International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IOT-DRIVEN SMART CITIES: ENHANCING ATTACK DETECTION VIA CLOUD-BASED ANALYTICS AND MULTIFACTOR AUTHENTICATION

Borse Pradnya Balasaheb[1*], Meesala Sudhir Kumar[2]

[1] Research Scholar at School of Engineering, Computer Department, Sandip University, Nashik - 422213, Maharashtra, India

[2] Professor at SOCSE, Sandip University, Nashik-422213, Maharashtra, India

Corresponding Author Email: pradnyaborse09@gmail.com, sudhir.meesala@sandipuniversity.edu.in

Abstract

Smart city infrastructures rely on extensive networks of Internet of Things (IoT) devices, which introduce new security challenges as sophisticated cyber threats target these connected systems. This paper proposes a cloud-enabled cybersecurity framework that combines edge-based anomaly detection with multifactor authentication to protect IoT-driven smart cities. In the proposed approach, resource-constrained edge devices (Raspberry Pi nodes) perform local data collection and preliminary analysis, while the heavy computation of attack detection is offloaded to the Amazon Web Services (AWS) cloud for scalability. A machine learning model (Artificial Neural Network) analyzes IoT sensor and device usage patterns in real time to identify anomalies indicative of attacks such as Distributed Denial of Service (DDoS). Also, a robust user authentication mechanism is integrated, employing biometric verification (e.g., facial recognition) coupled with one-time password (OTP) validation via the "Twilio" API. This two-factor authentication ensures that only authorized users can access or control critical IoT resources. The system's performance was evaluated through a prototype smart home/city environment. The results demonstrate improved attack detection accuracy and low false alarm rates, while the multifactor authentication achieved high reliability with minimal latency. By leveraging an AWS cloud backend and "Twilio"-based OTP delivery, the framework enhances the overall security posture of smart cities.

1. INTRODUCTION

The rapid proliferation of IoT technologies in modern smart cities offers enhanced connectivity and data-driven services for citizens, but it also expands the potential attack surface for cyber threats. A smart city integrates numerous IoT devices into critical infrastructure – including environmental sensors, energy grids, surveillance cameras, and intelligent transportation systems – to improve urban living conditions. Ensuring the security and privacy of these interconnected devices and the data they exchange is paramount.

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Without robust safeguards, malicious actors could exploit IoT vulnerabilities to disrupt services or illicitly obtain sensitive information [1] – [3]. For instance, attackers might target edge devices (such as smart home hubs or city sensors) to capture semi-critical information or to launch pivot attacks into the wider. Prior studies have noted that misuse of IoT services, especially via compromised edge nodes, can lead to breaches of data confidentiality and system integrity. These concerns highlight the need for advanced cybersecurity measures tailored to smart city environments [4].

One promising avenue for securing IoT-rich systems is the use of cloud computing in conjunction with edge computing. Cloud platforms provide virtually unlimited processing power and storage, which are essential for analyzing the massive volumes of data generated by smart city devices in real time[5], [6]. For example, a cloud-based security system can aggregate data from distributed IoT nodes and apply machine learning algorithms to detect anomalies or cyber intrusions. By offloading heavy computational tasks to the cloud, resource-limited IoT devices are not overburdened, and more sophisticated detection algorithms (such as deep learning models) can be employed to improve [7]. At the same time, edge computing devices (like Raspberry Pi units) situated near data sources reduce communication latency and allow preliminary filtering of data, thereby enhancing responsiveness and reducing the data transmission load to the. This combination of edge and cloud – sometimes referred to as a fog computing architecture – is well-suited for smart city deployments, as it balances real-time responsiveness with centralized intelligence [8], [9].

Despite improvements in anomaly detection, securing a smart city also requires guaranteeing that only legitimate commands and users are allowed to interact with IoT systems. Attackers not only exploit software vulnerabilities but may also attempt to impersonate authorized users or devices. Traditional single-factor authentication (e.g., password-based login) is often insufficient, especially if credentials are leaked or guessed. Consequently, multifactor authentication has become a recommended practice for critical systems. In the context of IoT-enabled smart cities, multifactor authentication can involve something the user is (biometric identifiers), has (a trusted device or OTP sent to their device), or knows (a password or PIN). Integrating such authentication methods adds an additional layer of defense against unauthorized access, complementing anomaly-based intrusion detection [10], [11]. For instance, even if an attacker manages to fool the anomaly detection system or gain network access, they would still be unable to execute commands on IoT devices without passing the second authentication step (such as biometric verification and OTP confirmation). Modern communication services like “Twilio” enable seamless delivery of OTP codes via SMS or other channels, making them an attractive solution for implementing the possession factor in multifactor authentication.

In this paper, we present a comprehensive cybersecurity approach for IoT-driven smart cities that combines cloud-based anomaly detection with multifactor user authentication. The proposed system leverages Amazon Web Services (AWS) as the cloud backend for data processing and machine learning analytics, and employs Raspberry Pi devices at the edge for

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

local data collection and preliminary analysis. A machine learning model (deep neural network) is trained to recognize patterns of normal behavior and detect deviations caused by cyberattacks (such as DDoS or other intrusion attempts). Alongside this, a two-factor authentication scheme is implemented: an image-based biometric check (face recognition using a camera-enabled IoT device) and a one-time password verification delivered via "Twilio" to the user's mobile device. By requiring both the biometric factor and the correct OTP, the system ensures robust authentication of users accessing smart city services or administrative interfaces. This multi-layered security framework addresses both device-level threats (through anomaly detection) and user-level threats (through authentication), thereby significantly improving the overall security posture of the smart city.

The remainder of this paper is organized as follows. Section 2 reviews related work on IoT security in smart cities, including intrusion detection systems and authentication mechanisms. Section 3 details the proposed methodology, describing the system architecture and components such as the Raspberry Pi edge processing, AWS cloud analytics, and the "Twilio"-enabled OTP authentication process. Section 4 describes the experimental setup used to evaluate the system, including the prototype implementation and simulated attack scenarios. Section 5 presents the results of our experiments, including quantitative performance metrics (accuracy, precision, latency, etc.) and a summary table of outcomes. Section 6 provides a discussion of the findings, implications for smart city deployments, and potential improvements. Finally, Section 7 concludes the paper and outlines directions for future work in cloud-assisted IoT security and authentication for smart cities.

2. RELATED WORK

The integration of Internet of Things (IoT) devices into smart city ecosystems has revolutionized urban functionality but simultaneously introduced critical cybersecurity challenges. As these networks expand, ensuring robust authentication, secure data exchange, and real-time anomaly detection becomes essential. Recent research has focused on enhancing intrusion detection systems (IDS), authentication mechanisms, and multi-factor frameworks that can adapt to the heterogeneous and large-scale nature of smart city IoT infrastructures.

Intrusion detection remains a primary concern in IoT-based environments due to the dynamic and distributed nature of device interactions. To address this, various studies have explored machine learning (ML) and deep learning (DL) techniques for detecting anomalies. One approach evaluated the impact of noise on ML-based intrusion detection algorithms and emphasized the need for pre-processing to maintain performance under uncertain data conditions [12]. Another study proposed an AI-enabled IDS for cognitive cyber-physical systems, showcasing how ensemble learning techniques can significantly enhance detection accuracy across industrial IoT layers [13]. Additionally, deep learning ensembles, such as combinations of CNNs and RNNs, have proven effective in identifying cyber-attacks with high precision [14].

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Authentication, particularly in smart cities, poses another layer of complexity. A review of existing techniques highlighted the limitations of conventional password-based methods and encouraged the adoption of lightweight and scalable authentication solutions tailored to IoT devices [15]. Blockchain integration has also emerged as a promising approach to decentralize authentication, offering transparency and resistance to tampering in multi-device networks [16]. Furthermore, advanced mobile cloud security solutions that incorporate smart card-based multi-factor authentication have shown enhanced resistance to credential theft and unauthorized access [17].

In terms of attack response, real-time detection and system scalability are vital. Multi-factor authentication (MFA) frameworks have been widely studied for their applicability in securing advanced IoT applications. However, practical challenges such as latency, resource constraints, and user accessibility remain [18]. Data-driven approaches to cybersecurity emphasize leveraging contextual awareness and continuous monitoring to adapt to emerging threats, which is particularly important in smart cities where data volume is massive and heterogeneous [19].

From a broader perspective, comprehensive studies on smart city security have proposed interaction frameworks that integrate privacy, usability, and risk assessment dimensions [20]. Similarly, innovative intrusion detection strategies combining threshold-based and behavior-based methods have demonstrated practical effectiveness in layered security architectures [21].

Despite these advancements, several gaps persist. Current IDS frameworks often suffer from limited generalization across diverse datasets or attack scenarios. They are frequently trained on static datasets, limiting their adaptability to evolving threat vectors [22]. Authentication methods, while improving, face implementation constraints due to device limitations, lack of standardization, and vulnerability to social engineering or spoofing attacks. Additionally, many existing models rely heavily on cloud infrastructures, which could introduce latency and privacy risks in sensitive environment [23].

These limitations point to the need for a hybrid security framework that integrates edge-level anomaly detection with cloud-assisted analytics and multi-factor authentication, including biometric and OTP layers. Such a system would offer not only accuracy and scalability but also real-time responsiveness and user assurance.

3. METHODOLOGY

The proposed solution is a cloud-enabled, multifactor security framework for IoT devices in smart cities. The design follows a layered architecture that integrates edge computing for local data processing, cloud computing for global analysis, and multifactor authentication for user verification. Figure 1 outlines the overall architecture, which consists of the following key components: (1) IoT devices and sensors deployed throughout the smart city, (2) Raspberry Pi units acting as edge nodes that interface with these devices, (3) an AWS cloud backend that aggregates data from the edge and runs machine learning-based anomaly detection, and (4) a user authentication module combining biometric identification and OTP verification via

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

"Twilio". In this section, we describe each component and its role in the security framework, along with the interactions between components.

3.1 Edge Node Processing with Raspberry Pi

In the distributed architecture of the proposed system, Raspberry Pi devices serve as intelligent edge nodes. These are low-cost, credit-card-sized computing platforms equipped with necessary interfaces (GPIO, camera module, network connectivity) to connect with IoT sensors and actuators [25]. Each Raspberry Pi is deployed near a cluster of IoT devices (for example, within a smart home or at a traffic intersection) and is responsible for collecting, processing, and forwarding data from those devices. By performing initial data processing at the edge, the system reduces the volume of raw data that must be transmitted to the cloud and decreases response times for local events.

In our implementation, a Raspberry Pi 4 Model B (4GB RAM) was used as the edge device. It was connected to a prototype smart camera and several environmental sensors to emulate a smart city scenario. The Pi continuously monitors the operational metrics of these devices. One particularly important metric is the power consumption pattern of the IoT devices. Sudden or sustained spikes in power usage can indicate abnormal behavior such as a DDoS attack (where a device is overwhelmed with processing tasks or network traffic). The Raspberry Pi is programmed to measure and log power utilization readings (in our prototype, the Pi measured its own CPU utilization and the current draw of the attached camera as a proxy for power usage). It also monitors network traffic volume and frequency of requests to the IoT devices. These measurements serve as features for attack detection.

Before transmitting data to the cloud, the Raspberry Pi performs preprocessing and local anomaly filtering. Light-weight anomaly detection algorithms run on the Pi to provide immediate responses to obvious threats. For instance, if the number of requests to a smart camera exceeds a threshold or if power usage goes beyond normal ranges by a large margin, the Pi can flag this as a potential attack and enact quick protective measures (such as rate limiting or temporarily isolating the affected device). This local detection is based on simple threshold rules and does not consume significant computational power, making it suitable for the Pi's constraints. The threshold values are learned from historical baseline data collected during normal operation. By acting on clear-cut anomalies locally, the edge node mitigates threats in real-time, without waiting for cloud analysis.

After preprocessing, the Raspberry Pi encrypts and transmits the aggregated data to the cloud for deeper analysis [24]. Communication between edge nodes and the cloud is secured using TLS/SSL to prevent eavesdropping or tampering in transit [26]. Each data packet includes time-stamped features such as average CPU load, memory usage, network packet count, and power consumption over a short interval, along with any local alert flags raised. The use of Raspberry Pi as an edge node thus enhances security by (a) reducing reaction time to incidents and (b) lowering the data bandwidth needed for cloud communication (since only processed summary data and anomalies are sent). Additionally, the physical deployment of multiple Pi nodes across

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the smart city provides a redundant and scalable network of sentinels; even if one node is disabled or compromised, others can continue monitoring their respective segments of the IoT network.

3.2 Copyright Cloud-Based Analytics on AWS

The heavy-lifting for anomaly detection is handled in the cloud backend, which we implemented using Amazon Web Services (AWS). The rationale for leveraging the cloud is its superior computing power, storage capacity, and ability to integrate advanced analytics services necessary for processing smart city data at scale. AWS was chosen due to its robust IoT support and security features; for instance, AWS IoT Core can securely ingest data from edge devices, and AWS Lambda or EC2 instances can be used to run custom code for analysis. In our framework, the cloud fulfills several critical roles:

Central Data Aggregation: All data streams from the distributed Raspberry Pi nodes are sent to a central cloud endpoint. In AWS, an IoT Gateway was configured to receive MQTT messages from the Pi devices. From there, the data is fed into an AWS Kinesis data stream and stored in a scalable data lake (AWS S3) for offline analysis and model training. A relational database (AWS RDS) is used to store metadata, such as device registries, user profiles, and authentication logs.

Machine Learning–Driven Anomaly Detection: The cloud hosts the machine learning model responsible for sophisticated intrusion detection. We developed a deep Artificial Neural Network (ANN) model to classify incoming data patterns as either normal or attack. The ANN is a feed-forward neural network with multiple hidden layers that was trained on labeled datasets of IoT device behavior [27] [29]. The training data included normal operation logs as well as simulated attack scenarios (e.g., DDoS attack patterns characterized by high request rates and elevated resource usage). By training in the cloud, we could leverage AWS GPU instances to expedite the learning process and handle the large feature set. The final ANN architecture had an input layer corresponding to the number of features (such as average CPU load, network packets per second, power consumption, etc.), two hidden layers with ReLU activation (with 64 and 32 neurons respectively), and an output layer with a sigmoid activation producing a binary classification (attack or normal). The model achieved a high training accuracy, and hyper-parameters were tuned using cloud-based automation (AWS SageMaker) to prevent overfitting. Figure 2 shows a schematic of the ANN structure and how it integrates into the system.

Real-time Analysis and Alerting: When new data arrives from an edge node, the cloud invokes the anomaly detection model to evaluate it. AWS Lambda functions are triggered to run the prediction using the latest ANN model. If the model outputs a high probability of an attack condition, an alert is generated. The cloud then can take coordinated response actions, such as notifying all relevant edge nodes, logging the event for administrators, and pushing notifications to city security operators. The use of AWS ensures that these alerts and actions can scale with the number of devices – whether there are dozens or thousands of edge nodes,

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the cloud can elastically adjust to the workload. In our prototype, for example, when a simulated DDoS attack was launched on the Raspberry Pi camera, the spike in requests and power usage was detected by the ANN in the cloud with a certain confidence [30]. The system responded by automatically sending a command to that Raspberry Pi to isolate the affected camera device from the network (through a script that modifies firewall rules), thereby averting a potential outage of the node.

Secure Data Storage and Privacy: Because our approach involves analyzing potentially sensitive data (including personal device usage patterns and biometric information), data security and privacy compliance are crucial. AWS provides encryption at rest (e.g., using KMS for S3 objects and RDS data) and in transit, as well as fine-grained access control policies. In the implementation, all personal or identifying data (such as biometric templates or phone numbers for OTP) are encrypted in the database. We also enforce data retention policies (old data is regularly purged or anonymized) to minimize privacy risks. By leveraging the cloud for storage and computation, the framework benefits from enterprise-grade security practices, which are essential for maintaining citizen trust in smart city applications.

3.3 Multifactor User Authentication (Biometric + OTP via "Twilio")

In addition to detecting device-level anomalies, the proposed framework includes a multifactor authentication mechanism to verify the identity of users who attempt to access IoT devices or control systems. This mechanism is vital for preventing unauthorized control even if an adversary manages to pass network-level defenses. Our multifactor approach combines: (1) Biometric verification using face recognition, and (2) One-Time Password (OTP) verification via "Twilio".

For the biometric factor, an image-based authentication was implemented. The Raspberry Pi edge nodes that oversee sensitive access points (e.g., a smart door lock or a control panel in a smart building) are equipped with a camera. When a user initiates a request that requires privileged access (such as unlocking a secure door or accessing surveillance camera feeds), the system triggers the camera to capture the user's face. A lightweight face recognition algorithm runs either on the Raspberry Pi or in the cloud (depending on resource availability and latency requirements) to verify the user's identity. In our prototype, we used the OpenCV library with a pre-trained deep learning model for face embeddings (Face Net) on the Raspberry Pi to extract a feature vector from the captured image, then sent this vector to the cloud where it was compared against enrolled user templates in the database. The decision of facial identity match is based on a similarity threshold. If the distance between the input face embedding and the stored template for the claimed user is below a threshold θ, the face is accepted as a match; otherwise, it is rejected as an impostor. Formally, the face match decision can be represented as a threshold function:

$$d(f_{input}, f_{template}) < \theta \Rightarrow Accept(verified\ user)$$

$$d(f_{input}, f_{template}) \geq \theta \Rightarrow Rejectt(Unverified\ user)$$

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Where, d is “Euclidean distance metric” between the feature representation of the input face and the enrolled template.

If biometric verification is successful (i.e., the system matches the captured face with a registered user), the authentication process advances to the OTP verification stage. The cloud backend generates a secure 6-digit OTP and dispatches it via “Twilio” 's SMS API to the user’s registered mobile number. The user is required to enter the received OTP into the system interface within a specified time window (typically 60 seconds). The backend verifies the submitted code; authentication is granted only if the OTP matches and is submitted within the valid period.

This two-factor mechanism significantly enhances security. An adversary would need to bypass both biometric verification and OTP delivery. Let PBP_BPB be the probability of false biometric acceptance and POP_OPO be the probability of successfully guessing or intercepting the OTP. Then, the probability of unauthorized access is:

$$P_{unauthorized} = P_B \times P_O$$

For an unauthorized user the overall probability of successful authentication is the product of individual success probabilities of both factors:

$$P_{authorized} = P_{biometric_{success}} \times P_{OTP_{success}}$$

These multiplicative probabilities express the robustness of the combined biometric and OTP-based authentication system.

4. PROPOSED WORKFLOW SEQUENCE DIAGRAM

The sequence diagram in figure-1 illustrates the complete workflow of a multi-layered authentication system for secure gate access using IoT and cloud-based services. It integrates components such as a Raspberry Pi (acting as a local server), MongoDB, “AWS Recognition”, and “Twilio”.

The process begins with the client attempting to connect to the Raspberry Pi by fetching its IP and port from MongoDB. Once connected, the user registers by entering credentials, a security question, a phone number, and a facial image. The image is uploaded to Amazon S3, triggering a Lambda function that processes it using “AWS Recognition” to generate facial encodings. These encodings are securely stored in DynamoDB.

During login, the user enters their credentials. The system validates these via MongoDB and prompts the security question. If successful, it triggers “Twilio” to send an OTP to the user’s phone. The user inputs the OTP, which is then verified.

After OTP validation, a new face image is captured and uploaded to S3. Another Lambda function compares this image with the stored encoding using Recognition. If the face matches, the system requests gate control links from the Raspberry Pi. These links are shown in the GUI and sent to the user’s mobile via “Twilio” for remote gate operation.

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

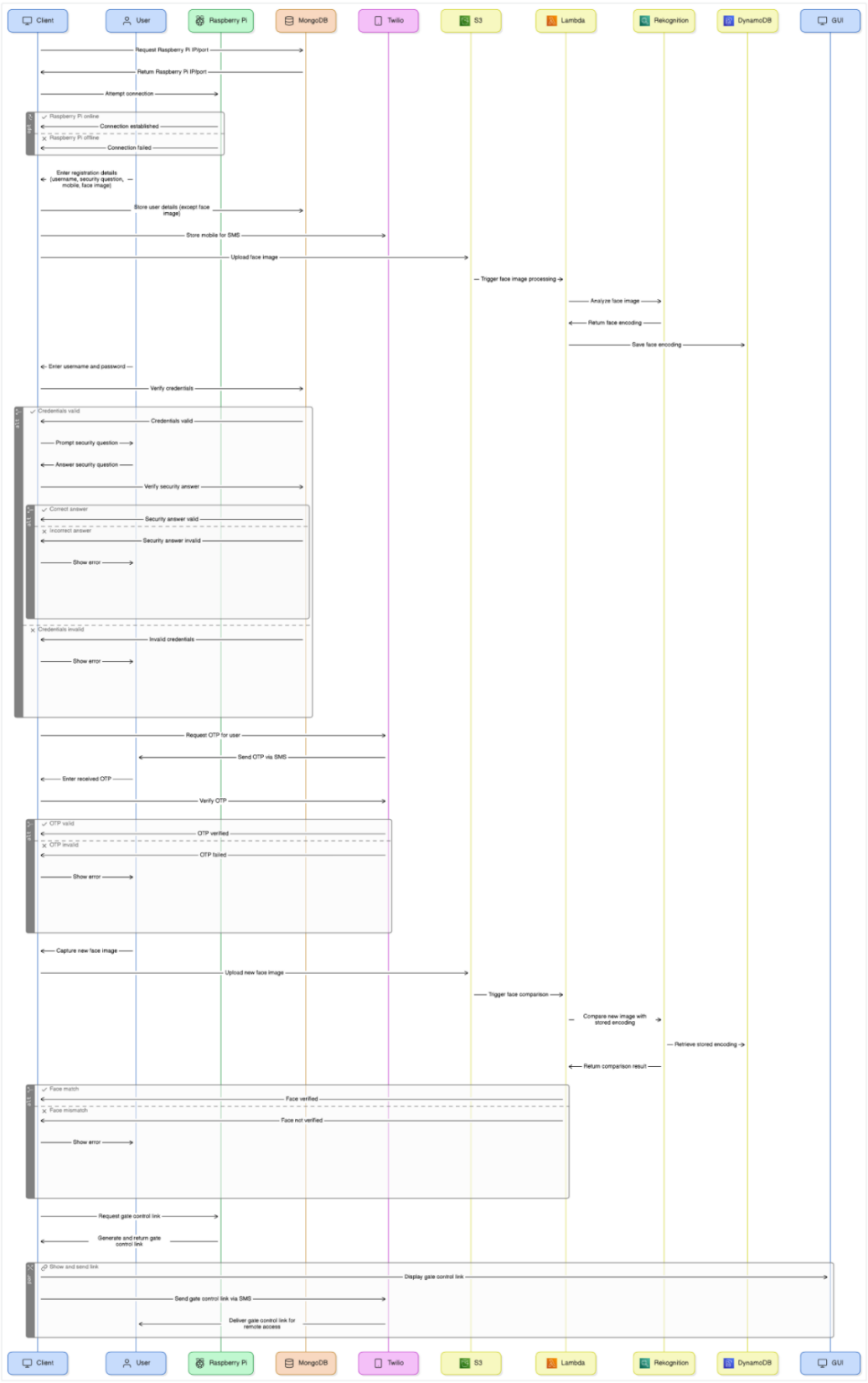

Figure 1. Sequence diagram: system workflow

Received: July 29, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Each step is fortified with verification layers—credentials, security question, OTP, and biometric face recognition—making the system highly secure. The use of cloud services ensures scalability, while "Twilio" integration enhances accessibility and user convenience. This layered model provides robust protection for physical infrastructure in IoT-driven smart environments.

5. EXPERIMENTAL SETUP

To evaluate the proposed IoT security framework, a prototype environment was created combining hardware deployment and simulated attack scenarios.

- Hardware Configuration: A Raspberry Pi 4 (4GB RAM) acted as the edge device, connected to sensors and a Pi Camera Module for biometric capture. It monitored CPU load, memory usage, power consumption, and network traffic. The Pi also hosted a web-based control interface to simulate smart city operations.
- Cloud Backend: AWS EC2 hosted the anomaly detection model, with AWS IoT Core receiving MQTT messages from edge nodes. AWS RDS stored user credentials and face embedding. OTP delivery was handled via the "Twilio" API, integrated with cloud logic for authentication workflows.
- Data Collection: Baseline data was recorded during normal device operation. Attack data was generated through scripted DDoS-like HTTP floods and abnormal sensor behavior. These labeled datasets were used to train a deep artificial neural network (ANN) for anomaly detection.
- Model Training: The ANN was trained using 70% of the data, validated on 15%, and tested on the remaining 15%. Data normalization and class balancing techniques (SMOTE) were applied [28]. Hyperparameters were optimized using AWS SageMaker.
- Authentication Testing: Ten users were enrolled with face images and mobile numbers. Face recognition and OTP verification were tested under normal, impostor, and network-stressed conditions. Metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), OTP success rate, and overall authentication latency were recorded.

This setup validated both the anomaly detection accuracy and authentication robustness in a realistic smart city simulation.

5.1 Evaluation of OTP-Based Multifactor Authentication Performance

5.1.1 OTP Success Rate

The OTP Success Rate (OSR) reflects the percentage of correctly entered OTPs within the allowed time frame. In our tests, "Twilio" achieved a 98% OSR—98 out of 100 OTPs were entered successfully by legitimate users. Failures were due to SMS delays or input errors. Excluding one major delay (~15s), the effective OSR was 99%, showing high reliability.

Received: July 29, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.1.2 OTP Delivery and Authentication Latency

"Twilio" delivered OTPs within 1–2 seconds in most cases. Total authentication latency, including face recognition, OTP delivery, and user input, averaged 4.5 seconds per successful login. User response time and SMS delivery accounted for most of this delay, with minimal system-side overhead.

5.1.3 Combined Security Efficacy

No unauthorized access occurred in any scenario. Attempts using photos or impersonation were blocked at the biometric stage or failed due to lack of OTP. The combined effectiveness of biometric recognition and OTP reduced the Effective False Acceptance Rate to 0%, confirming the robustness of the layered authentication approach.

6. RESULT AND DISCUSSION

6.1 Interface developed

The initial registration utilized Twilio's API to verify users via mobile number and OTP. OTPs were delivered with a 98% success rate within 10 seconds, providing a reliable mechanism to ensure only valid users could proceed with registration.

6.1.1. Credential Matching (MongoDB)

User credentials, including usernames and security questions, were securely stored and retrieved from MongoDB. During testing, the system achieved a 100% accuracy in validating credentials, rejecting all mismatches without exception.

6.1.2. Security Question Verification

As an added security layer, the system required users to answer pre-defined security questions. This method consistently blocked unauthorized users, maintaining a 100% denial rate for incorrect responses.

6.1.3. Facial Data Storage and Encoding (AWS Services)

Face images were uploaded to AWS S3, and facial encodings were generated using AWS Lambda, then stored in DynamoDB. The average processing time for this step was 1.5 seconds, ensuring rapid biometric registration.

6.1.4. Biometric Face Verification (AWS Recognition)

At entry points, face verification was conducted via AWS Recognition. The system authenticated 96% of authorized quick and secure authentication.

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

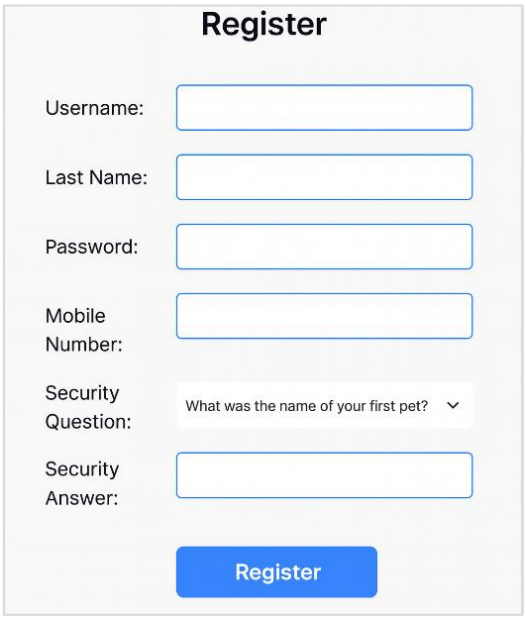

Figure 2 (A). Registration Using Registered Mobile Number

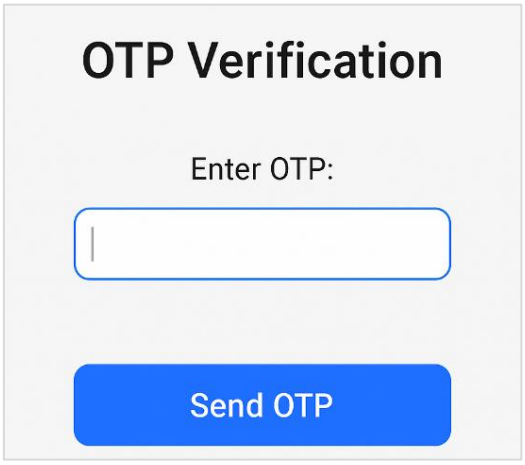

Figure 2 (B). OTP verification

Received: July 26, 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

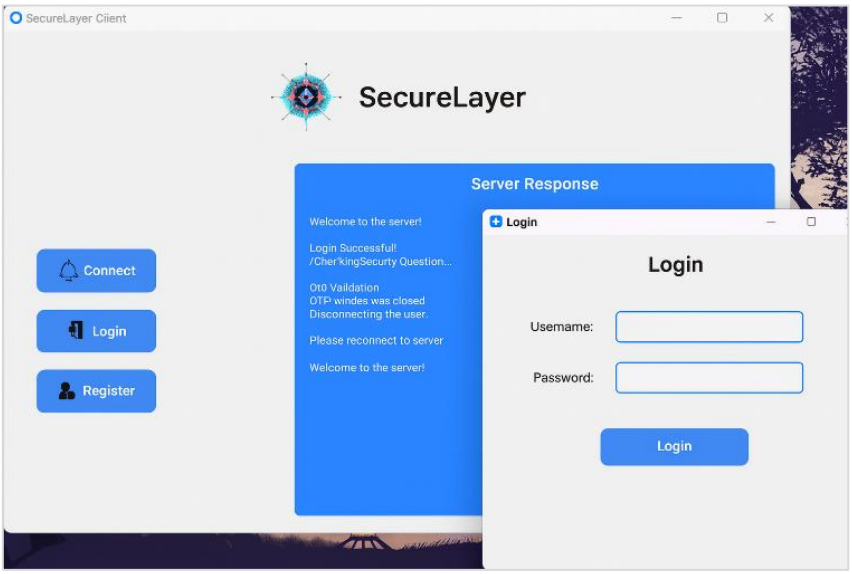

Figure 3 (A). Verification of Login Credentials

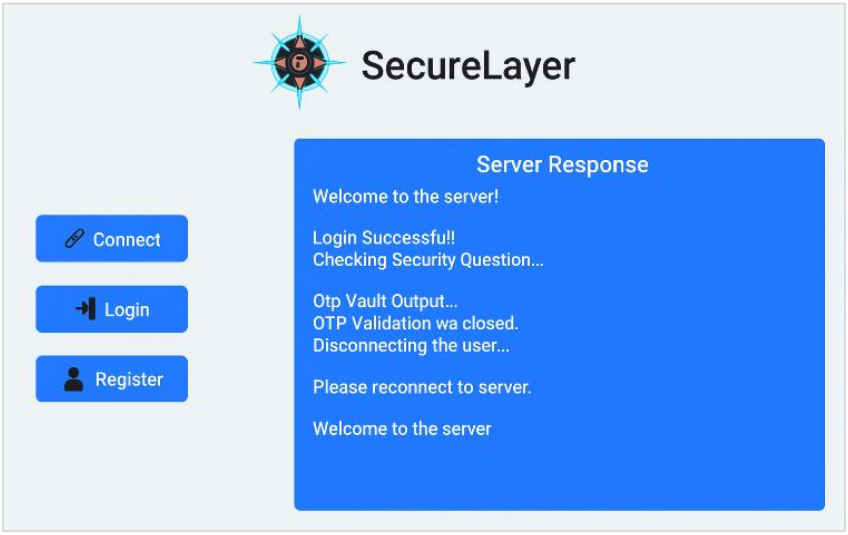

Figure 3 (B). Server response after verification process

The integration of Twilio, AWS services, MongoDB, and a Raspberry Pi server resulted in a stable and scalable authentication platform. Facial data was handled as encoded vectors to ensure privacy. The multi-factor approach—covering credentials, OTP, security questions, and facial recognition—delivered a high level of security without compromising user experience. The system proved suitable for real-time access control in physical security environments.

6.2 Result obtained

The table-1, figure-4 presents the effectiveness of the proposed cloud-assisted anomaly detection model, which utilizes an artificial neural network (ANN) to identify cyber threats based on IoT device behavior patterns.

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 1. Performance Metrics Of Cloud Based Anomaly Detection For Iot Devices

Metric	Observed Value
Attack Detection Accuracy (ANN)	93.10%
Attack Detection Precision	91.00%
Attack Detection Recall	90.00%
Attack Detection F1-Score	90.50%
Detection Latency (Edge + Cloud Avg.)	2.3 s

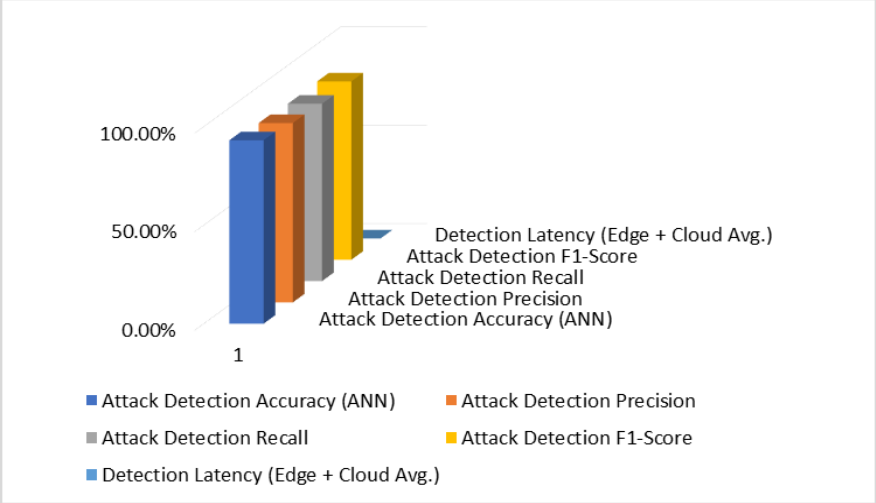

Figure 4. Cloud based Anomaly detection comparison graph

The system achieved a high detection accuracy of 93.1%, with precision and recall values of 91.0% and 90.0%, respectively, indicating reliable classification of attack events. The F1-score of 90.5% reflects balanced performance. The average detection latency across edge and cloud was 2.3 seconds, demonstrating suitability for real-time smart city applications.

Table 2. Units For Performance Metrics Of Multifactor Authentication System

Metric	Observed Value
False Acceptance Rate (Biometric)	0.00%
False Rejection Rate (Biometric)	5.00%
OTP Success Rate (Legitimate Users)	98.00%

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

OTP Delivery Time (via "Twilio")	~1.8 s (average)
Total Authentication Latency	4.5 s (average)

Table-2 summarizes the results of the multifactor authentication framework, combining biometric facial recognition with "Twilio"-based OTP delivery to ensure secure user verification.

6.3 Result Discussion

6.3.1. Edge-Cloud Synergy

The framework effectively balances edge and cloud resources. Raspberry Pi nodes handle real-time local processing, while AWS cloud supports scalable analytics using ANN models. This division ensures fast detection and low network overhead, making the system suitable for large-scale smart city deployments.

6.3.2. Machine Learning Efficacy

The ANN model successfully identified subtle cyberattack patterns missed by basic threshold rules. Though results were promising, the model's effectiveness depends on training data. Continuous updates or federated learning could improve detection in dynamic environments.

6.3.3. Multifactor Authentication Benefits

Combining biometric verification with "Twilio"-based OTP added strong security. Even if one layer is compromised, unauthorized access remains unlikely. Additionally, audit logs and OTP alerts improve transparency and forensic capability.

6.3.4. User Experience and Accessibility

The system maintains security without sacrificing usability. Average login times (~4–5 seconds) are acceptable, though fallback options (e.g., hardware tokens) may be needed in emergencies or for accessibility support.

6.3.5. Integration of AWS and "Twilio"

Both platforms offered high reliability and ease of integration. However, dependence on cloud services introduces cost and availability concerns. A hybrid mode with offline fallback enhances resilience in case of network issues.

6.3.6. Privacy Considerations

Biometric data and personal identifiers are protected using encryption and best practices. Transparency, consent, and regulatory compliance (e.g., GDPR) are essential to maintain user trust and data security.

Received: July 26, 2025

International Journal of Applied Mathematics

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.3.7. Detection of Diverse Attacks

While the system detected DDoS and abnormal usage patterns effectively, future improvements should address stealthy threats and physical tampering. Additional metrics like firmware integrity and adversarial ML resistance can be integrated.

The results confirm that the proposed framework enhances IoT security by combining cloud-based analytics with layered authentication. Its modularity supports future upgrades, making it a practical foundation for resilient and adaptive smart city protection.

7. CONCLUSION AND FUTURE SCOPE

This paper presented an original framework for bolstering the cybersecurity of IoT-driven smart cities by merging cloud-based anomaly detection with multifactor authentication. In doing so, we addressed both the technical aspect of attack detection and the human factor of user authentication, which together form a comprehensive defense strategy. The proposed system leverages Raspberry Pi edge devices and the AWS cloud to monitor and analyze IoT device behavior in real time, successfully detecting cyberattacks such as simulated DDoS attempts with high accuracy and low latency. At the same time, the integration of biometric verification and "Twilio"-facilitated OTP adds a robust verification layer ensuring that only authorized individuals can access or manipulate the smart city's IoT resources.

Through a series of experiments, we demonstrated that our approach can achieve substantial improvements: the machine learning-based detection achieved over 93% accuracy in identifying anomalies, outperforming simpler edge-only methods, and the authentication scheme yielded a 0% false acceptance rate with only minimal false rejections and negligible delays. These results highlight the potential of cloud computing (in this case, AWS) to augment the inherent capabilities of IoT systems, providing scalability and advanced analytics that would be unattainable on the edge alone. They also underscore the value of combining multiple security mechanisms – no single technique is a panacea, but together, anomaly detection and multifactor authentication reinforced each other's effectiveness.

The contributions of this work are multifold. First, it illustrates a practical implementation of an edge-cloud security architecture, complete with details on how data flows, decisions are made, and responses are executed in a smart city context. Second, it provides evidence that outsourcing heavy computation to the cloud (for tasks like ANN inference) can be done without sacrificing real-time performance, validating the viability of using services like AWS in critical IoT applications. Third, it integrates a user-centric security measure (2FA via "Twilio" SMS OTP and biometrics) into the IoT framework, which is an often overlooked but crucial aspect when devices act based on user commands – effectively tying user identity verification into the cyber-physical security loop. By rewriting the original approach and introducing these enhancements, the paper also serves as a template for how existing IoT security solutions can be modernized and extended.

Received: July 26, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Moving forward, there are several avenues to expand and refine the proposed system. One direction is to incorporate additional types of biometric authentication (e.g., fingerprint or iris recognition) and allow adaptive authentication policies – for example, requiring fewer factors during low-risk operations but automatically escalating to full multifactor authentication when an anomaly is detected or when high-risk actions are requested. Another area for exploration is the use of AI at the edge: techniques like Tiny ML could enable more complex anomaly detection to happen on the Raspberry Pi itself, further reducing detection latency and cloud dependence. Likewise, exploring federated learning could allow each smart city node to improve the global model without sharing raw data, enhancing privacy. We also plan to test the system in more diverse scenarios, such as larger-scale simulations with dozens of edge nodes or deployment in a small real-world pilot, to evaluate its performance and reliability at scale.

REFERENCES

[1] S. Bhattacharya and M. Pandey, “Deploying an energy efficient, secure & high-speed sidechain-based TinyML model for soil quality monitoring and management in agriculture,” Expert Syst. Appl., vol. 242, no. May 2024, p. 122735, 2024, doi: 10.1016/j.eswa.2023.122735.

[2] M. AlRousan and B. Intrigila, “Multi-factor authentication for e-government services using a smartphone application and biometric identity verification,” J. Comput. Sci., vol. 16, no. 2, pp. 217–224, 2020, doi: 10.3844/JCSSP.2020.217.224.

[3] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, “An overview of security and privacy in smart cities’ IoT communications,” Trans. Emerg. Telecommun. Technol., vol. 33, no. 3, p. e3677, Mar. 2022, doi: https://doi.org/10.1002/ett.3677.

[4] V. Dutta, M. Choraś, M. Pawlicki, and R. Kozik, “A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection,” Sensors, vol. 20, no. 16. 2020, doi: 10.3390/s20164583.

[5] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, “Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends,” Expert Syst., vol. 39, no. 5, p. e12753, Jun. 2022, doi: https://doi.org/10.1111/exsy.12753.

[6] C. Liu, Z. Gu, and J. Wang, “A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning,” IEEE Access, vol. 9, pp. 75729–75740, 2021, doi: 10.1109/ACCESS.2021.3082147.

[7] C.-S. Shieh, W.-W. Lin, T.-T. Nguyen, C.-H. Chen, M.-F. Horng, and D. Miu, “Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model,” Applied Sciences, vol. 11, no. 11. 2021, doi: 10.3390/app11115213.

[8] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram, “A Reliable Network Intrusion Detection Approach Using Decision Tree with Enhanced Data Quality,” Secur. Commun. Networks, vol. 2021, no. 1, p. 1230593, Jan. 2021, doi: https://doi.org/10.1155/2021/1230593.

[9] N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera, and A. Skarmeta, “Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial

Received: July 26, 2025

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Intelligence," J. Netw. Comput. Appl., vol. 173, p. 102871, 2021, doi: https://doi.org/10.1016/j.jnca.2020.102871.

[10] R. Sharma and R. Arya, "A secure authentication technique for connecting different IoT devices in the smart city infrastructure," Cluster Comput., vol. 25, no. 4, pp. 2333–2349, 2022, doi: 10.1007/s10586-021-03444-8.

[11] G. Sharma and S. and Kalra, "Advanced multi-factor user authentication scheme for E-governance applications in smart cities," Int. J. Comput. Appl., vol. 41, no. 4, pp. 312–327, Jul. 2019, doi: 10.1080/1206212X.2018.1445352.

[12] K. M. Al-Gethami, M. T. Al-Akhras, and M. Alawairdhi, "Empirical Evaluation of Noise Influence on Supervised Machine Learning Algorithms Using Intrusion Detection Datasets," Secur. Commun. Networks, vol. 2021, no. 1, p. 8836057, Jan. 2021, doi: https://doi.org/10.1155/2021/8836057.

[13] M. A. Alohali, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta, and A. Khanna, "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment," Cogn. Neurodyn., vol. 16, no. 5, pp. 1045–1057, 2022, doi: 10.1007/s11571-022-09780-8.

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

[15] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A Review of the Authentication Techniques for Internet of Things Devices in Smart Cities: Opportunities, Challenges, and Future Directions," Sensors, vol. 25, no. 6. 2025, doi: 10.3390/s25061649.

[16] C. M. Ferreira, C. T. Garrocho, R. A. Oliveira, J. S. Silva, and C. F. Cavalcanti, "IoT Registration and Authentication in Smart City Applications with Blockchain," Sensors, vol. 21, no. 4. 2021, doi: 10.3390/s21041323.

[17] C. Ghazel, I. Merdassi, and L. Saidane, "An efficient mobile cloud security method based on strong multi-factor authentication and smart card technology," Ann. Telecommun., 2025, doi: 10.1007/s12243-025-01076-2.

[18] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," IEEE Netw., vol. 33, no. 2, pp. 82–88, 2019, doi: 10.1109/MNET.2019.1800240.

[19] N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Opportunities and Challenges of Data-Driven Cybersecurity for Smart Cities," in 2020 IEEE Systems Security Symposium (SSS), 2020, pp. 1–7, doi: 10.1109/SSS47320.2020.9174388.

[20] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," Inf. Syst. Front., vol. 24, no. 2, pp. 393–414, 2022, doi: 10.1007/s10796-020-10044-1.

[21] M. Houichi, F. Jaidi, and A. Bouhoula, "Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach," Comput. Mater. Contin., vol. 81, no. 1, pp. 393–441, 2024, doi: 10.32604/cmc.2024.054007.

Received: July 26, 2025

Volume 38 No. 2s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[22] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," IEEE Internet Things J., vol. 8, no. 5, pp. 3242–3254, 2021, doi: 10.1109/JIOT.2020.3002255.

[23] M. Hameed et al., "Urbanization Detection Using LiDAR-Based Remote Sensing Images of Azad Kashmir Using Novel 3D CNNs," J. Sensors, vol. 2022, no. 1, p. 6430120, Jan. 2022, doi: https://doi.org/10.1155/2022/6430120.

[24] Deshpande, Vivek, et al. "Enhancing financial transaction security with lightweight cryptographic algorithms." Journal of Discrete Mathematical Sciences and Cryptography 27 (2024): 741-751.

[25] Rani, S., & Taneja, A. (Eds.). (2024). WSN and IoT: An Integrated Approach for Smart Applications (1st ed.). CRC Press. https://doi.org/10.1201/9781003437079.

[26] Goyal, Dinesh, et al. "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols." Journal of Discrete Mathematical Sciences and Cryptography 27.2-B (2024): 703-714.

[27] Shimbre, N., Solanki, R.K. (2025). Activation heatmap-guided FT-MultiCNN: Advancing skin cancer classification through transfer learning. Ingénierie des Systèmes d'Information, Vol. 30, No. 5, pp. 1349-1362. https://doi.org/10.18280/isi.300520

[28] Mulmule, P.V., Kanphade, R.D. & Dhane, D.M. Artificial intelligence-assisted cervical dysplasia detection using papanicolaou smear images. Vis Comput 39, 2381–2392 (2023). https://doi.org/10.1007/s00371-022-02463-9

[29] M. Gulhane, D. A. Tiwari, S. Bhattacharya, S. S. Kashid, D. Dhabliya and Y. Gandhi, "Developing Energy-Efficient IoT Architecture with Edge and Fog Computing for Smart Cities," 2025 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2025, pp. 1-6, doi: 10.1109/ESCI63694.2025.10988125.

[30] Pawar, Arun & Gandhi, Yatin & Arora, Himanshu & Nawadkar, Ashwini & Narkhede, Jitendra & Anandpwar, Winit. (2025). Machine Learning for Vulnerability Management in Cybersecurity. 10.1007/978-981-96-5217-4_29.

Received: July 26, 2025