Date available online: 30-06-2026
Vol. 4, Issue 1 (January - June 2026)

DOI: https://doi.org/10.24312/ucp-jeit.04.01.885

Design and Implementation of Integrated Security Solutions Using Internet of Things and Artificial Intelligence

Ghazanfar Rehman[1], Anayat Ali[2], Namsh Ghauri[3], Zia Ul Rehman[4]

[1]Central Technologies Inc., Canada (e-mail: rey@centraltechonologies.ca)
[2]Central Protection Services Inc., Canada (e-mail: aanayat@centralprotection.ca)
[3]Central Technologies Inc., Canada (e-mail: nghauri@centraltechonologies.ca)
[4]Department of Computer Science, Government College University Lahore, Pakistan (e-mail: ziaulrehman@gcu.edu.pk)

*Corresponding author: Ghazanfar Rehman (e-mail: rey@centraltechonologies.ca).

ABSTRACT

In recent years, the need for advanced security systems has increased due to rapid urban development and the growing use of smart technologies. Traditional security approaches often depend on manual monitoring, which limits their effectiveness in handling complex and evolving threats. This study presents the design and development of an integrated security system that combines Internet of Things (IoT) devices with Artificial Intelligence (AI) techniques. The proposed solution uses connected sensors, surveillance devices, and intelligent algorithms to monitor environments and detect threats in real time. Firstly, the data is gathered through these edge devices, this data can vary in form. Some of the data gets processed near the source of its production. This pre-processed data becomes more efficient for data transmission. Any immediate threat can also be detected during this pre-processing. Once the data is transmitted it is analyzed by more advanced AI algorithms. Pattern recognition is also performed during this. The system is designed to improve situational awareness, reduce the reliance on human intervention, and enable a faster response to security incidents. It achieved significantly higher detection accuracy (up to 98.7%) and improved system performance compared to conventional security approaches.

INDEX TERMS: Artificial Intelligence, Edge Computing, Integrated Security System, IoT, Real-Time Monitoring, Smart Surveillance, Wireless Sensor Networks

I. INTRODUCTION

Security has become an essential requirement in modern environments such as smart cities, industrial setups, and commercial spaces. Conventional surveillance systems mainly rely on human operators to monitor activities, which can lead to delays, inefficiencies, and errors. We have moved from the need of traditional security systems to the requirement of highly advanced security systems which not only detects threats but are also able to take efficient decisions.

Efficient decision-based security systems are now being introduced in the mix of conventional surveillance systems. The idea behind this technology is to facilitate ever growing urban population to keep security risks at minimum. This idea requires not only for threats to be identified but also have an informed decision made regarding it. Such an idea can be implemented with the collective use of IoT based devices and AI systems.

With the advancement of connected technologies, more intelligent solutions are now possible. IoT enables devices to communicate and share data efficiently, while AI allows systems to analyze that data and make informed decisions. Together, these technologies create opportunities for automated and intelligent security systems.

This research introduces a unified security framework that integrates IoT devices with AI-based analysis. The aim is to provide a system that can monitor activities continuously, detect unusual behavior, and respond quickly to potential threats. Additionally, the proposed system introduces a hybrid edge-cloud architecture that enhances real-time processing and reduces latency compared to existing models.

The overall aim of this framework is to provide better security in this ever-evolving world. Threat levels need to remain low despite the growing population and its development. Traditional systems that provided security were highly dependent on human supervision and control. For a vastly connected world there is a need for vastly connected security system that can make accurate and efficient decisions on the spot without human intervention.

II. LITERATURE REVIEW AND COMPARATIVE ANALYSIS

IoT edge devices are used in combination with various other technologies to present a security system in various fields of life such as, smart home systems and smart cities with their state-of-the-art security systems. A research study [1] focused on cyber-threats encountered in a smart city system. A smart city network and its IoT devices are linked to much larger cloud servers and hence are exposed to higher number of attacks and threats. The paper [1] explored various types of attacks

and in turn devised varying measures to deal with such attacks. Various Machine Learning (ML) algorithms, namely, Logistic Regression (LR), Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbors (KNN) and Artificial Neural Network (ANN) were used to defend against malicious cyber-security threats in a smart city. The detection system's performance was improved with the techniques such as boosting, stacking, and bagging. Along with this, the techniques of feature selection, multi-class classification and cross validation were incorporated. The results showed an accurate detection of cyberattacks.

Manual monitoring of data for security purposes is considered tedious and is susceptible to errors. Taking this into account, a paper [2] proposed the use of LSTM-based deep learning. It was used for anomaly detection in real-time video-graphic data. It was used to monitor traffic and security. For feature selection the method made use of hybrid spatio-temporal technique. It used LSTM (Long Short-Term Memory) and CNN (Convolutional Neural Network). It extracted not only spatial features but also temporal motion patterns in video sequences. Sequentially dependent information was learned through the LSTM model. This helped in accurate identification of abnormal events that were time sensitive. Various ML (such as Histogram-Based Gradient Boosting, Extreme Gradient Boosting, K-Nearest Neighbor) models were used after feature extraction. Extreme Gradient Boosting (XGBoost) showed best performance with 98% accuracy.

Research [3] proposed a novel method of machine learning classifiers to improve security provided by IoT systems. After studying the various security threats encountered in an IoT based security setup the paper proposed an ML security system that was able to deal with such attacks autonomously. An accurate classifier among the 7 ML based algorithms was to be selected for the AI reaction agent. This was done in the implementation phase of the agent. Through this step attack patterns were identified in the network of the IoT devices. The rapid use of IoT devices and growth of cloud computing has led to an increase in cyber-attacks in this area. A paper [4] proposed a unique framework for anomaly detection. This framework made use of OCSVM (One-Class Support Vector Machine) and IF (Isolation Forest), which are two unsupervised machine learning algorithms. In addition to them, CSAD (Combined Scoring Anomaly Detection) were used for comparative analysis. OCSVM proved to have the best results among the three.

Another technology that showed improved security in IoT based devices was the incorporation of Blockchain and AI. A paper [5] proposed an architecture of 3 layers which focused on cloud layers, devices and edge. The architecture took into account legitimacy scores and in turn took care of initial security concerns. Serving as a prospective trapdoor property, the architecture made use of Ethereum based data repositioning. In addition to this, a concise evidence matrix was generated through a simplified consensus module, this improved accountability. Security was further optimized with an unconventional NN (Neural Network) method. Metaheuristic techniques were used to enhance its performance. Furthermore, a study [6] highlighted the collective use of AI and blockchain in providing a revolutionized system for smart cities. The framework made use of AI, IoT devices and cloud computing. This framework was used to not only obtain important information but also process it. The system provided results in the form of digital analytics, and in turn saved them in a decentralized cloud repositories with the help of blockchain algorithms. This framework provided an additional incentive of a secure and protected system for an application of smart city.

Research [7] focused on IoD (Internet of Drones), specifically their use in healthcare environment was conducted. The research highlighted various malicious attacks that exist in AI-enabled IoT-based drone systems in healthcare. Major issues and threats exist in the network of drones and its wireless communication with the station on the ground. For such an environment, state of the art authentication systems and access control was provided in the paper [7]. In addition to this, blockchain mechanism was introduced with authentication which provided additional security against various attacks. Another research work [8] that focused on IoT devices in healthcare highlighted the lack of protection in these devices because of its minuscule size. The research concluded that use of Blockchain with IoT in healthcare not only improved the system's security but also efficiency. The paper [8] mainly focused on three points, firstly it proposed a medical clinic which required no medical staff interference, keeping the staff safe. Secondly a deep learning detection program was introduced for identification of corona virus. Lastly, a new blockchain based secure pharmaceutical system was proposed.

A paper [9] stated AI, blockchain technology and IoT as three most important and promptly evolving technologies. It stated that a combined use of these can be very useful for cloud-based environment. The framework provided a secure, and therefore reliable system that could be used for data exchange and analysis. The framework (based on the three components) ensured data privacy and security, transparency and immutability.

Secure authentication remains a challenge in IoT. A paper [10] proposed HAC-based (Hybrid and Adaptive Cryptographic) framework for secure authentication. The paper made use of varying cryptographic techniques such as ExOR operation, hybrid encryption and hashing function, for the process of authentication. The hybrid function itself was composed of two different steps. One comprised of AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography). The other comprised of RSA (Rivest Shamir Adleman) and AES. The hybrid function was used to deal with various security flaws. When it comes to the role of 5G-IoT, it has become indispensable in smart applications and in applications of e-health. In a paper [11], patient's data in cloud is secured

through deep learning hybrid algorithms. The article proposed CNN-DMA (Convolutional Neural Network-Deep Malicious Attack), a deep learning model to detect malicious attacks based on a classifier-CNN.

A paper [12] assessed the blockchain and AI technology in different business models. Overall, the integration of these two can lead to a technology known as decentralized AI. With this new technology, the paper proposed a better AI enabled analysis and self learning on data shared and trusted on Blockchain. Decision making and collaboration was made easy for autonomous agents leading to increased system performance. Another plus point of IoT devices is its cost effectiveness. A study [13] proposed a cost-effective solution for air monitoring. It made use of blockchain technology which enhanced reliability, accessibility and overall data transparency. Three sensors, namely, MQ7 (Carbon Monoxide Sensor), MQ135 (Air Quality Sensor) and DHT11 (Digital Humidity and Temperature Sensor) were used to collect various environmental parameters such as temperature, carbon monoxide, humidity and carbon dioxide. The system introduced was consistent with eco-friendly policies and sustainable development. The data generated could be shared with various stakeholders such as researcher and government.

To better understand the performance of existing IoT-based security solutions, a comparative analysis of different research studies is presented in Table 1. This analysis focuses on AI techniques, detection accuracy, strengths, and limitations. Table 1 gives us comparison of various research studies in terms of their accuracies, strengths and limitations.

Each study has its own advantages and disadvantages, regardless of that, there is an approximate accuracy of more than 95%. Even if the studies show optimum accuracy there are some factors lacking in each. Such as study [14] is based on a system built on various AI models. Majorly various ML and Deep Learning models. Even if the research promised real world validation and user accessibility (application designed through MATLAB), a major drawback of hardware dependency existed in it. The system specifically requires 16-bit ADC (Analog-to-Digital Converter) in contrast to built in ADCs which comes with ESP32 microcontrollers. Research [15] integrates ML techniques with SDN (Software Defined Networking) and NFV (Network Function Virtualization). Furthermore, the system design makes use of monitoring agent. NFV focused on security whereas SDN dealt with traffic manipulation. This method saved energy by shifting security processing to virtualized instances of network. However, there are standardization problems with this technique, as various framework can not yet communicate among themselves.

Table 1 also shows work of a technique which used Post-Quantum Cryptography. The study [16] seems promising, it is designed specifically for 6G networks. The design was scalable however only in 6G network environment. It becomes a bit resource sensitive as it may require energy consumption which may not abode well with resource constrained devices. Another research [17] made use of various techniques, namely AI, edge computing and blockchain protocol. This integrated system designs offered scalability and decentralization but with a trade factor of communication link vulnerability. The system design makes an assumption regarding security. The design shifted the security detail to network provider. Therefore, it is sensitive to DoS and jamming attacks.

The research work [18] mentioned in Table 1 was based on AAD (Autonomous Anomaly Detection) within the network of SDN-IoT. The application itself was focused on different DL algorithms. The architecture focuses on autonomy. It shifted the dynamic of passive monitoring system to autonomous system. Such a system was capable of investigating threats and giving a response. The DL algorithms are complex hence this technique was computationally demanding on resources.

Table 1: Comparative Analysis of Modern IoT Security Techniques

Ref	Technique Used	Accuracy	Strengths	Limitations
[14]	AI (various ML and DL models)	99.78%	Real world validation, User accessibility	Hardware dependency, Sensitivity to Noise
[15]	ML (Anomaly Based ID) + SDN/NFV	~99%	Resource Efficiency, Real world Validation	Standardization Issues, Dataset Limitations
[16]	Post Quantum Cryptography	11.7 ms (Overhead)	High Scalability	Key Management Sensitivity, Resource Demands
[17]	Edge + AI + New Blockchain	95%	Decentralization, Scalability	Communication Link Vulnerability
[18]	Autonomous Anomaly Detection + SDN-IoT + DL	~99%	Focus on Autonomy	Scalability Challenges
[19]	Deep Convolutional Neural Network	99%	Resource Efficiency	Lack of Interpretability, Adversarial Vulnerability
[20]	Hybrid Cipher + IoT	7.9995 (Entropy)	Lightweight Design	Device Constraints, Key Management
[21]	AI + Blockchain	99.12%	High Scalability	Performance Bottleneck

AAD systems also exhibited scalability issues. Large scale processing strained the system. Research work [19] proposed the use of Deep-CNN. The study also compared various models. The system was efficient in terms of resources and adaptive. However, the model proposed remained susceptible to adversarial attacks.

The use of hybrid cipher was proposed in study [20], within an IoT environment. The design itself made use of chaotic maps, dynamic S-boxes and XOR operations. The method proposed was lightweight, that is it required limited memory and power consumption. The major issue in this method was of key management. The design lacked a lightweight model for key generation especially in dynamic IoT scenarios. The study [21] proposed the use of an integrated system of Blockchain and AI. The design was highly scalable and efficient in terms of energy consumption. There are limitations of performance bottlenecks, as scalability dropped from 95% to 92% when devices increased from 1000 to 2000. There was also a drawback of balancing security as it may require further optimization in terms of hardware accelerators.

III. PROPOSED SYSTEM ARCHITECTURE

A. SYSTEM OVERVIEW

The proposed system is structured into three main layers to ensure efficient operation and scalability. Each layer makes sure each operation is handled efficiently and is scalable. The designed architecture is made sure to provide an intelligent solution for real time security management and monitoring. The layered architecture ensures distinct tasks. These tasks namely focus on data collection, communication of said data and its analysis. All these tasks are performed in a secure environment. The main aim of the system remains accurate detection of events and possible threats. This is performed with an infused use of sensor technology, network infrastructure and AI-based algorithms. The layered architecture also ensures scalability. Following is the breakdown of each layer in the architecture.

Perception Layer: This layer includes physical devices such as cameras, motion sensors, access control systems, and environmental sensors. These devices are responsible for collecting real-time data from the environment. The layer is used to continuously monitor the environment and feed various physical signals into the system. The signal is dependent on the type of sensor inputting the data, such as, cameras will be used for video frame input, a door scanner reads a fingerprint etc. Hence, this layer basically caters to real time data generation.

Network Layer: This layer handles communication between devices using wireless networks and secure protocols. It also integrates edge and cloud computing to manage data transmission and processing. The idea behind this layer is to act as a bridge between data collected from various sensors (devices) and intelligence. As this layer works on integration between edge and cloud computing it is important that there exists a secure path for communication.

Application Layer: This layer includes AI-based algorithms that analyze the collected data. It performs tasks such as threat detection, facial recognition, behavior analysis, and alert generation. This is the most important layer of the framework as it is designed to be the decision-making part of the system – in other words the brain of the system. It is designed to detect suspicious activities, such as intrusion in restricted areas. Faces are matched with the stored data to perform facial recognition. The system is also designed to keep track of unusual behavior such as loitering or any abnormal movement. In any questionable circumstances alerts are generated in the form of SMS or alarms.

A workable example of such a system would entail perception layer detecting a person in a restricted area through camera lens. The network layer sends the video feed and lastly the application layers with the use of AI goes through a set of steps to identify the person as a threat or not. If the person is unauthorized the system generates an alert.

B. KEY FEATURES

- **Continuous real-time monitoring:** In contrast to the traditional system which relies on manual monitor checks and interference periodically, this system is designed to monitor data in its true essence. Various sensor devices continuously input all sorts of data in real-time. This improves situational awareness of the system. Especially when a few seconds of delay can pose as a potential threat.
- **Intelligent anomaly detection using AI:** Instead of just relying on predefined dataset and rules the system continues to learn from any incoming data. Based on real time data generation the system is designed to identify any suspicious patterns. This improves the overall accuracy of the system. The identification between normal human movement and any sort of loitering behavior becomes identifiable by AI.
- **Remote system access and control:** Any sort of physical presence of a person is not required by the system. This prompts to faster reaction time to any problem. Live feed and any possible threat alerts are accessible to the user at any point.
- **Flexible and scalable architecture:** The architecture is designed to incorporate any additional technology making it flexible. Any additional device or use case would not require a major change in design. Furthermore, the system is scalable, a small setup can easily be upgraded to a large-scale setup. The performance of the system would remain constant. This is possible due to the layered architecture which can incorporate changes in individual layers independently.

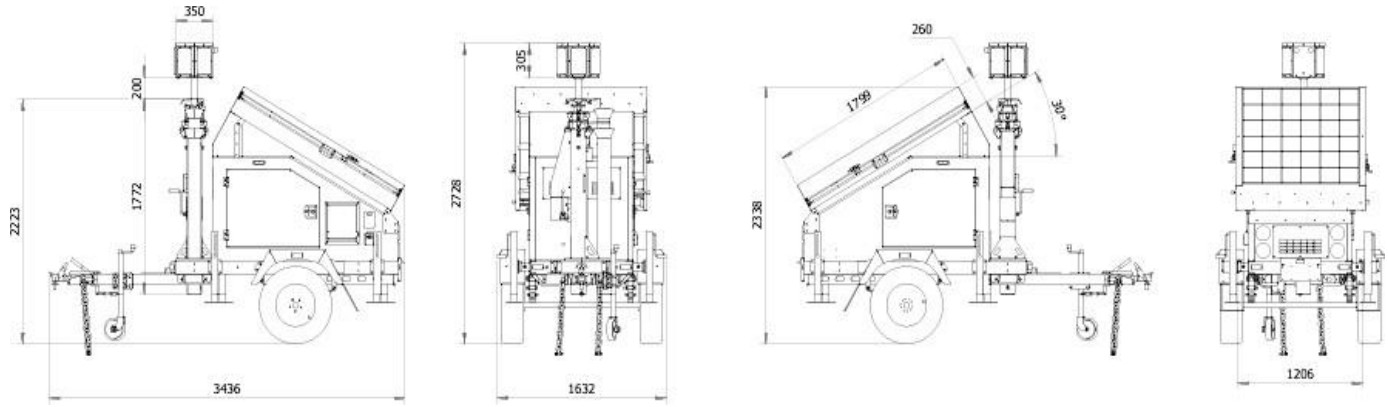

Figure 1: Drawing of 3 panelled solar powered CCTV Tower.

- **Compatibility with existing security systems:** The system is capable enough to work with current security systems effectively. This reduces any over the top cost required to change security equipment preinstalled in the building infrastructure. Instead, the system enhances security with its state-of-the-art AI-analytics.

IV. METHODOLOGY

Following is a step-by-step process from raw data collection to its processing to its analysis.

A. DATA COLLECTION

Data is gathered using various IoT devices placed within the monitored area. These devices capture video streams, motion signals, and access-related information. This data is gathered in real time from all these IoT devices. These devices are to be installed in such places that ensures maximum coverage which in turn ensures maximum security. The data gathered from each device helps in a different type of analysis such as video analytics gives us facial recognition and even intrusion detection. The real time streaming of data ensures most updated information. Besides this, the multi-source sensor data warrants that no event critical in nature is missed. A drawing of a 3 paneled solar powered device is shown in Fig. 1. The implementation of this device is shown in later section. It can be used to collect data.

B. DATA PROCESSING

After real time data collection, the data needs to be processed. To ensure fast response, edge computing is

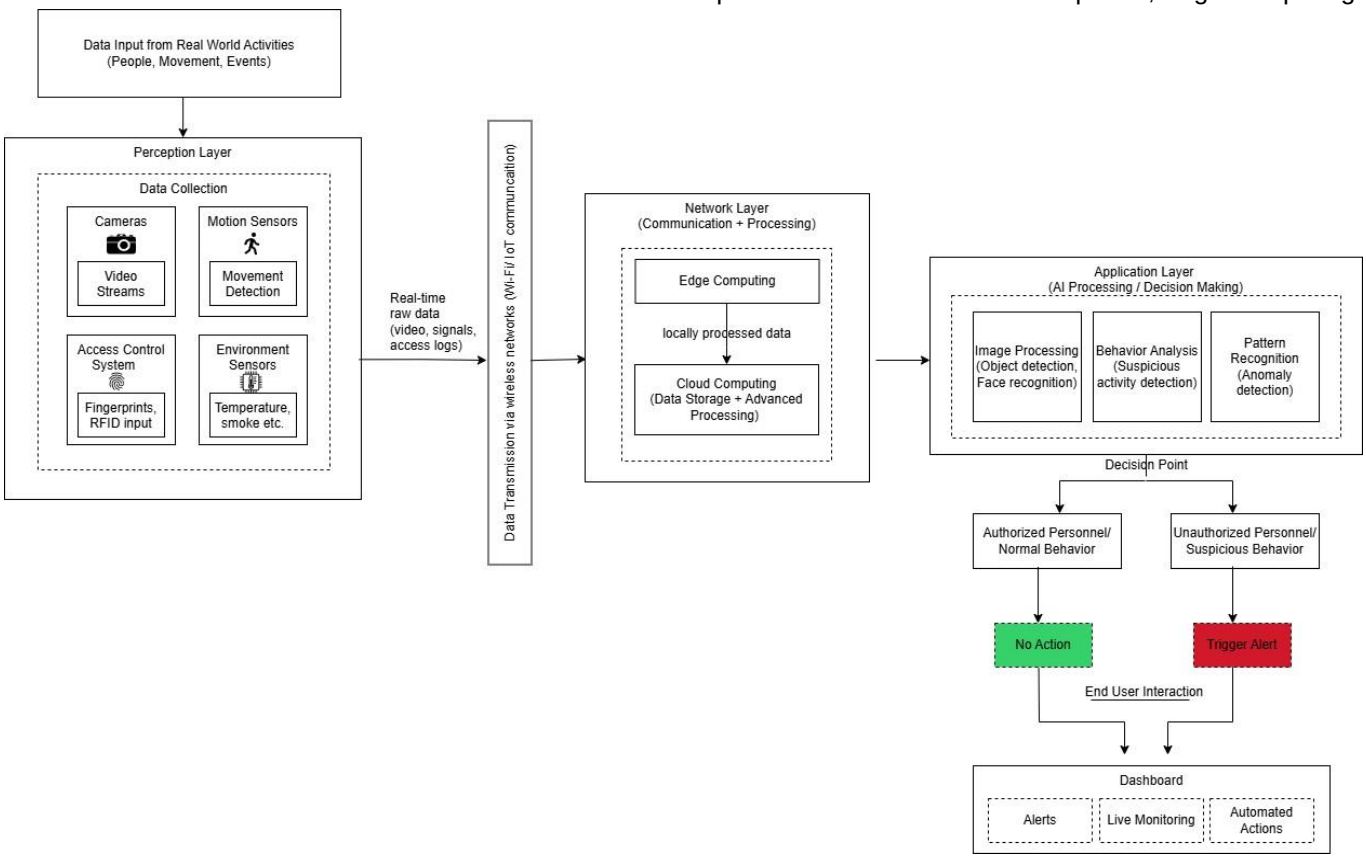

Figure 2: Drawing of a 3-paneled solar powered device to collect data.

used for immediate data processing. Larger datasets are stored and analyzed on cloud platforms for deeper insights. The initial processing needs to happen near the data source or in this case a local edge server. This processing can range from filtration of noise in the data or compression of video data streams. The processing at edge server leads to multiple benefits mainly reduced latency time and in case of critical problems immediate step can be taken. However, main processing takes place during cloud computing. Deeper insights can be collected at this point, such as various trends and patterns can be extracted.

C. AI-BASED THREAT DETECTION

The system uses AI models trained on different types of data. These include image-based detection for identifying intruders, behavior analysis for recognizing suspicious activities, and pattern recognition for detecting unusual events. Diverse datasets are fed to the system to identify different types of critical events. Image based detection takes care of authorized and unauthorized personnel. Behavior analysis focuses on patterns such as, loitering or sudden running may indicate threat and may raise alerts. Lastly pattern recognition differentiates based on historical data and contrasts between normal and abnormal behavior. Overall, with a combined use of these techniques system accuracy is improved and false positives and negatives are reduced while simultaneously increasing the true positive and negatives.

D. COMMUNICATION PROTOCOL

Secure communication is maintained through standard protocols such as MQTT and HTTP. Encryption methods are applied to protect data and ensure privacy. MQTT helps achieve transmission of data in real time while simultaneously giving us the edge of minimal bandwidth usage. On the other hand, HTTP is useful for any web applications or even remote access of data.

E. MODEL EVALUATION

For evaluation of proposed layered architecture, the dataset is divided into 80% training and 20% testing. The 80% training data is used to learn various behavior patterns and the remaining 20% is used to check how the architecture behaves on unknown and unseen data. The system performance is measured using standard metrics including accuracy, precision, recall, and F1-score.

V. IMPLEMENTATION

Following is the description of how the layered architecture is physically built and how various functions are executed. The details focus on both the hardware as well as the software aspect of the system.

A. HARDWARE COMPONENTS

The system uses IoT-enabled cameras, motion sensors, and micro-controllers such as Raspberry Pi and Arduino for data collection and processing. The hardware aspect mostly focuses on the IoT devices that are used. Different types of sensors are included in this hardware as each sensor focus on security differently. Tasks such as

Table 2: AOPRE-Link8081 (POE) Technical Specifications

Feature	Specification
Model No.	AOPRE-Link8081(POE)
10/100BASE-TX Port	8 port RJ-45 auto-MDI / MDI-X
PoE Specification	IEEE 802.3af / IEEE 802.3at; Ports 1-8
Power Output	Max. 15.4W (af) / 30W (at); DC 48V
Power Pin / Type	1/2+, 3/6-; End-span
Bandwidth	1.6 Gbps
Packet Forwarding	1.2 Mpps
Enclosure	IP40 aluminum housing; DIN rail
LED Indicators	Power (Red), Eth (Yellow), POE (Green)
Power Input	48 to 57 VDC
Surge Protection	±4KV
Network Cables	Cat5 or later UTP (≤100m)
Industry Standards	FCC Part 15, Class A; IEC 61000-4-2 to 16
Certifications	CE, FCC, RoHS compliance
MTBF	>300,000 hours
Dimensions	148 x 106 x 54 mm
Weight	0.65 KG (Product) / 0.72 KG (Packing)
Environment	Operating: -40 to 80°C; Humidity: 5%–95%
Warranty	1-year replacement; 3-year main parts

surveillance, detection of unknown entries and facial recognition is taken care through cameras. These devices transmit data back in real time. Physical movement is detected with the help of motion sensors as well. These types of motion sensors act in a certain range.

Lastly, micro-controllers and edge devices are used to process data locally. For this task devices such as Raspberry Pi and Arduino are used. Raspberry Pi is also useful for running smaller and lightweight AI models. It also takes care of handling communication between devices. Arduino on the other hand is useful for performing operations on smaller scale. This helps take action immediately if needed, specifically closer to edge devices.

Different sides of a CCTV Tower is shown in Fig. 4. It is a solar powered device with a camera head at the top. It is a device that is used to gather data and it can do so by moving around instead of remaining stationary.

An industrial PoE switch is shown in Fig. 3. It is used for connecting devices such as switch, computer, server, hub, etc. It can also be used for network camera, wireless AP industrial VoIP phone and other PoE support devices. It is specially designed for harsh outdoor applications. Its 6KV network port surge protection can adapt to harsh outdoor environment and ensure the reliability of the uninterrupted PoE system. Power input also chooses industry-standard types of power. Further specifications regarding the device is given in Table 2.

Figure 3: AOPRE-Link8081

B. SOFTWARE COMPONENTS

The software aspect handles the intelligent part of the system. AI tools such as TensorFlow and OpenCV are used for analysis, while cloud services like AWS and Azure support data storage and system scalability. Data analysis, its storage and user interaction is handled through software. TensorFlow deals with threat detection and pattern recognition and OpenCV deals with real-time processing of video data. During the processing of video data multiple things are catered, such as, object detection and facial recognition. Cloud platform is useful for various cloud services especially when it comes to storing large amount of data. It plays an important role in running intensive AI models. A user-friendly dashboard is also developed for monitoring and control. These dashboards come handy in having access to live video streams, alert signals and overall, the entire system is accessible remotely.

C. SYSTEM WORKFLOW

Table 3 shows a general set of steps taken by the architecture. Initially, the sensors collect the data in various forms. It is then transmitted through the network to the desired location. After data transmission AI data analysis takes place. At this point if any unwanted behavior is detected, alerts are generated to raise caution. In result of those alerts, desired personnel can act. Depending on the alert generated either an automated set of steps can take place or personnel dedicated for such critical situations can handle the event themselves.

Table 3: System Workflow Steps

Step	Action
1	Sensors collect data continuously
2	Data is transmitted through the network
3	AI models analyze incoming data
4	Alerts are generated when threats are detected
5	Users or security teams take necessary action

VI. RESULTS AND DISCUSSION

A. PERFORMANCE METRICS COMPARISON

Table 4 shows a general comparison of traditional IoT systems, existing AI systems and lastly the proposed system. Metrics such as Detection Accuracy, Response Time, False Alarm Rate, Scalability and Latency are discussed. It is also important to note that the proposed system is being evaluated against all these metrics and shows optimum results against all metrics. The system shows a lot of potential especially compared to traditional system designs and existing AI systems.

Fig. 5 shows bar graph comparisons, which focuses mainly on three different types of system when it comes to security of IoT devices. First of all, traditional systems are evaluated and than the existing AI solutions. The results of both these are compared with the proposed architecture. The traditional system seems to be lacking in-front of both the currently used AI solutions and the proposed architecture.

Fig. 5 depicts traditional system having 84% accuracy. This shows that the conventional ways are not enough to deal with real time situation and ever evolving world. There are limitations when it comes to working with conventional systems. This moves us towards the already existing AI solutions. They had the accuracy of 94.5%. This showed that the use of machine learning algorithms has had a positive effect on the overall system security. Lastly the proposed architecture shows the most superior accuracy of 98.7%. With just one simple graph we can observe the evolution of technology. There is a significant change in values since we have moved forward from our traditional methods. The superior

Table 4: Performance Evaluation of Proposed System

Metric	Traditional Systems	Existing AI Systems	Proposed System
Detection Accuracy	84%	94.5%	98.7%
Response Time (seconds)	7.5	3.5	1.2
False Alarm Rate (%)	18%	9%	2.5%
Scalability (1-10)	4.0	6.0	9.0
Latency (ms)	320	180	45

performance is visible from the accuracy of proposed architecture.

Fig. 6 focuses on the response time among the three different evaluated models. The model with higher values in response time indicates delays in system. This delay can happen due to multiple reasons, such as, delay in manual processing or even inefficient technologies. Such delays might be seen in conventional systems as it has the highest value in its response time, which is 7.5. Moving on with existing AI solutions we observe an improve in performance, having response time value of 3.5. However, there is some latency still observed in existing AI solutions. The response time of proposed architecture is 1.2. This value is 88% more improved than traditional systems and 66% faster than existing AI solutions. Faster response time indicates efficient use of edge computing technologies and overall improved communication protocols. One of the most important factor response time indicates towards is efficient and reliable real-time processing.

Fig. 7 represents the resultant value of false alarm rates generated in the 3 comparing models. The most frequent false alarms raised are observed in the traditional systems with the rate as high as 18%. This rate highlights the limited detection abilities of the system. When talking about existing AI solutions this value decreases to 9%, which better in comparison to traditional systems but still remain alarmingly on the higher side. The proposed system with its cutting-edge technology and operations is able to achieve a false alarm rate of 2.5%. The improvement is majorly due to the improved and efficient AI models; better set of data used for training and therefore improved behavior and pattern recognition ability of the system. Overall, there is an observation of minimized incorrect decisions made by the proposed algorithm.

When a system is dependent on a fixed infrastructure it becomes difficult to expand and modify which makes the system less scalable. Such a factor is observed in the traditional set up of security systems. The scalable score of traditional systems lies as low as 4 out of 10. The system lacks the ability to modify as per the changing requirements at any given point in time. In other cases, scalability may also face hindrances due to central processing system designs or higher resource demands. Such may be the case when only AI models are added to the scenario. Existing AI solutions raises the scalability score up to 6 (out of 10). The proposed system however is able to achieve the astounding score of 9 (out of 10). This score is the proof that the system is adaptable to change. The system is flexible to newer resource allocation, and cloud services are chosen to facilitate the user as per the requirement of the task. The comparison is showed in Fig. 8.

Fig. 9 shows the combined summary of all the metrics discussed earlier. Once again, the results indicate that the proposed model is accurate, efficient in terms of response time; and has an astonishingly low value for false alarm generation. The results are done in comparison to traditional systems and other existing AI solutions.

Fig. 10 holds the percentage improvements across various metrics discussed earlier. Out of all the metrics the most prominent change is visible in the latency. With the improvement of 75% the system shows faster reactions. Next in line is the false alarm rate with an improvement of 72.2%. This highlights the system's reliability in threat detection. The combined effect of these metrics not only indicates system's reliability but also shows how fast the system responds to possible critical situations. Likewise, the other metrics also indicates system's improvement.

Table 5 shows different metrics on which the proposed architecture is being evaluated against. Third column of the table also shows (in percentage), the improvement of the proposed model against the already existing AI techniques.

Figure 4: CCTV Tower Close-up View. (a) Right View (b) Top View (c) Far View (d) Front View (e) Camera (f) Left View

Table 5: Key Findings Summary

Metric	Achievement	Improvement vs Existing AI
Detection Accuracy	98.7%	▲ +4.4%
Response Time	<1.5 seconds	▼ -65.7%
False Alarm Rate	2.5%	▼ -72.2%
Scalability	9/10	▲ +50%
Latency	45 ms	▼ -75%

Table 6: Proposed System Applications

Application Area	Description
Smart Cities	Urban surveillance and traffic monitoring
Commercial Security	Office buildings, shopping malls, banks
Industrial Monitoring	Factory floors, warehouses, supply chains
Residential Environments	Home security and gated communities
Critical Facilities	Airports, power plants, government buildings

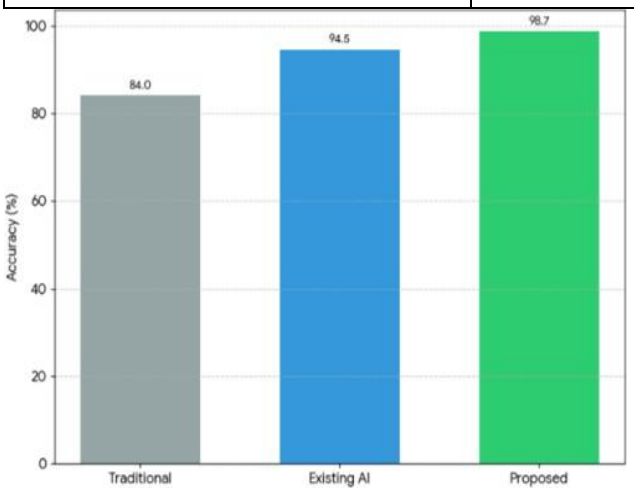

Figure 5: Comparison of Detection Accuracy across Different Systems.

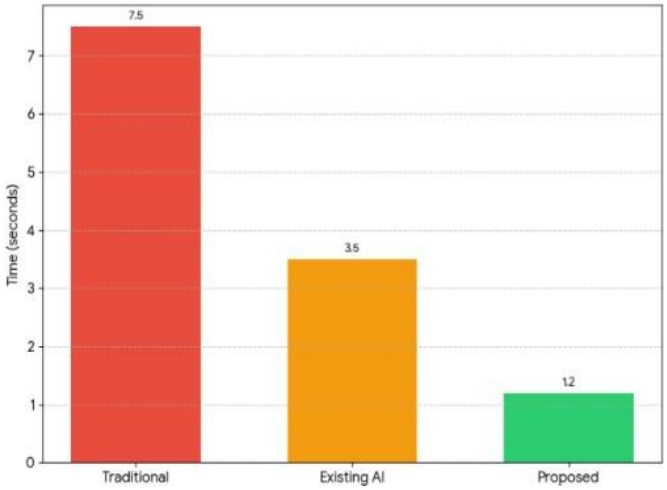

Figure 6: Response time comparison. The proposed system responds in 1.2 seconds — 66% faster than existing AI systems and 84% faster than traditional systems.

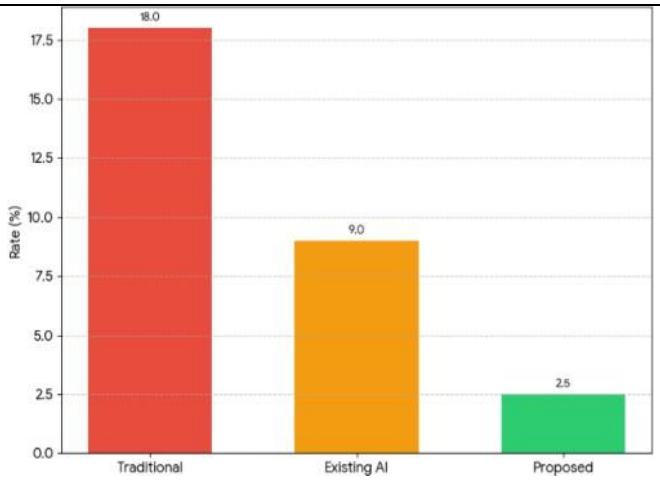

Figure 7: False alarm rate comparison. The proposed system reduces false alarms to only 2.5%, compared to 18% in traditional systems.

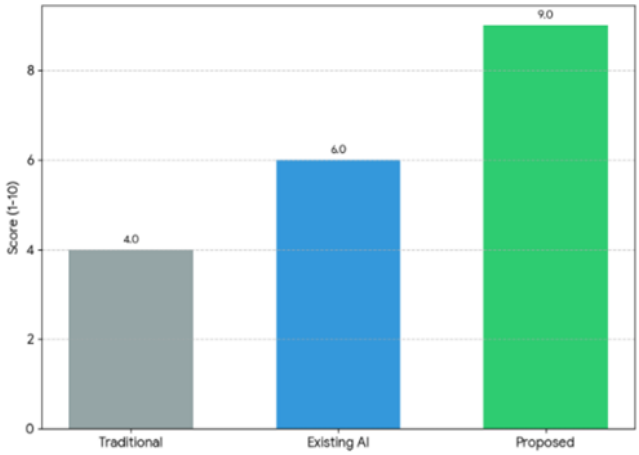

Figure 8: Scalability Score Comparison. The proposed system's modular edge-cloud architecture achieves a scalability score of 9/10.

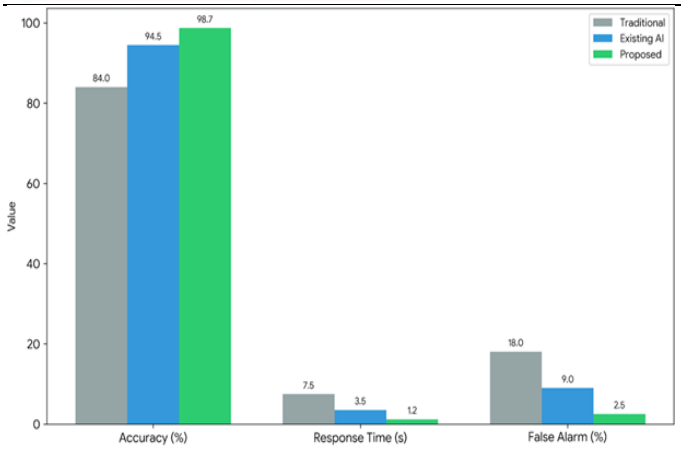

Figure 9: Multi-metric comparison showing the proposed system's superior performance across all key metrics.

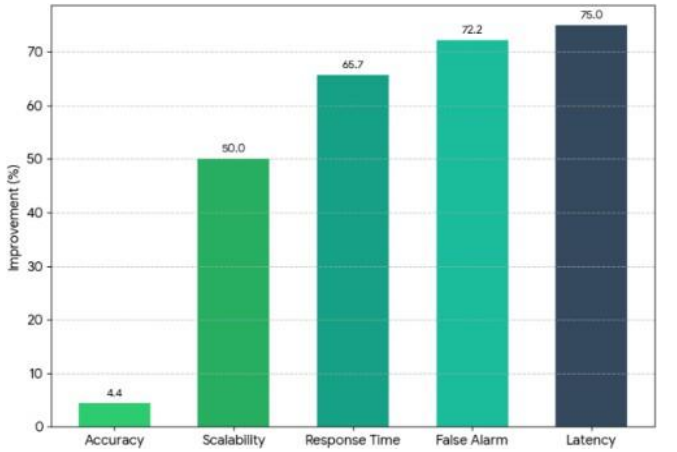

Figure 10: Percentage improvement of proposed system over existing AI systems. The most significant improvements are in false alarm reduction (72.2%) and latency reduction (75.0%).

Metric	Value	Improvement vs Existing AI
Detection Accuracy	98.7%	▲+4.4%
Response Time	1.2 sec	▼-65.7%
False Alarm Rate	2.5%	▼-72.2%
Scalability	9.0/10	▲+50.0%
Latency	45 ms	▼-75.0%
Reliability	99.5%	▲+8.0%

Figure 11: Performance dashboard summarizing key achievements of the proposed integrated security system.

VII. APPLICATIONS

Table 6 lists down various areas of life in which the proposed model can be used in. Instead of designing an area focused architecture, the model is adaptive to its environment. The environment may vary from surveillance of urban areas in smart cities to commercial securities. The system is useful in industrial environment as well.

VIII. CHALLENGES AND FUTURE WORK

A. CHALLENGES

Table 7 lists down some of the challenges faced by proposed architecture. The initial cost of the setup is high. The initial setup of IoT devices and edge infrastructure requires ample investment. Then comes the issue of data privacy. This issue is concerned with data handling of the surveillance data that would be gathered. Lastly, the system architecture faces some network delays. This is specifically faced during large scale deployment of data.

Table 7: Challenges and Limitations

Challenge	Description
Data Privacy	Ensuring secure handling of sensitive surveillance data
Network Delays	Managing latency in large-scale deployments
Initial Cost	Higher upfront investment for IoT and edge infrastructure

B. FUTURE WORK

Table 8 discusses future work that can be performed on the proposed architecture. Integration of couple of more technologies will help in improving the system. Integration of 5G network would lead to lower latency value and hence provide faster communication. Integration of Blockchain will lead to improved security. Higher level of privacy can be achieved through Federated Learning, which can be done without centralization of data. Integration of Predictive Analysis can help in threat detection before any incident takes place.

Table 8: Future Work Directions

Direction	Benefit
5G Integration	Faster communication and lower latency
Blockchain	Enhanced security and tamper-proof logging
Federated Learning	Improved privacy without centralizing data
Predictive Analytics	Proactive threat detection before incidents occurs

IX. CONCLUSION

This research presented a smart security system that integrated IoT devices with AI technologies. The system provides continuous monitoring, intelligent analysis, and quick response to potential threats. By combining connectivity and intelligence, the proposed solution offers a modern approach to security that is more efficient, scalable, and reliable than traditional methods. It has strong potential for use in various real-world applications and future smart environments. The proposed system can serve as the foundation for next-generation intelligent security solutions in smart cities and industrial environments.

REFERENCES

[1] Md Mamunur Rashid, Joarder Kamruzzaman, Mohammad Mehedi Hassan, Tasadduq Imam, and Steven Gordon. Cyberattacks detection in iot-based smart city applications using machine learning techniques. International Journal of environmental research and public health, 17(24):9347, 2020.

[2] Ghazanfar Rehman, Muhammad Aqeel, Anis Maqbool, Muhammad Allah Razi, Hammad Shahab, and Shahzad Hussain. Traffic and security management system: Real-time video anomaly detection using ai models. International Research Journal of Management and Social Sciences, 7(1):48–62, 2026.

[3] Hosam El-Sofany, Samir A El-Seoud, Omar H Karam, and Belgacem Bouallegue. Using machine learning algorithms to enhance iot system security. Scientific Reports, 14(1):12077, 2024.

[4] Amna Zahoor, Waseem Abbasi, Muhammad Zeeshan Babar, and Abeer Aljohani. Robust iot security using isolation forest and one class svm algorithms. Scientific Reports, 15(1):36586, 2025.

[5] Burhan Ul Islam Khan, Khang Wen Goh, Abdul Raouf Khan, Megat F Zuhairi, and Mesith Chaimanee. Integrating ai and blockchain for enhanced data security in iot-driven smart cities. Processes, 12(9):1825, 2024.

[6] Imran Ahmed, Yulan Zhang, Gwanggil Jeon, Wenmin Lin, Mohammad R Khosravi, and Lianyong Qi. A blockchain- and artificial intelligence-enabled smart iot framework for sustainable city. International Journal of Intelligent Systems, 37(9):6493–6507, 2022.

[7] Mohammad Wazid, Basudeb Bera, Ankush Mitra, Ashok Kumar Das, and Rashid Ali. Private blockchain-envisioned security framework for ai-enabled iot-based drone-aided healthcare services. In Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond, pages 37–42, 2020.

[8] Rayed AlGhamdi, Madini O Alassafi, Abdulrahman A Alshdadi, Mohamed M Dessouky, Rabie A Ramdan, and Bassam W Aboshosha. Developing trusted iot healthcare information-based ai and blockchain. Processes, 11(1):34, 2022.

[9] V Hemamalini, Anand Kumar Mishra, Amit Kumar Tyagi, and Vijayalakshmi Kakulapati. Artificial intelligence–blockchain-enabled–internet of things-based cloud applications for next-generation society. Automated secure computing for next-generation systems, pages 65–82, 2024.

[10] Kavitha S Patil, Indrajit Mandal, and C Rangaswamy. Hybrid and adaptive cryptographic-based secure authentication approach in iot based applications using hybrid encryption. Pervasive and Mobile Computing, 82:101552, 2022.

[11] Ankita Anand, Shalli Rani, Divya Anand, Hani Moaiteq Aljahdali, and Dermot Kerr. An efficient cnn-based deep learning model to detect malware attacks (cnn-dma) in 5g-iot healthcare applications. Sensors, 21(19):6346, 2021.

[12] Bhaskar Chavali, Sunil Kumar Khatri, and Syed Akhter Hossain. Ai and blockchain integration. In 2020 8th international conference on reliability, infocom technologies and optimization (ICRITO), pages 548–552. IEEE, 2020.

[13] Ahmed K Hassan, Mohamed S Saraya, Amr MT Ali-Eldin, and Mohamed M Abdelsalam. Low-cost iot air quality monitoring station using cloud platform and blockchain technology. Applied Sciences, 14(13):5774, 2024.

[14] Amro Moursi, Uvais Qidwai, Syed Rafay Hasan, Abdulla Al Ali, and Abdelkarim Erradi. Ai-based hardware trojan intrusion detection system for iot and edge devices. IEEE Access, 13:191689–191706, 2025.

[15] Miloud Bagaa, Tarik Taleb, Jorge Bernal Bernabe, and Antonio Skarmeta. A machine learning security framework for iot systems. IEEE access, 8:114066–114077, 2020.

[16] Kranthi Kumar Singamaneni, Anil Kumar Budati, Shayla Islam, Raenu AL Kolandaisamy, and Ghulam Muhammad. A novel hybrid quantum-crypto standard to enhance security and resilience in 6g-enabled iot networks. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 18:7876–7891, 2025.

[17] Subhi M Alrubei, Edward Ball, and Jonathan M Rigelsford. A secure blockchain platform for supporting ai-enabled iot applications at the edge layer. IEEE Access, 10:18583–18595, 2022.

[18] Tharindu Lakshan Yasarathna, Madhusanka Liyanage, and Nhien-An Le-Khac. Deep learning based autonomous anomaly detection for security in sdn-iot networks. IEEE Open Journal of the Communications Society, 2025.

[19] Faiza Habib, Syed Hamad Shirazi, Khursheed Aurangzeb, Asfandyar Khan, Bharat Bhushan, and Musaed Alhussein. Deep neural networks for enhanced security: Detecting metamorphic malware in iot devices. IEEE Access, 12:48570–48582, 2024.

[20] Biswarup Yogi, Ajoy Kumar Khan, and Satyabrata Roy. Hl-caiot: Hybrid lightweight cipher for iot with chaotic maps and cellular automata. IEEE Access, 2025.

[21] William Villegas-Ch, Jaime Govea, Rommel Gutierrez, and Aracely Mera-Navarrete. Optimizing security in iot ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection. IEEE Access, 13:16933–16958, 2025.