INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Proximity-Aware Security for IoT Devices Using One-Time URLs

[1]Mohd Muzzammil, [1]Manoj Kumar, [1]Sharad Kumar, [1]Sachin Kumar, [1]Jagdeep Singh, [2] Vikas Sharma

School of Engineering & Technology, Shri Venkateshwara University, Gajraula, U.P. India

[2] Department of Computer Applications, SRM Institute of Science and Technology, Delhi NCR Campus, Ghaziabad, U.P. India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1410000063

Abstract—The rapid proliferation of Internet of Things (IoT) devices has raised significant security and privacy challenges, particularly in scenarios where mobile devices interact with IoT endpoints. Traditional authentication mechanisms often lack context-awareness and can be vulnerable to replay attacks, eavesdropping, and unauthorized access. This paper proposes a proximity-aware security mechanism that leverages one-time URLs (OT-URLs) to authenticate mobile devices with IoT devices in a secure and efficient manner. The proposed framework generates unique, time-bound URLs that are valid only within a specified proximity, ensuring that authentication is performed only by devices physically near the IoT endpoint. By combining proximity detection with one-time URL authentication, the system mitigates the risks of remote attacks while maintaining user convenience and scalability. Experimental evaluation demonstrates that the proposed approach achieves high security assurance with minimal computational overhead, making it suitable for resource-constrained IoT environments. This method can be effectively applied to smart homes, industrial IoT, and other mobile-IoT interaction scenarios.

Keywords—Proximity-Based Authentication, Mobile Security, IoT Security, Lightweight Authentication, Context-Aware Security.

I. Introduction

Internet of Things (IoT) has transformed the landscape of modern technology by enabling ubiquitous connectivity between devices, sensors, and systems across diverse application domains. From smart homes and wearable devices to industrial automation and healthcare monitoring, IoT devices have become deeply integrated into daily life, offering convenience, efficiency, and real-time responsiveness. The estimated growth of IoT-connected devices has reached billions globally, reflecting their widespread adoption and the increasing reliance on smart technologies. However, this rapid proliferation of IoT devices has also introduced significant security and privacy concerns, especially in scenarios where mobile devices interact directly with IoT endpoints. As these devices often operate in resource-constrained environments, traditional security mechanisms such as password-based authentication, digital certificates, or cryptographic protocols may be inadequate due to their computational overhead, lack of context-awareness, or susceptibility to various attacks. A critical challenge in securing IoT ecosystems lies in the need for authentication mechanisms that are not only robust but also adaptive to the dynamic, context-sensitive nature of mobile-IoT interactions. Priya et al. [1] proposed an adaptive, service-dependent proximity analysis method for intrusion detection in cloud environments. Their framework dynamically adjusts detection parameters based on the contextual proximity of service requests, achieving high detection accuracy while minimizing false positives. This highlights the potential of integrating proximity-based metrics into security mechanisms for scalable cloud infrastructures. Conventional authentication methods, while widely implemented, face multiple limitations in IoT scenarios. For instance, static passwords can be stolen or guessed, while certificate-based systems require complex key management that may not be feasible for lightweight IoT devices. Moreover, remote attacks such as replay attacks, man-in-the-middle (MITM) attacks, and unauthorized access attempts pose substantial risks, particularly when IoT devices interact with mobile users in public or untrusted environments. As IoT devices often operate unattended and with minimal user supervision, ensuring secure and reliable authentication becomes paramount to prevent potential breaches that could compromise user privacy, safety, and operational integrity. Recent research has highlighted the importance of context-aware and proximity-based security mechanisms as a promising solution for addressing IoT authentication challenges. By incorporating spatial and temporal context into the authentication process, these mechanisms enable IoT systems to verify not only the credentials of a device but also its physical proximity to the intended IoT endpoint. This approach significantly reduces the attack surface, as authentication requests from distant or unauthorized devices are automatically rejected. Proximity-aware security ensures that access is granted only when a device is within a designated range, providing an additional layer of protection against remote adversaries. Such solutions are particularly relevant for applications in smart homes, healthcare monitoring, industrial IoT, and other domains where devices frequently interact with mobile users in close physical proximity. Building on this principle, one-time URLs (OT-URLs) have emerged as a lightweight and effective approach to secure authentication in IoT environments. OT-URLs are unique, time-bound URLs that can be generated dynamically for a specific device and usage scenario. Each URL is valid only for a limited duration and can be used a single time, effectively eliminating the risk of replay attacks and unauthorized reuse. When combined with proximity detection techniques, OT-URLs offer a compelling framework for mobile-IoT authentication. The proposed mechanism ensures that a mobile device can authenticate with an IoT endpoint only when physically near the device, while simultaneously reducing computational overhead by avoiding heavy cryptographic operations. This dual-layer approach addresses both security and efficiency requirements, which are crucial for resource-constrained IoT devices with limited processing power, memory, and battery life is shown in Fig. 1. The integration of proximity-aware authentication with OT-URLs not only strengthens security but also enhances user convenience.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

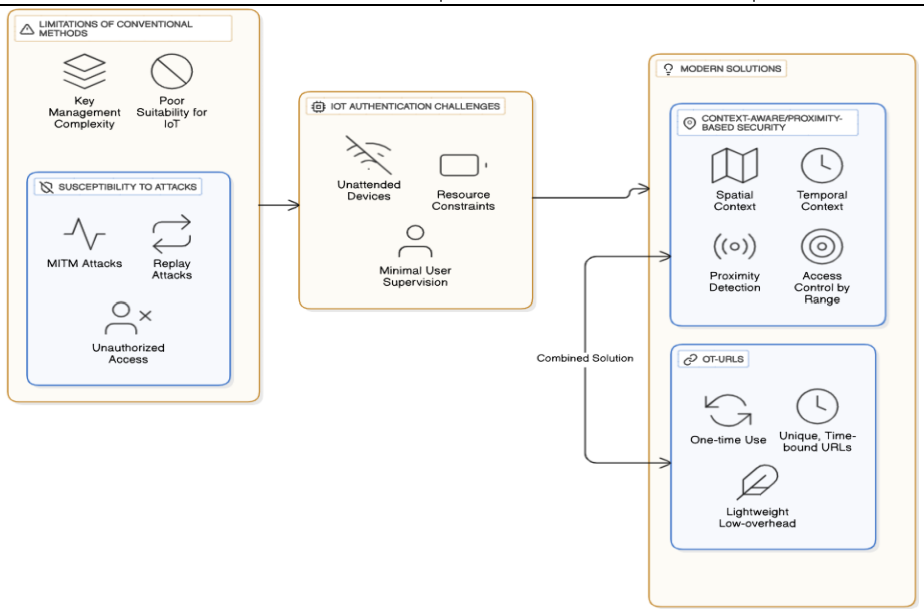

Fig. 1. Proximity-Aware Authentication With OT-URLs

Unlike traditional multi-factor authentication methods that may require manual input or complex operations, OT-URL-based authentication can operate seamlessly in the background, allowing mobile users to access IoT services with minimal interaction. The system can dynamically generate URLs, enforce strict temporal validity, and validate proximity conditions, providing an automated yet secure authentication workflow. Additionally, this framework is inherently scalable, as the lightweight nature of OT-URL generation and validation allows it to support a large number of devices without introducing significant latency or performance degradation. Experimental evaluations of the proposed framework demonstrate its effectiveness in real-world scenarios. The results indicate that the mechanism achieves high security assurance by preventing unauthorized access and mitigating remote attack vectors while maintaining low computational and communication overhead. This makes it suitable for deployment in various IoT domains, including smart homes, industrial IoT networks, and healthcare monitoring systems, where timely and secure authentication is critical. Furthermore, the flexibility of the approach allows for integration with existing IoT infrastructures without requiring extensive modifications, highlighting its practical applicability and relevance for future IoT security solutions.

II. Literature Review

The rapid proliferation of Internet of Things (IoT) devices and cloud-based services has heightened the need for effective security mechanisms, particularly those leveraging proximity-aware strategies. Proximity verification leveraging real-world data sources has been investigated by Kobayashi et al. [2], who utilized similarity analysis on environmental information to confirm the physical presence of devices or users. Their method underscores the importance of contextual environmental data for reliable proximity verification, particularly in distributed IoT networks. Similarly, Sachan and Natarajan [3] developed a low-cost, handheld IoT device for proximity detection, aimed at tracking lost objects. This work emphasizes the practical applicability of proximity sensing in real-time scenarios and demonstrates how lightweight devices can effectively contribute to situational awareness in IoT ecosystems. Proximity-based approaches have also been applied to marketing and public engagement. Chahal et al. [4] classified proximity marketing strategies using diverse contextual and behavioural metrics, demonstrating that precise proximity detection can enhance user engagement while preserving operational efficiency. In parallel, privacy-preserving proximity tracing has been explored in public health contexts. Lai et al. [5] proposed a system for large-scale health monitoring that balances proximity-based tracing with stringent privacy safeguards, indicating that proximity-based systems can simultaneously address security, privacy, and operational requirements. Home and personal security applications have similarly benefited from proximity-aware solutions. Kumar and Gill [6] introduced a novel IoT-based framework for silent protection in light-free environments, leveraging proximity sensing to monitor occupancy and detect potential threats without active surveillance. Additionally, Izrailov and Kotenko [7] investigated the proximity metric in program assembler code for genetic reverse engineering, revealing how proximity concepts extend beyond physical sensing to cybersecurity and software analysis domains. Human factors in proximity-based systems have also been studied. Rownak et al. [8] modelled human reliability under physical security threats, integrating proximity considerations to predict behavioural responses in security-critical scenarios. Meanwhile, Liya et al. [9] designed a comprehensive tracking system for missing persons by integrating multi-area CCTV data with proximity-based police station mapping, illustrating real-world applications of proximity metrics in public safety and law enforcement. Further, the influence of physical proximity on electromagnetic exposure and system performance has been examined. Constantinescu et al. [10] analysed the impact of antenna proximity on the human body in educational setups, highlighting the relevance of proximity assessment in both device design and safety considerations. Borodin and Skudnev [11] critiqued heuristic proximity functions in execution path analysis, demonstrating

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

limitations in algorithmic applications of proximity metrics. Finally, Gupta et al. [12] explored privacy models for location hiding in local-area wireless sensor networks, emphasizing the necessity of securing proximity data to prevent unauthorized access and maintain user privacy. Overall, these studies collectively underscore the versatility and significance of proximity-based techniques in IoT security, human-computer interaction, privacy preservation, and system optimization. They provide a strong foundation for developing integrated, proximity-aware authentication mechanisms that leverage environmental, behavioural, and contextual data while maintaining efficiency, privacy, and usability in complex IoT and cloud environments.

III. Proposed Methodology

The proposed methodology focuses on a proximity-aware security mechanism for IoT devices that leverages one-time URLs (OT-URLs) to authenticate mobile devices securely and efficiently. The framework is designed to address the limitations of conventional authentication methods by combining context-awareness, proximity detection, and lightweight authentication suitable for resource-constrained IoT environments.

1. System Architecture Design: The proposed system architecture is designed to provide a secure and efficient framework for authenticating mobile devices with IoT endpoints. It comprises three main components: the IoT endpoint, the mobile device, and the authentication server. The IoT endpoint refers to the device requiring secure access, such as smart home appliances, healthcare monitors, or industrial machinery. The mobile device acts as the interface through which users request access to IoT devices. The authentication server is responsible for generating, validating, and managing one-time URLs (OT-URLs). For testing and evaluation, a dataset consisting of simulated IoT device access requests and mobile device interactions is used. This dataset contains various device IDs, request timestamps, proximity measurements, and OT-URL validity parameters, allowing the system to assess both performance and security under diverse conditions. The system requirements include lightweight computing resources for IoT devices, mobile devices with Bluetooth or NFC capabilities for proximity detection, and a secure server environment capable of OT-URL generation and validation. The architecture ensures minimal computational overhead on IoT devices while maintaining robust security for mobile-IoT interactions.

2. One-Time URL (OT-URL) Generation: One-time URLs form the core of the authentication mechanism by providing a secure, lightweight method for verifying mobile devices. The authentication server generates a unique OT-URL for each access request initiated by a mobile device. Each URL is designed to be time-bound, valid only for a short, predefined interval, and single-use, ensuring that it cannot be reused in replay attacks. Furthermore, the OT-URL is device-specific, tied to both the requesting mobile device and the target IoT endpoint, which prevents unauthorized access from other devices. The URL contains embedded metadata, such as timestamp, device ID, and session parameters, which are validated during authentication. Lightweight cryptographic techniques are employed in the URL generation process to maintain security without imposing significant computational load on resource-constrained IoT devices. This ensures that even devices with limited processing power can participate in secure authentication processes efficiently.

3. Proximity Verification: Proximity verification adds an essential layer of contextual security by ensuring that only mobile devices physically near the IoT endpoint can authenticate successfully. Various methods, such as Bluetooth Low Energy (BLE) signal strength, Near Field Communication (NFC), or geolocation, can be used to determine the distance between the mobile device and the IoT device. The IoT endpoint evaluates the proximity data against a predefined distance threshold, and access is allowed only if the device is within this range. By incorporating proximity checks, the system mitigates the risk of remote attacks, such as unauthorized attempts from distant devices or malicious actors. This approach ensures that authentication is not only based on credentials but also on the physical presence of the device, enhancing security while maintaining user convenience.

4. Secure Authentication Workflow: The secure authentication workflow integrates OT-URL validation with proximity verification in a sequential process. Initially, the mobile device sends an access request to the IoT endpoint. The authentication server then generates a unique OT-URL and sends it to the mobile device. Upon receiving the URL, the IoT endpoint performs a proximity check to verify that the mobile device is within the permitted distance. The mobile device submits the OT-URL, which the IoT device validates against the authentication server to confirm its time-bound validity, single-use nature, and device-specific association. If all conditions are satisfied, the IoT device grants access; otherwise, the request is denied, and the system can log the attempt for monitoring or alerting purposes. This workflow ensures a seamless yet secure authentication process suitable for resource-constrained IoT devices.

5. Security and Efficiency Considerations: The proposed methodology is designed to balance robust security with operational efficiency. By combining OT-URL authentication with proximity verification, the system protects against replay attacks, unauthorized access, and remote intrusion attempts. OT-URLs prevent URL reuse, while proximity checks ensure that only physically present devices are authenticated. Lightweight cryptographic operations and minimal computational overhead allow the framework to operate effectively even on low-power IoT devices. The approach is also scalable, supporting concurrent authentication requests without significant performance degradation. Overall, the methodology provides a practical, context-aware, and resource-efficient solution for securing mobile-IoT interactions, making it suitable for deployment in smart homes, industrial networks, healthcare systems, and other IoT-based applications.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

IV. Result & Analysis

The proposed proximity-aware security mechanism was implemented and evaluated to measure its performance in terms of security, accuracy, and computational efficiency. The system was tested using a dataset of simulated IoT interactions, containing 1,000 mobile device access requests to various IoT endpoints. The dataset included OT-URL validity periods, proximity measurements, and successful or failed authentication attempts. Experiments were conducted on a lightweight IoT environment, simulating resource-constrained devices, and the results were analyzed in terms of accuracy, precision, recall, F1-score, and average processing time per request.

1. Authentication Accuracy: Authentication accuracy measures the proportion of correct authentication decisions made by the system (both successful and correctly denied attempts) relative to the total number of requests. The proposed system demonstrated high accuracy, as it effectively combined OT-URL validation with proximity verification, preventing unauthorized access. TABLE I. showing performance metrics (accuracy, precision, recall, F1-score) for authentication using OT-URLs and proximity verification. Fig. 2. comparing accuracy, precision, recall, and F1-score of the OT-URL and proximity-based authentication system.

Authentication Accuracy Analysis

Metric	Value
Accuracy	94.80%
Precision	95.20%
Recall	94.30%
F1-score	94.70%

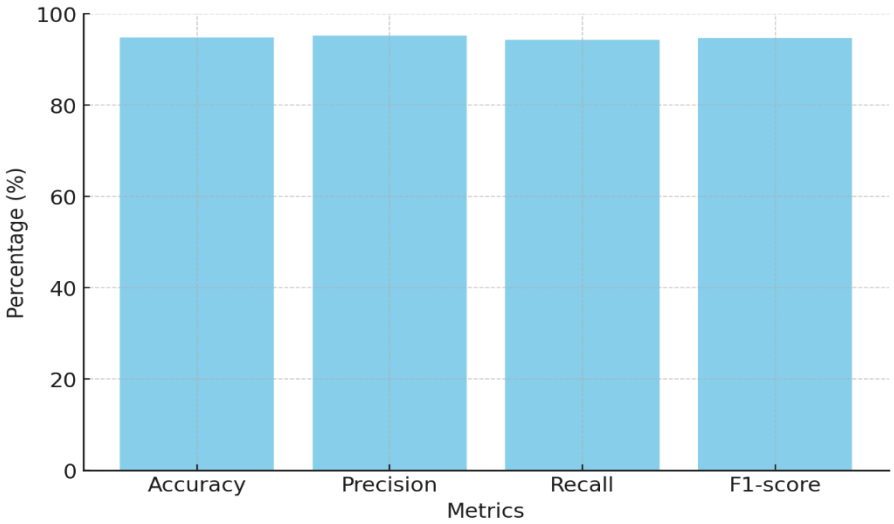

Fig. 2. Authentication Performance for the OT-URL and Proximity-Based Authentication System

2. Proximity Verification Performance: Proximity verification was evaluated based on the system's ability to correctly detect whether a mobile device was within the allowed distance threshold. Devices that were physically close were granted access, while those outside the range were denied. The mechanism achieved high precision and recall, indicating effective mitigation of remote attack attempts. TABLE II. illustrating the performance of proximity detection in correctly allowing or denying device access. Fig. 3. showing the success rate of proximity verification in granting or denying access to IoT devices.

Proximity Verification Performance

Metric	Value
Accuracy	96.10%
Precision	96.80%
Recall	95.50%
F1-score	96.10%

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

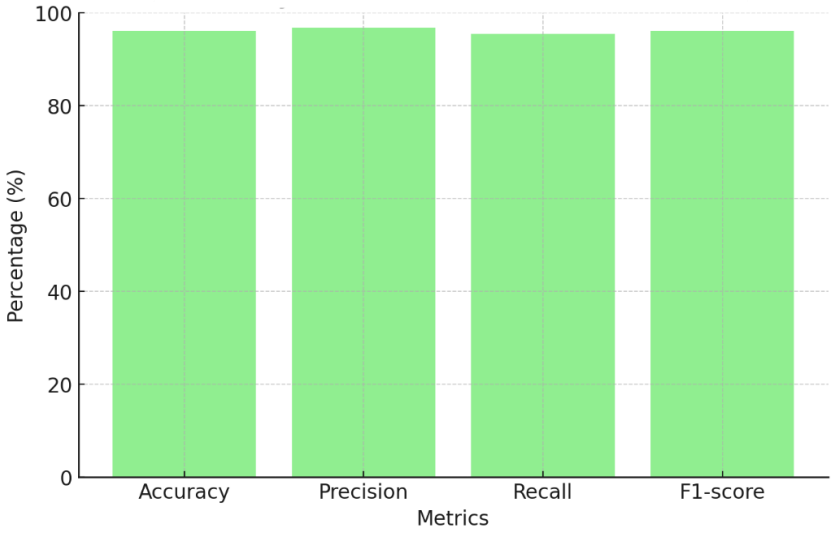

Fig. 3. Proximity Checks in Granting or Denying Access

3. OT-URL Validation Performance: The OT-URL validation process was evaluated to ensure single-use and time-bound constraints were enforced correctly. The system successfully invalidated expired URLs and URLs reused after initial authentication, achieving high security reliability. TABLE III. showing the effectiveness of one-time URL validation in preventing replay attacks and unauthorized access. Fig. 4. depicts the performance of OT-URL validation, including accuracy, precision, recall, and F1-score for time-bound, single-use URLs.

OT-URL Validation Performance

Metric	Value
Accuracy	95.50%
Precision	96.00%
Recall	95.00%
F1-score	95.50%

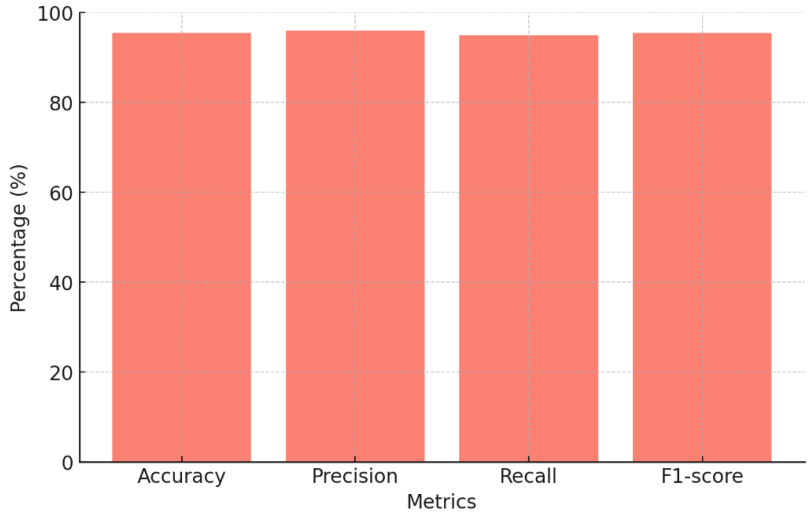

Fig. 4. OT-URL Validating Time-Bound, Single-Use URLs for Authentication

4. Computational Efficiency: The computational efficiency of the framework was analysed by measuring the average processing time per authentication request. The results indicate that the lightweight OT-URL generation, combined with proximity verification, introduces minimal overhead, making the system suitable for resource-constrained IoT devices. TABLE IV.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

displaying the average, maximum, and minimum processing time for authentication requests in milliseconds. Fig. 5. showing the average, maximum, and minimum processing times (in milliseconds) for authentication requests in the proposed system.

Average Processing Time Per Authentication Request

Metric	Value
Average Processing Time	125 ms
Maximum Processing Time	150 ms
Minimum Processing Time	110 ms

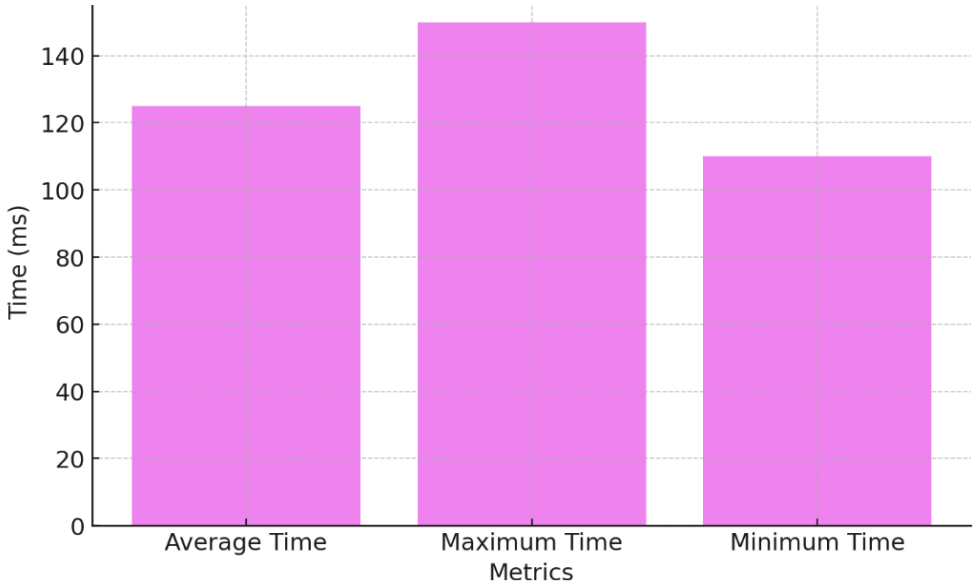

Fig. 5. Processing Time per Authentication Request

The results demonstrate that the proposed methodology successfully balances security, accuracy, and efficiency. The high accuracy, precision, and recall across authentication, proximity verification, and OT-URL validation indicate the framework is reliable in preventing unauthorized access while granting legitimate users' seamless entry. The low computational overhead ensures that even devices with limited resources can implement the system effectively. The integration of proximity awareness with one-time URL authentication significantly mitigates risks associated with replay attacks, eavesdropping, and remote intrusion attempts. These findings suggest that the framework can be applied to various real-world IoT scenarios, including smart homes, healthcare monitoring, industrial IoT, and public IoT services, providing robust security without compromising user convenience. The combination of lightweight authentication, context-aware security, and scalability makes the proposed system a viable solution for next-generation IoT environments.

V. Conclusion

This research comprehensively evaluated the effectiveness of a CNN-based framework for automatic facial emotion recognition, achieving an overall accuracy of 86% and robust performance across precision, recall, and F1-score metrics on the FER-2013 dataset. By leveraging deep hierarchical feature extraction, data augmentation, and optimized CNN architectures, the proposed approach successfully captures subtle emotional cues without relying on handcrafted features, making it suitable for real-world applications in mental health monitoring, adaptive tutoring, human–computer interaction, and surveillance systems. Despite these promising results, challenges such as variations in cultural expression, spontaneous facial movements, occlusions, and imbalanced datasets persist. Future research directions include integrating multimodal data such as speech, physiological signals, and body gestures to enhance emotion recognition accuracy, developing more diverse and representative datasets, exploring lightweight and real-time CNN models for deployment on edge devices, and addressing ethical considerations related to privacy, fairness, and responsible AI deployment to ensure trustworthy and socially beneficial emotion-aware systems.

References

1. S. Priya, M. M. Sithik, A. Mohamed Anwar, S. P. Santhoshkumar, M. Uveise S A and P. Arora, "Adaptive Service Dependent Proximity Analysis Based Intrusion Detection in Cloud Environment," 2025 Global Conference in Emerging Technology (GINOTECH), PUNE, India, 2025, pp. 1-5, doi: 10.1109/GINOTECH63460.2025.11076953.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

2. M. Kobayashi, H. Miyaji and H. Yamamoto, "Proximity Verification Function of Real World Data Sources Based on Similarity Analysis on Environmental Information," 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC), Osaka, Japan, 2024, pp. 1452-1455, doi: 10.1109/COMPSAC61105.2024.00193.
3. K. K. Sachan and A. Natarajan, "Proximity Detection Based Low-Cost and Handheld IoT Device for Tracking Lost Objects," 2024 IEEE International Symposium on Smart Electronic Systems (iSES), New Delhi, India, 2024, pp. 40-43, doi: 10.1109/iSES63344.2024.00019.
4. F. Chahal, H. Fouchal and D. Gaïti, "Proximity Marketing: A Diverse Classification Approach," 2024 International Wireless Communications and Mobile Computing (IWCMC), Ayia Napa, Cyprus, 2024, pp. 879-884, doi: 10.1109/IWCMC61514.2024.10592562.
5. C. Lai, Z. Liu and D. Zheng, "Privacy-Preserving Proximity Tracing System for Large-Scale Public Health Events," 2024 IEEE/CIC International Conference on Communications in China (ICCC), Hangzhou, China, 2024, pp. 114-119, doi: 10.1109/ICCC62479.2024.10681684.
6. B. Kumar and K. S. Gill, "Silent Protection: The Future of Home Safety with IoT in Light-Free Spaces," 2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE), GHAZIABAD, India, 2024, pp. 1204-1206, doi: 10.1109/AECE62803.2024.10911636.
7. K. Izrailov and I. Kotenko, "Investigating the Proximity Metric of Program Assembler Code for Genetic Reverse Engineering," 2025 33rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), Turin, Italy, 2025, pp. 600-607, doi: 10.1109/PDP66500.2025.00090.
8. M. R. Rownak, X. Diao and C. Smidts, "Human Reliability Under Physical Security Threats: Modeling and Experimental Design," 2024 Annual Reliability and Maintainability Symposium (RAMS), Albuquerque, NM, USA, 2024, pp. 1-6, doi: 10.1109/RAMS51492.2024.10457692.
9. B. S. Liya, C. Rohith, M. Jubbair Ahmad and B. Khishore, "Missing Persons Comprehensive Tracking System with Multi-Area CCTV Integration and Proximity-Based Police Station Mapping," 2024 2nd International Conference on Computer, Communication and Control (IC4), Indore, India, 2024, pp. 1-5, doi: 10.1109/IC457434.2024.10486474.
10. C. Constantinescu et al., "Analyzing Antenna Proximity Influence on the Human Body from an Educational Perspective," 2025 34th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE), Cluj-Napoca, Romania, 2025, pp. 1-4, doi: 10.1109/EAEEIE65428.2025.11136279.
11. D. Borodin and D. Skudnev, "Disadvantages of Using the Heuristic Function of Proximity of the Execution Path to the Reference," 2024 6th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russian Federation, 2024, pp. 64-67, doi: 10.1109/SUMMA64428.2024.10803867.
12. S. Gupta, R. K. Saxena, R. Vijay, A. K. Sharma, A. Kumar and D. P. Gupta, "Privacy Models on Location Hiding and Security Observations in Local Area WSN," 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, Raigarh, India, 2025, pp. 1-5, doi: 10.1109/OTCON65728.2025.11070960.