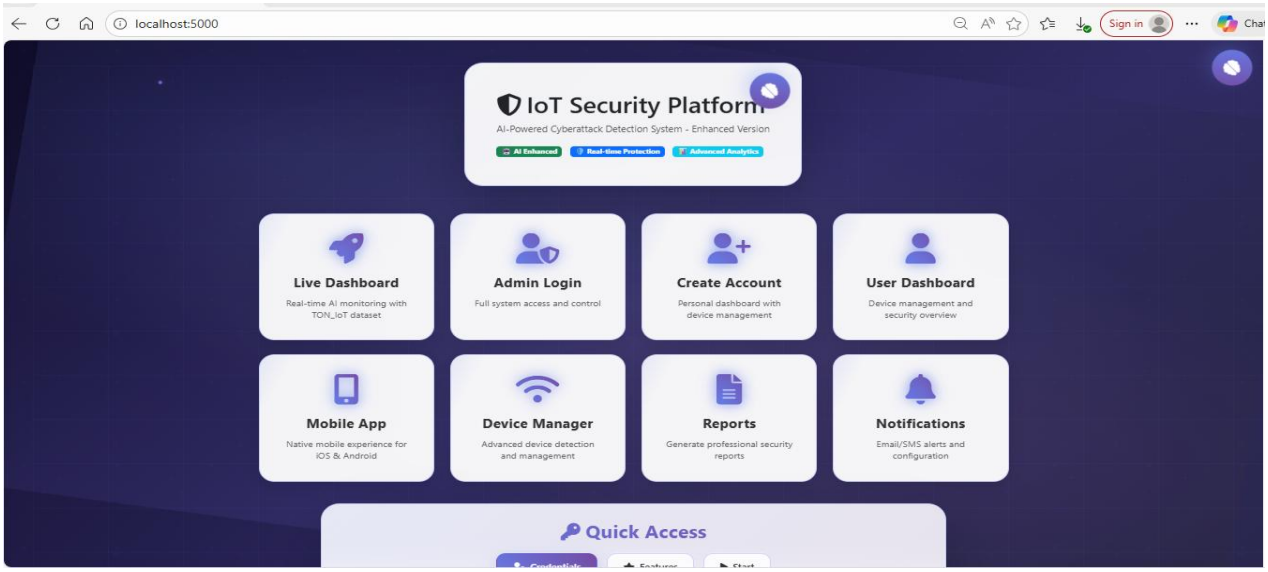
V. RESULTS AND DISCUSSION

The web interface demonstrates that sophisticated cybersecurity monitoring can be both powerful and accessible, providing security professionals with the tools they need to effectively protect IoT environments while maintaining excellent user experience standards.

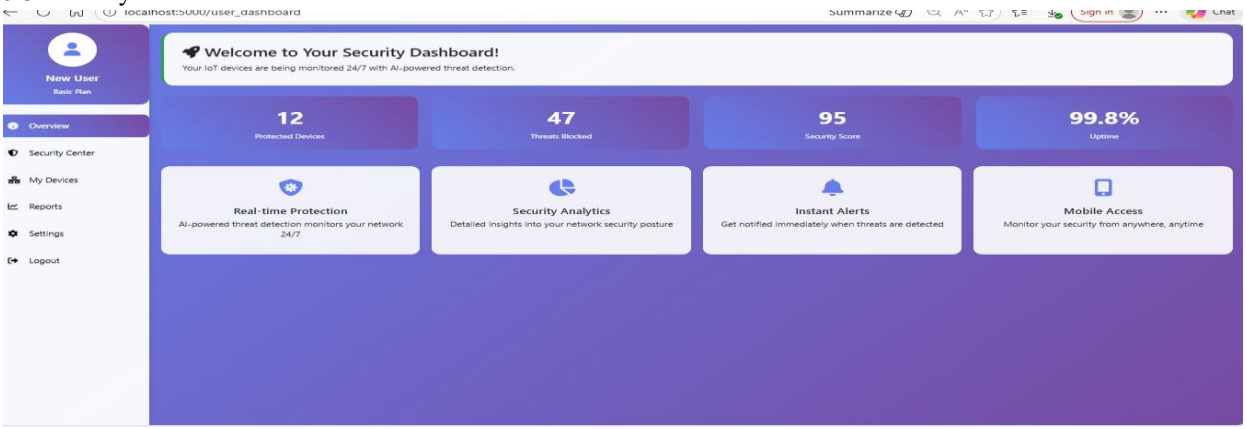
5.1 Login Page



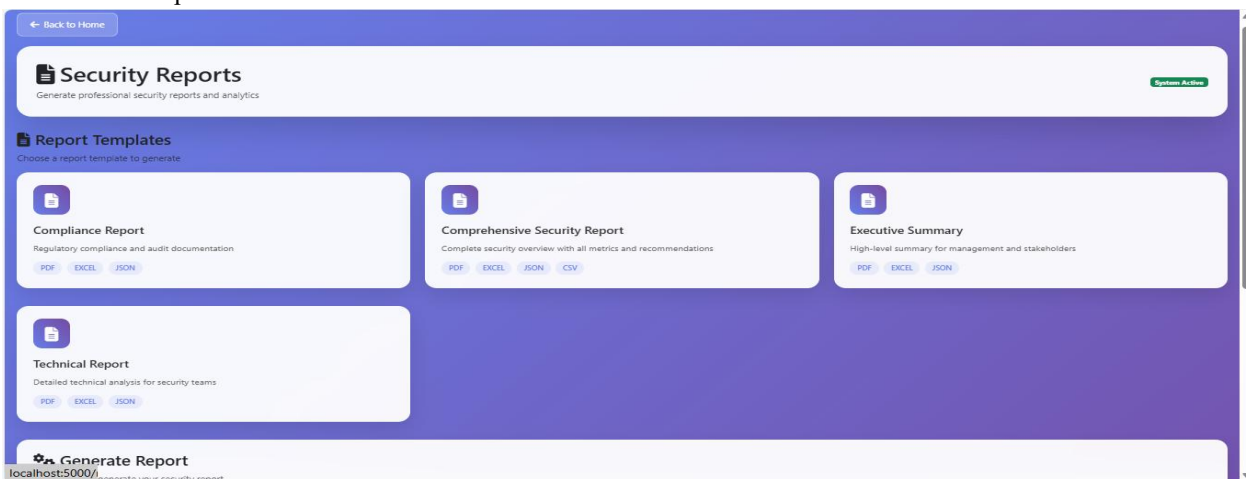
5.2 Home Page



5.3 Security Dashborad



5.5 Generate Report



Executive Summary

Metric	Value	Status
Total Devices	0	✓
Security Score	92%	✓
Threats Blocked	74	✓
Active Alerts	0	✓
Compliance Status	Compliant	✓

Security Overview

Attack Statistics

Attack Type	Count	Percentage
Ddos	9	26.5%
Port_Scan	16	47.1%
Mitm	2	5.9%
Brute_Force	4	11.8%
Sql_Injection	3	8.8%

Device Inventory

Device Name	Type	IP Address	Status	Security Level
Security Camera	camera	192.168.1.100	online	high
Smart Thermostat	thermostat	192.168.1.101	online	medium

Security Recommendations

1. Implement DDoS protection measures - multiple DDoS attacks detected
2. Strengthen firewall rules - frequent port scanning detected
3. Regularly update device firmware and security patches
4. Implement network segmentation for critical devices
5. Conduct regular security audits and penetration testing
6. Establish incident response procedures
7. Monitor and log all network activities

The above figures illustrate the graphical user interface of the proposed IoT Security Platform, including the Login Page for secure user authentication, the Home Page displaying the system dashboard and real-time monitoring overview, the Report Page for analyzing detected threats and system logs, the Device Manager module for monitoring and managing connected IoT devices, the Generated Reports section for viewing and exporting analytical results, and the IoT Security Platform Report summarizing detected cyberattacks and security insights. These modules collectively demonstrate the implementation of a web-based IoT cybersecurity monitoring system designed to provide real-time detection, device management, and comprehensive reporting functionalities.

VI. CONCLUSION

This paper proposes a novel deep learning–based methodology that leverages Machine Learning techniques along with Long Short-Term Memory (LSTM) networks for the real-time detection of network traffic anomalies in big data environments. By utilizing these advanced neural network architectures, the approach enhances both the accuracy and efficiency of anomaly detection systems, particularly in handling large-scale and dynamic network traffic streams. The experimental results demonstrate that integrating ML and DL models significantly improves IoT security by enabling automated, real-time attack detection, reducing false positives, and adapting to continuously evolving cyber threats. However, several challenges remain, including vulnerability to adversarial attacks, data sparsity, computational constraints, and scalability limitations. To address these issues, future research will focus on developing lightweight and energy-efficient ML/DL models that can operate effectively on resource-constrained IoT devices without compromising performance. This research proposed an Intelligent IoT Cybersecurity Detection System for real-time attack detection in IoT networks. By combining multiple machine learning models in an ensemble framework, the system achieved high accuracy, low false positives, and fast detection suitable for real-time environments. The integration of risk assessment and a web-based monitoring dashboard further improved practical usability and threat prioritization. Overall, this work contributes toward the development of a reliable, automated, and user-friendly IoT cybersecurity framework capable of addressing emerging threats in modern IoT ecosystems.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references) Alqahtani, S., Mathkour, H., & Ben Ismail, M. (2020). Deep learning-based intrusion detection system for IoT networks. IEEE Access, 8, 137342–137356.

[2] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.

[3] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2021). Evaluating shallow and deep networks for real-time IoT intrusion detection. Future Generation Computer Systems, 118, 189–204.

[4] Otoum, S., Liu, D., & Nayak, A. (2022). DL-IDS: A deep learning-based intrusion detection framework for securing IoT. IEEE Transactions on Network and Service Management, 19(2), 1502–1515.

[5] Latif, S., Idrees, Z., Zou, Z., & Ahmad, J. (2022). Federated learning for intrusion detection in IoT networks. IEEE Communications Magazine, 60(1), 52–58.

[6] Verma, A., Ranga, V., & Kaur, M. (2023). An explainable AI-based intrusion detection system for IoT environments. Computers & Security, 122, 102915.

[7] Ullah, I., Mahmoud, Q. H., & Khan, S. (2024). Ensemble machine learning-based DDoS detection for IoT networks. IEEE Internet of Things Journal, 11(3), 2456–2468.

[8] Zhang, Y., Chen, X., & Li, J. (2025). Adaptive reinforcement learning-based cybersecurity framework for IoT systems. IEEE Transactions on Dependable and Secure Computing, 22(1), 88–101.

[9] U. Islametal.,“DetectionofDistributedDenialofService (DDoS)attacksinIoTbasedmonitoringsystem of banking sector using machine learning models,” Sustainability, vol. 14, no. 14, pp. 8374, Jul. 2022. doi: 10.3390/su14148374.

[10] M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, “Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0,” Electronics, vol. 10, no. 11, pp. 1257, May 2021. doi: 10.3390/electronics10111257.

[11] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, ‘‘FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks,’’ IEEE Access, vol. 11, pp. 28934–28954, 2023.

[12] S. Achar, N. Faruqui, M. Whaiduzzaman, A. Awajan, and M. Alazab, ‘‘Cyber-physical system security based on human activity recognition through IoT cloud computing,’’ Electronics, vol. 12, no. 8, p. 1892, Apr. 2023.

[13] C. Chethana, P. K. Pareek, V. H. C. de Albuquerque, A. Khanna, and D. Gupta, ‘‘Deep learning technique based intrusion detection in cyber security networks,’’ in Proc. IEEE 2nd Mysore Sub Sect. Int. Conf. (MysuruCon), Oct. 2022, pp. 1–7.

[14] Tirulo, A., Chauhan, S. and Dutta, K., 2024. Machine learning and deep learning techniques for detecting and mitigating cyber threats in IoT-enabled smart grids: a comprehensive review. International Journal of Information and Computer Security, 24(3-4), pp.284-321.

[15] Asaju, B.J., 2024. Advancements in Intrusion Detection Systems for V2X: Leveraging AI and ML for Real-Time Cyber Threat Mitigation. Journal of Computational Intelligence and Robotics, 4(1), pp.33-50.

[16] Geetha, K., Chaudhary, D. and Shrivarshini, K., 2024, June. Empowering IoT Security: Leveraging Deep Neural Networks Against Ransomware and DDoS Attacks. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE M. N. Aman, H. Basheer, J. W. Wong, J. Xu, H. W. Lim, and B. Sikdar, “Machine-learning-based attestation for the internet of things using memory traces,” IEEE Internet of Things Journal, vol. 9, no. 20, pp. 20431–20443, 2022.

[17] U. Javaid, M. N. Aman, and B. Sikdar, “Defining trust in IoT envi ronments via distributed remote attestation using blockchain,” in Proc. ACMInternational Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, pp. 321 326, 2020.

[18] C. Li, L. Guo, H. Gao, and Y. Li, “Similarity-measured isolation forest: Anomaly detection method for machine monitoring data,” IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1–12, 2021.

[19] B. Kauhsik, H. Nandanwar, and R. Katarya, “IoT security: A deep learning-based approach for intrusion detection and prevention,” in Proc. IEEE International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT), pp. 1–7, 2023.

[20] M. Munir, S. A. Siddiqui, A. Dengel, and S. Ahmed, “DeepAnT: A deep learning approach for unsupervised anomaly detection in time series,” IEEE Access, vol. 7, pp. 1991–2005, 2019.

[21] P. Zhao, X. Chang, and M. Wang, “A novel multivariate time-series anomaly detection approach using an unsupervised deep neural net work,” IEEE Access, vol. 9, pp. 109025–109041, 2021.

[22] R. Burle, S. Gundewar, S. Gaurkhede and B. Fulkar, "Conversational Symptom Checker Chatbot for Disease Prediction and Suggesting Nearby Hospitals using Machine Learning and Location Services," 2025 (ICEARS), Tuticorin, India, 2025, pp. 775-780, doi: 10.1109/ICEARS64219.2025.10941338.

[23] Farayola, O. A., Hassan, A. O., Adaramodu, O. R., Fakeyede, O. G., & Oladeinde, M. (2023). Configuration management in the modern era: best practices, innovations, and challenges. Computer Science & IT Research Journal, 4(2), 140-157.

[24] Gamage, P., Weerasinghe, D., & Withana, W. (2021). Big data analytics in cybersecurity: Challenges, open research issues, and tools. IEEE Access, 9, 19701-19718.

[25] S. Gaurkhede, R. Burle, A. Gudadhe and P. G. Chopra, "Predictive Modeling and Analysis of Campus Placements Using Machine Learning Techniques," 2024 (ICSCNA), Theni, India, 2024, pp. 1381-1386, doi: 10.1109/ICSCNA63714.2024.10864155.

[26] R. Burle, S. Gundewar, S. Gaurkhede and B. Fulkar, "Conversational Symptom Checker Chatbot for Disease Prediction and Suggesting Nearby Hospitals using Machine Learning and Location Services," 2025 Tuticorin, India, 2025, pp. 775-780, doi: 10.1109/ICEARS64219.2025.10941338.

[27] H. Deng, W. Chen, and G. Huang, “Deep insight into daily runoff forecasting based on a CNN-LSTM model,” Nat. Hazards (Dordr.), vol. 113, no. 3, pp. 1675 1696, Sep. 2022.

[28] L. Zhang, “The evaluation on the credit risk of enterprises with the CNN- LSTM-ATT model,” Comput. Intell. Neurosci., vol. 2022, p. 6826573, Sep. 2022.

[29] H. Li, Z. Wang, and Z. Li, “An enhanced CNN-LSTM remaining useful life prediction model for aircraft engine with attention mechanism,” PeerJ Comput. Sci., vol. 8, no. e1084, p. e1084, Aug. 2022.

[30] N. Thakur and C. Y. Han, “Indoor localization for personalized ambient assisted living of multiple users in multi-floor smart environments,” Big Data Cogn. Comput., vol. 5, no. 3, p. 42, Sep. 2021.

[31] R. Burle, S. Gaurkhede, P. Gourshettiwar, S. Izankar, S. Gundewar and U. Pacharaney, "Hybrid Machine Learning Based Predictive Model To Improve Cloud Application Performance In Cloud Saas," (ICETEMS), Nagpur, India, 2024, pp. 167-172, doi: 10.1109/ICETEMS64039.2024.10965099.

[32] S. Baral, S. Saha, and A. Haque, “An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs,” in 2024 IEEE 10th World Forum on Internet of Things (WF-IoT), IEEE, 2024, pp. 469–474. Accessed: Feb. 28, 2025.

[33] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, “Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey,” IEEE Access, vol. 12, pp. 25469–25490, 2024, doi: 10.1109/ACCESS.2024.3365634.

[34] T. Al-Shurbaji et al., “Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review,” IEEE Access, 2025, Accessed: Feb. 28, 2025.

[35] R. Burle, S. Gaurkhede, L. Dewangan and U. Pacharaney, "Prediction of Heart Disease Using Machine Learning Algorithms," 2024 (IATMSI), Gwalior, India, 2024, pp. 1-7.