Department: Head

Continuous Authentication for Consumer Electronics in Smart City Surveillance

Basudeb Bera
National University of Singapore

Prakash Tekchandani
International Institute of Information Technology, Hyderabad

Ashok Kumar Das
International Institute of Information Technology, Hyderabad

Marimuthu Karuppiah
Presidency University, Bengaluru

Biplab Sikdar
National University of Singapore

***Abstract*—In the realm of smart city surveillance, consumer electronics (CE) devices communicate through vulnerable wireless channels, posing significant security risks. To ensure secure and uninterrupted services for residents, continuous monitoring is imperative. Existing authentication methods for CE in smart cities authenticate users/devices at the onset of a communication session, assuming they remain authenticated throughout. However, temporary access by an attacker to the user's or CE device can lead to impersonation. To mitigate this security threat, we propose a continuous authentication (CA) protocol utilizing vector similarity search (VSS), which has emerged as a novel approach to enhance security and privacy in CE deployed within smart city surveillance systems. Through the employment of VSS techniques and secure communication via session key establishment, the proposed scheme continuously monitors user behavior and verifies legitimacy, ensuring seamless operation and protection against a myriad of potential threats. This innovative framework enhances the resilience of smart city infrastructures against unauthorized access, data tampering, data poisoning attacks, and other malicious activities.**

CONSUMER ELECTRONICS (CE) refer to electronic devices and gadgets designed for personal and household use, typically for entertainment, communication, productivity, and convenience purposes. Consumer electronics encompass a wide range of prod-

Digital Object Identifier 10.1109/MCE.YYYY.Doi Number
Date of publication DD MM YYYY; date of current version DD MM YYYY. (Corresponding authors: Ashok Kumar Das; Marimuthu Karuppiah).

Published by the IEEE Consumer Technology Society

ucts. Smart thermostats, refrigerators, lighting systems, speakers, displays, locks, cameras, and robotic vacuum cleaners are commonly found in smart home applications. Additionally, wearable devices such as smartwatches, fitness trackers, smart glasses, and smart clothing are worn on the body to track health metrics, receive notifications, and perform various tasks. Smart cities leverage information and communication technology (ICT), Internet of Things (IoT) technology, artificial intelligence (AI) based data analytics, and digital connectivity through wired or wireless networks to enhance the quality of life for residents, improve sustainability, and optimize resource utilization. These cities utilize cutting-edge technologies to address various urban challenges, such as transportation congestion, energy consumption, environmental pollution, public safety, migration problem, and infrastructure management [1].

CE Appliances

CE in smart cities encompass a wide range of devices, applications, and technologies. Some examples of CE commonly found in smart cities environments include:

- *CE in Smart Grid:* Smart grid technologies utilize smart meters, grid sensors, advanced monitoring and control systems, and communication networks that enable real-time monitoring, analysis, and optimization of energy usage and distribution.
- *CE in Smart Home:* In smart homes, CE include smart thermostats, lighting systems, surveillance cameras, smart locks, voice-activated assistants, smart refrigerators, washing machines, and wearable devices for health monitoring. Often interconnected via IoT technology, these devices contribute to remote monitoring and management of various aspects of homes, optimizing energy usage, enhancing security, and creating personalized living experiences.
- *CE in Intelligent Transportation Systems (ITS):* ITS integrate CE such as sensors, cameras, tracking devices, connected vehicle technologies, and communication networks, including traffic monitoring systems and adaptive traffic signal control. This integration aims to improve the efficiency, safety, and sustainability of transportation systems within smart cities.
- *CE in Smart Healthcare:* Smart thermometers, smart blood pressure monitors, wearable fitness trackers, smartwatches, smartphone applications for symptom tracking and telemedicine consultations, smart electrocardiogram (ECG) monitors, continuous glucose monitoring (CGM) sensors, and others are utilized in smart healthcare systems to monitor patient health metrics, deliver personalized medical insights, and promote proactive self-care.
- *CE in City Security and Surveillance:* Smart cities often deploy surveillance cameras and IoT sensors for monitoring public spaces, traffic, crowd, migration, and infrastructure.
- *CE in Smart Waste Management (SWM):* IoT-enabled waste bins sensors and smart trash compactors are utilized in SWM to monitor and optimize waste collection routes, reduce operational costs, and improve recycling rates.
- *CE in City Environmental Monitoring Systems:* Air and water quality smart sensors, radiation detectors, soil moisture sensors, and noise pollution sensors are utilized to monitor air and water quality, radiation levels, soil moisture levels, noise levels, and other environmental parameters to mitigate potential disasters.
- *CE in Urban Mobility Solutions (UMS):* In UMS, CE include ride-sharing platforms, electric vehicle charging infrastructure, bike-sharing systems, and mobile applications that provide convenient, efficient, and sustainable transportation options within smart cities.

From the above discussion, it is noted that CE smart cameras play an important role in smart city surveillance. These smart cameras are deployed in various locations throughout the smart city, including public places, schools, malls, marketplaces, bus terminals, etc., and collect sensing information about their designated zones, such as images of people, vehicles, and traffic. Primarily, these devices are connected through wireless networks and transmit their collected information to associated cloud servers. However, during the transmission of data between smart devices and servers, they become vulnerable to various attacks if a strong security mechanism is not adopted, which has become a significant concern nowadays.

Security and Privacy Issues in CE

Security and privacy issues in CE are becoming increasingly significant in today's world. In smart city environments, CE devices are installed in various areas where continuous monitoring is not always feasible.

Taking advantage of this, adversaries can gain access to these devices and install malicious sensor devices. CE devices collect and store sensitive information in smart cities, including transaction-related data in shopping malls, personal information, location data, and usage patterns. Insufficient security measures can render this data vulnerable to unauthorized access and exploitation by adversaries, leading to data breaches and privacy violations [2]. Weak authentication in communication channels can make them vulnerable, allowing unauthorized users to access sensitive information and potentially compromise privacy and security. Unauthorized access to these devices can also enable attackers to spy on users, eavesdrop on conversations, or monitor activities within homes, violating individuals' privacy rights. Outdated software and firmware make these CE devices easy targets for cyberattacks, posing prolonged security risks. Moreover, CE devices often communicate with external servers over insecure channels, such as unencrypted Wi-Fi networks or poorly secured Internet connections. This exposes sensitive data, compromising data confidentiality and integrity due to the risk of data modification [3].

Traditional Methodologies

The traditional security mechanisms include symmetric/asymmetric encryption, access control, key agreement, user/device authentication, and certificates. Encryption of data helps to securely store it on CE devices or transmit it over networks to protect it from unauthorized access. Certificates also contribute to preventing unauthorized access. User/device authentication ensures that only authorized users can access CE devices and their functionalities. This may involve passwords, biometric authentication, two-factor authentication, or multi-factor authentication. Utilizing access control mechanisms allows administrators to define and enforce policies regarding who can access what resources on CE devices. One-way cryptographic hash functions are used to maintain the integrity of data during communication between CE devices and their related systems. Nowadays, blockchain technology is also utilized for secure storage of CE data [4]. By implementing these traditional security methodologies [5], manufacturers and users can enhance the security posture of CE and mitigate the risk of security breaches and data compromises.

Security Gaps in Existing Works

In 2022, Meher et al. [6] presented an authentication mechanism that relied on the elliptic curve discrete logarithm problem (ECDLP) for a consumer warehouse management system. However, adversaries can disclose the used identities and launch ESL attacks under the CK-adversary model and replay attack. In 2023, Wang et al. [7] proposed a cloud-based authentication and key agreement scheme for IoT applications. In their scheme, a session key is created through a combination of a hash function and elliptic curve cryptography (ECC), integrating random numbers and public parameters. Nonetheless, this method is susceptible to Ephemeral Secret Leakage (ESL) attacks under the Canetti and Krawczyk's adversary model (CK-adversary model) [8] and replay attacks. In 2023, Mahmood et al. [9] suggested an access control solution for AI-powered autonomous aerial vehicles within consumer electronics. Their system constructs a session key between a drone and a ground station server with hash function and ECC, and fails to provide forward secrecy. In 2023, Ayub et al. [10] proposed an authentication scheme utilizing ECC for a consumer-oriented demand response management system within the smart grid context. Nonetheless, a drawback of their scheme is its susceptibility to ESL attacks under the CK-adversary model. In 2023, Hu et al. [11] offered an authentication and key agreement protocol designed for smart metering within smart grid applications. However, their protocol lacks resilience against denial of service (DoS) attacks and fails to ensure anonymity. Moreover, their scheme is vulnerable to privileged insider and man-in-the middle (MiTM) attacks, as highlighted by Ma et al. [12].

In smart city surveillance, continuous monitoring is required to provide secure and seamless services to residents. Existing authentication protocols typically authenticate users/devices at the start of a communication session, assuming they remain authenticated throughout.

Novelty of vector similarity search in CA for smart city

Vector Similarity Search (VSS) is a technique used to identify and compare data points by analyzing their vector representations. It involves converting data into high-dimensional vectors and then measuring the similarity between these vectors to determine how closely related they are. VSS is commonly used in applications such as information retrieval, recommen-

dation systems, and pattern recognition, where it helps in efficiently finding and matching similar items or behaviors based on their vector embeddings [13].

The integration of VSS into CA introduces significant innovations in security and accuracy. VSS enables dynamic and ongoing analysis of user and device behavior by converting diverse data types, such as text, images, video, and audio, into structured vectors. This continuous monitoring enhances precision in verifying user identity and detecting anomalies, making it difficult for attackers to impersonate users or devices. The adaptability of VSS allows it to handle a wide range of data formats and contexts, improving its application in smart city environments. Furthermore, VSS supports real-time detection of suspicious activities, enabling prompt defensive actions and adaptive responses. Its scalability and flexibility make it well-suited for large-scale implementations, providing robust and versatile authentication across various scenarios. Overall, the use of VSS in CA represents a novel approach that significantly strengthens security by continuously validating behavior in real-time.

Motivation

Most research focuses on external attacks on CE devices, but internal threats from within the network can be more dangerous. Internal users can inflict significant harm, and existing authentication protocols often only verify users at the start of a session, leaving them vulnerable if an attacker briefly gains access. Therefore, continuous and seamless authentication is needed to maintain verification throughout the session. Current security flaws in CE are susceptible to various attacks, such as Man-in-the-Middle (MiTM), replay, impersonation, Ephemeral Secret Leakage (ESL), identity leakage, and Denial-of-Service (DoS). Many methods rely on static credentials like passwords or tokens, which fail to account for dynamic factors like user behavior or context.

Continuous authentication using VSS in smart city surveillance systems offers significant advantages in security and user experience. By continuously monitoring user behavior throughout a session rather than just at the start, VSS enhances security by detecting and responding to suspicious activities or potential breaches in real time. It effectively mitigates impersonation risks and adapts to the dynamic nature of smart city environments by continuously updating and verifying behavior patterns against a vector database. VSS also provides robust resistance to traditional attacks such as replay and data tampering, and improves user experience by minimizing the need for frequent logins. Additionally, it allows for precise fraud detection through detailed behavioral analysis and scales efficiently to handle large volumes of data, ensuring comprehensive security across extensive networks.

In smart city surveillance, continuous monitoring is crucial for secure and seamless services. CA with VSS, we can constantly verify user behavior by converting diverse data into structured vectors. This approach can trigger defensive measures, such as locking a device and sounding an alarm, if suspicious activity is detected. CA-based security offers stronger protection than traditional methods, ensuring robust defense without disrupting services.

The novel contributions of the proposed framework as follows:

- *Introduction of continuous authentication (CA):* The proposed protocol introduces CA for consumer electronics devices within smart city surveillance systems, moving beyond traditional methods that only authenticate devices at the start of a communication session.
- *Novel approach of VSS:* The scheme employs vector similarity search (VSS) technique, a novel approach, to enhance the security and privacy of smart city environment. This represents a novel application of VSS in the context of continuous authentication.
- *Continuous monitoring and verification:* The protocol continuously monitors user behavior and verifies their legitimacy throughout the communication session with VSS, addressing the security risk of temporary access by an attacker leading to impersonation.
- *Enhanced security measures:* By integrating VSS with secure session key, the proposed framework improves protection against unauthorized access, data tampering, data poisoning attacks, vector manipulation attacks, and other malicious activities.
- *Real-world efficiency:* The performance analysis of VSS demonstrates the scheme's efficiency and effectiveness in real-world scenarios, showcasing its practical applicability and robustness in smart city environments.

PROPOSED MODEL

In this section, we propose a CA protocol for CE in smart city surveillance to provide secure and seamless

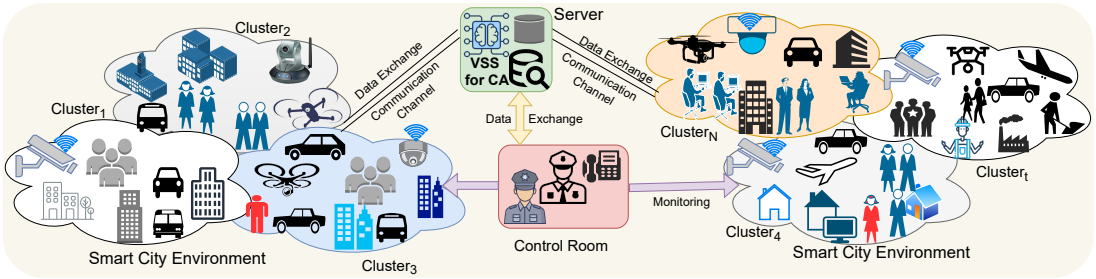


Figure 1. A general architecture for CE in smart city surveillance.

services to residents without disruption. CA continuously authenticates users whenever they attempt to access any smart city services. This authentication process is conducted via CE devices such as smart cameras, where the user's physiological or behavioral biometrics can be utilized for authentication. For instance, if an unauthorized individual attempts to access smart city services, such as e-healthcare services, CA can detect this using his/her behavioral biometrics and trigger an alarm for defensive measures to mitigate any potential threats.

Architecture

A smart city can be divided into various clusters, each of which contains installed CE devices. These devices are predominantly connected via wireless mediums and communicate with a server. Prior to deployment, each CE device undergoes a registration process with a trusted registration authority (RA). Users or residents within each cluster must register with the RA, after which the RA securely stores their data and certificates on the server, and also loads private and public parameters and certificates onto the CE devices. Once operational, a CE device collects user information from its respective cluster and securely sends it to the server. Vector Similarity Search (VSS) operates on server side to identifies authorized individuals by converting face images collected by the installed smart camera into high-dimensional feature vectors through a feature extraction process, such as using a deep neural network. These feature vectors, which capture unique facial characteristics, are stored in a database along with corresponding identities. When a new face image is presented for verification, it is processed to generate its own feature vector. This vector is then compared to the stored vectors in the database using similarity measures like Euclidean distance or cosine similarity. If the similarity score between the query vector and any stored vector exceeds a predefined threshold, the new face is considered a match, thereby confirming the individual's identity as authorized. This method ensures that the authentication system can accurately and efficiently verify individuals based on their facial features. In case of the verification fails, the server sends a notification to the control center to initiate defensive measures. A pictorial presentation of this architecture is depicted in Fig. 1.

Threat Model

Since CE devices in smart cities communicate through wireless mediums, many of which lack security measures, this raises security concerns. We assume that the adversary $\mathcal{A}$ is capable of launching attacks on the communication under the following security threat models: the Dolev-Yao (DY) [14] and Canetti-Krawczyk (CK) [8] and extended CK (eCK) adversary threat models. In the DY threat model, $\mathcal{A}$ can eavesdrop on communication and also modify, delete, or inject malicious content into it. In the CK-adversary threat model, $\mathcal{A}$ gains additional advantages over the DY model, such as the ability to alter, intercept, erase, or insert fake information into communication. Additionally, $\mathcal{A}$ can compromise short-term and long-term secrets, as well as session states, during the session establishment phase. In the eCK model, the adversary has extra powers compared to the CK model, making it a stronger threat. For instance, the adversary can actively perform queries like asking to reveal a session key for a specific session ID, which could undermine the security of that session. If a session or its related parts are compromised in the eCK model, they are considered exposed to adversary. Thus, the eCK model gives adversary much greater ability to interfere with or break communications. In the hostile environment

of a smart city, $\mathcal{A}$ can physically compromise a CE device and launch side-channel attacks, such as power analysis attacks [15], to extract saved credentials from the compromised device's memory. In addiotion, we consider data poisoning attack, where data poisoning as a type of adversarial attack where malicious actors inject false or misleading data into a system's training or operational datasets. This can skew the system's learning process or decision-making, leading to incorrect or compromised outputs. In the context of smart city surveillance, data poisoning attacks are particularly concerning because they can undermine the accuracy and reliability of surveillance systems, potentially allowing unauthorized access or misidentification of individuals.

Registration and Vector Database Creation Process

During the registration process, the RA assigns unique and distinct identities to each CE device, as well as private and public keys for both the CE devices and the server. The RA generates certificates using its own private key for each CE device and the server. Users in different clusters also securely register with the RA over time and receive unique identities. Upon successful registration, the RA securely loads private and public keys, as well as certificates, onto the CE devices and the server. Additionally, the RA uploads user data to the server and publishes all public keys.

Upon receiving data from the smart city, the server executes embedding vector calculation. This involves transferring the received data into vectors using embedding techniques. For example, image data can be converted into vectors using neural networks (NN). Subsequently, these vectors are used to construct an embedding vector database (EVDB), linking them to their original content where the embedding was created. Next, an indexing technique is performed for efficient similarity search.

Continuous Authentication Process

The CA process starts once an initial session key is established between a CE device and the server. To establish this key, both parties first mutually authenticate each other using their pre-loaded certificates. Then, they utilize their long-term secrets and generate fresh timestamps and random numbers, along with cryptographic secure hash functions, to construct this session key. Once the session key, denoted as SK, is established and is valid for a duration of ΔT, where ΔT represents the time interval during which the session key is validated in the continuous authentication process, the CA operates in the background using SK. The server continuously monitors user activity by encrypting data with the session key (SK) received from CE devices, and then decrypts it using the same SK to validate user legitimacy through VSS techniques and detect any suspicious behavior. The protocol monitors user face recognition behavior as a key aspect of continuous authentication. Specifically, the protocol tracks facial features and patterns to verify ongoing user identity. The deviations from the expected facial recognition patterns are detected through real-time analysis of feature vectors using VSS, comparing them to previously established profiles. If significant deviations are identified such as changes in facial features due to unauthorized access or spoofing attempts, the system flags these anomalies and may trigger re-authentication or other security measures. Throughout this process, raw data (say, $data_i$) from the CE devices are collected in an encrypted form as $Enc_{SK}(data_i)$ with the session key SK and undergo the following steps:

- The server first decrypts the $data_i$ as $data_i \longleftarrow Dec_{SK}(Enc_{SK}(data_i))$.
- $[v_i] \longleftarrow Embeding(data_i)$: This embedding vector calculation technique transforms the received data $data_i$ into vectors $[v_i]$ using feature extraction or embedding methods. For example, Convolutional Neural Networks (CNNs) are widely used for image feature extraction and can generate high-dimensional feature vectors that capture the visual characteristics of an image.
- $\{1, 0\} \ni \theta \longleftarrow Querying(EVDB, [v_i])$: Given the query $[v_i]$, the EVDB retrieves the most similar vectors from the indexed dataset using a distance metric, and these vectors are returned as the search results. The search results are then verified with the existing identities database for a match. If the match result θ is 1, then the received $data_i$ corresponds to a valid user; otherwise, it corresponds to an unknown user.

This continuous validation remains active until the session duration expires. Once the session expires, the next session will be initiated, and a session key will be established between the CE device and the server. Similarly, the CA will continue to execute in the background until the session expires. The overall process of the proposed scheme for smart city surveillance in

shown in Fig. 2.

SECURITY ANALYSIS

This section discusses how the proposed framework is able to resist the following important attacks.

1) Replay Attacks

During the initial session key set up process, the communicated message contains a fresh timestamp and random number which is used to calculate a hash digest. As a result, an adversary $\mathcal{A}$ cannot change timestamp and random number to launch replay attacks, since $\mathcal{A}$ is unable to alter the cryptographically secure hash digest. Moreover, after receiving the messages, the receiver verify its freshness and it can be detect the older message easily. Hence, the proposed scheme is secure against replay attacks.

2) Man-in-the-Middle (MiTM) Attacks

In this scenario, $\mathcal{A}$ might intercept the session key setup request message under the DY threat model and attempt to create a valid message on behalf of the CE device in real-time. To do this, $\mathcal{A}$ would need to generate a valid timestamp and random number. However, without access to the long-term secret key of the CE device, $\mathcal{A}$ cannot decipher the request message. Therefore, $\mathcal{A}$ cannot execute a MiTM attack, demonstrating that the proposed scheme effectively resists MiTM attacks.

3) Impersonation Attacks

In this attack, the adversary aims to establish a session and generate a valid session key (SK) on behalf of a CE device. To accomplish this, $\mathcal{A}$ requires both the long-term and short-term secrets. For the impersonation attack to be successful, $\mathcal{A}$ would need to obtain these secrets and the associated certificate. Since this information is securely protected by a hash function, computing a valid session key request message is computationally challenging. Therefore, the proposed scheme is secure against impersonation attacks.

4) CE Device Physical Capture Attacks

In this attack scenario, we consider the case where a CE device is either stolen or physically captured by $\mathcal{A}$. $\mathcal{A}$ gains access to the data stored on the compromised device's memory using power analysis attacks. However, each CE device has unique and distinct registration credentials. As a result, compromising one CE device does not impact others in the network. Therefore, the compromise of a single CE device does not affect the overall network, demonstrating that the proposed scheme is resilient to device capture attacks.

5) Session Key Leakage Attacks

In this attack scenario, we consider a more powerful adversary $\mathcal{A}$ under the CK-adversary threat model, which can reveal a session key and attempt to bypass continuous authentication. The session key is utilized to share the data $data_i$. Continuous authentication is then performed based on this data. The established session key is derived from both session-specific (ephemeral) credentials, such as random numbers and timestamps, and long-term secrets. $\mathcal{A}$ would need to compromise both the session-specific and long-term secrets to reveal the session key. Additionally, the use of random numbers and timestamps in each session ensures that session keys are always unique. Even if a session key is exposed for one session, it will not facilitate the computation of session keys for other sessions due to the combination of both short-term and long-term secrets. Thus, the proposed scheme is secure against the session key leakage attacks.

6) Vector Manipulation Attacks

Throughout the continuous authentication processes, the CE device transmits data to the server, with the data encrypted using the secure session key (SK) as $Enc_{SK}(data_i)$. After receiving the data, the server decrypts it as $Dec_{SK}(Enc_{SK}(data_i))$. Consequently, $\mathcal{A}$ is unable to access or disclose this data, nor can it inject modified vectors into the communication by compromising the session state. Upon receiving the data and decryption, the server extracts the feature vectors and verifies them against the existing database. As a result, $\mathcal{A}$ cannot manipulate the vectors used in VSS. Therefore, the proposed scheme effectively protects against vector manipulation attacks.

SIMULATION RESULTS AND DISCUSSIONS

In this research, we present a comprehensive methodology for generating multimodal embedding from images and performing efficient similarity search using Vertex AI Search. Our approach begins by employing a pre-trained multimodal embedding model to extract embedding from images in a specified folder, with the option to include metadata for each image. These embedding are then stored in a JSON file for

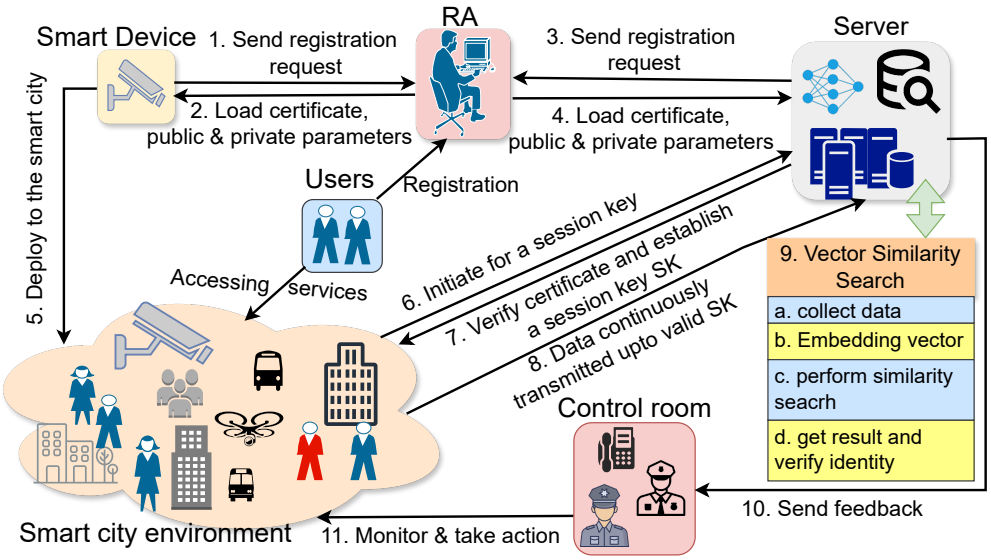
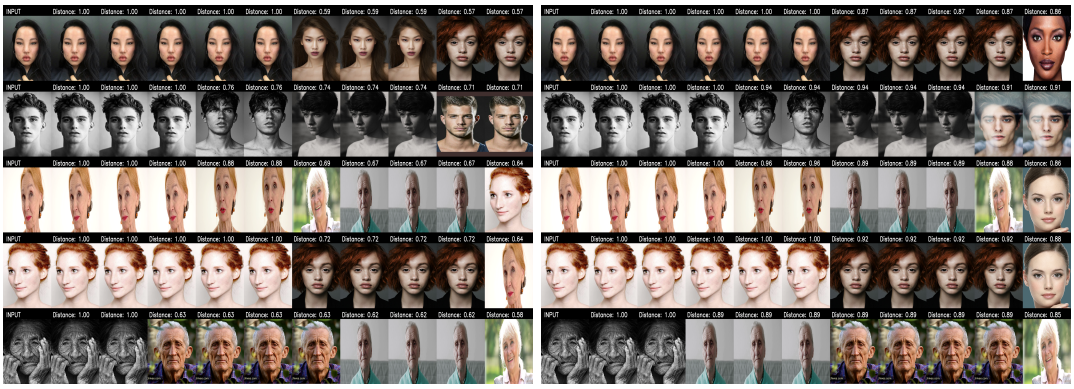


Figure 2. Overall process of the proposed method for smart city surveillance.



(a) (b)

Figure 3. Positive match for (a) 1408 dimensions (b) 128 dimensions.

subsequent analysis. Next, we utilize a Vertex AI Search index deployed with the tree-AH algorithm, configured with a dot product distance measure, a neighbor count of 10, and a dimensionality of 1408. This index allows us to conduct similarity search operations efficiently. We demonstrate the effectiveness of our method through practical implementation, where we query the Vertex AI Search index with the generated embedding. The query returns the nearest neighbors within the index, which are then visually presented alongside the input image to illustrate the similarity search results. Each input image yields 10 matching images along with their corresponding feature vectors and distances. This methodology showcases the potential of multimodal embedding and Vertex AI Search in enabling content-based image retrieval tasks across various domains.

We have used the dataset for our experiments available at https://www.kaggle.com/datasets/ashwingupta3012/human-faces. It contains approximately 7000 human face images. The dataset we used is designed to be diverse, incorporating various creeds, races, age groups, and profiles to ensure it is representative and unbiased. It includes both real and Generative Adversarial Network (GAN)-generated images to aid in distinguishing between authentic and synthetic faces. Special attention was given to including a significant number of images of senior citizens and a small portion of realistic fake faces to improve the robustness of identification across a

(a) (b)

Figure 4. Negative match for (a) 1408 dimensions (b) 128 dimensions.

broad spectrum of images. We conducted experiments considering both 128 and 1408-dimensional feature vector spaces, where the Vertex search Index was generated using feature vectors of these dimensions. These embedding were deployed to the Vertex AI index endpoint. Similarity is measured by the dot product and represented as a distance. A distance value of 1 indicates an exact match, while 0 indicates no match. In the first experiment, shown in Fig. 3(a), the inputs are known faces, already present in our Vertex AI. We observe that the INPUT face exactly matches the Vertex AI search. Additionally, it correlates with other images, but the distance is much less than 1. Fig. 3(b) also predicts a perfect match, but the similarity with the other images is also high. Thus, the results of the 1408 dimensions are more robust than those of 128 dimensions.

We also considered the case where the inputs are not known faces, i.e., not in our Vertex AI search. Figure 4 shows the results for a negative match for the 1408-dimensional feature vector. The similarity value is much less than 1, and hence, we can safely predict that this is a new human face. Figure 4 shows similar results for a negative match, but the values are close to 1, thus, again showing that the results of dimension 1408 are more robust.

The latency and queries per second (QPS) on machine type n1-standard-16 are shown in Fig. 5 and Fig. 6, respectively. The latency is very low, and the performance of queries per second is up to 0.12/s. This demonstrates the robustness of our platform.

CHALLENGES AND FUTURE DIRECTIONS

Achieving real-time processing of CA requests from numerous CE devices while maintaining low latency is crucial for ensuring seamless user experiences in smart city surveillance. Additionally, CE devices face resource constraints, posing challenges for implementing lightweight authentication protocols.

Future research directions include exploring hybrid authentication approaches that combine CA with other authentication methods and developing transparent and interpretable advanced machine learning models, such as deep learning and reinforcement learning, to enhance trust, accuracy, robustness, and accountability of CA in smart city surveillance. Exploring the integration of blockchain technology to enhance the security, transparency, and immutability of CA logs and identity management systems in smart city surveillance is also a promising avenue. With quantum computing emerging as a new threat to traditional cryptosystems based on computational hardness, investigating privacy-preserving techniques such as differential privacy, post-quantum cryptography, lattice based cryptography, and homomorphic encryption is essential to protect user privacy while performing CA using VSS in smart city surveillance scenarios.

CONCLUSION

In our proposed method, continuous authentication using vector similarity search presents a promising approach for enhancing security and privacy in CE for smart city surveillance systems. By continuously monitoring user behavior and verifying legitimacy through vector similarity search techniques, CA offers a robust defense against unauthorized access and ma-

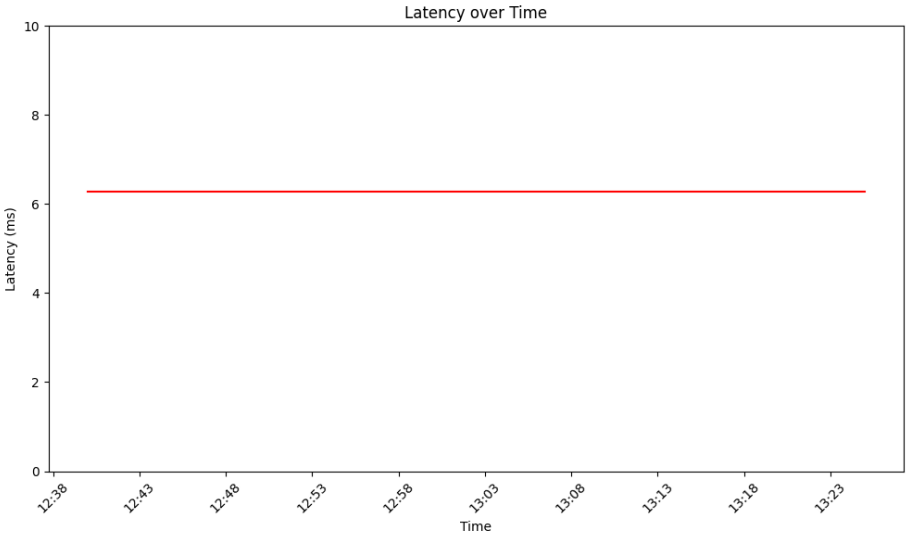


Figure 5. Latency

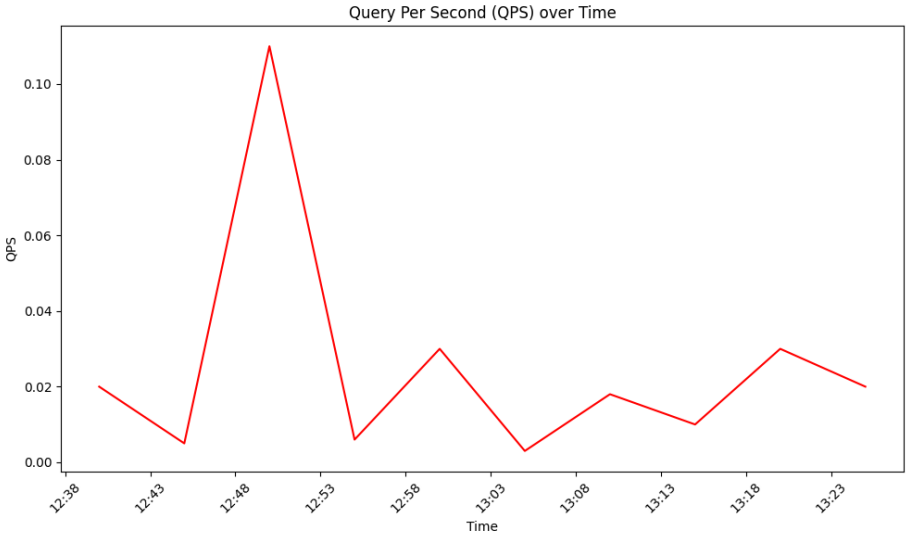


Figure 6. Queries per second

licious activities. In this proposed scheme, the data sharing between a CE device and the server utilizes a secure session key, indicating that this scheme is resilient against various potential attacks, including data poisoning, replay, MiTM, and ESL attacks. Furthermore, future research directions including hybrid authentication approaches, advanced machine learning models, blockchain integration, and post-quantum privacy-preserving techniques hold the potential to further enhance the effectiveness and resilience of CA in smart city surveillance. As smart city ecosystems continue to evolve, CA using VSS has emerged as a critical component for safeguarding user data, preserving privacy, and maintaining the integrity of smart city infrastructures.

REFERENCES

1. D. A. Hahn, A. Munir, and S. P. Mohanty, “Security and Privacy Issues in Contemporary Consumer Electronics [Energy and Security],” *IEEE Consumer Electronics Magazine*, vol. 8, no. 1, pp. 95–99, 2019.
2. A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, “A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications,” *IEEE*

Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1125–1159, 2021.

3. M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2019.
4. Y. Djenouri, A. Yazidi, G. Srivastava, and J. C.-W. Lin, "Blockchain: Applications, Challenges, and Opportunities in Consumer Electronics," *IEEE Consumer Electronics Magazine*, vol. 13, no. 2, pp. 36–41, 2024.
5. A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure," *IEEE Access*, vol. 9, pp. 71 856–71 867, 2021.
6. B. K. Meher, R. Amin, A. K. Das, and M. K. Khan, "KL-RAP: An Efficient Key-Less RFID Authentication Protocol Based on ECDLP for Consumer Warehouse Management System," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3411–3420, 2022.
7. C. Wang, D. Wang, Y. Duan, and X. Tao, "Secure and Lightweight User Authentication Scheme for Cloud-Assisted Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2961–2976, 2023, doi: 10.1109/TIFS.2023.3272772.
8. R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.
9. K. Mahmood, T. Tariq, A. K. Sangaiah, Z. Ghaffar, M. A. Saleem, and S. Shamshad, "A Neural Computing-based Access Control Protocol for AI-driven Intelligent Flying Vehicles in Industry 5.0-assisted Consumer Electronics," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023.
10. M. F. Ayub, X. Li, K. Mahmood, S. Shamshad, M. A. Saleem, and M. Omar, "Secure Consumer-Centric Demand Response Management in Resilient Smart Grid as Industry 5.0 Application With Blockchain-Based Authentication," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023, doi: 10.1109/TCE.2023.3320974.
11. S. Hu, Y. Chen, Y. Zheng, B. Xing, Y. Li, L. Zhang, and L. Chen, "Provably Secure ECC-Based Authentication and Key Agreement Scheme for Advanced Metering Infrastructure in the Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 5985–5994, 2023.
12. H. Ma, C. Wang, G. Xu, Q. Cao, G. Xu, and L. Duan, "Anonymous Authentication Protocol Based on Physical Unclonable Function and Elliptic Curve Cryptography for Smart Grid," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6425–6436, 2023.
13. K. Echihabi, K. Zoumpatianos, and T. Palpanas, "New trends in high-D vector similarity search: al-driven, progressive, and distributed," *Proceedings of the VLDB Endowment*, vol. 14, no. 12, pp. 3198–3201, 2021.
14. D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.
15. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

Basudeb Bera is a post-doctoral researcher at the Department of Electrical and Computer Engineering, National University of Singapore (NUS). His research interests include cryptography and network security, AI/ML security and post-quantum cryptography. Bera received his Ph.D. degree in computer science and engineering from International Institute of Information Technology, Hyderabad, India. Contact him at b.bera26@nus.edu.sg.

Prakash Tekchandani is currently a Ph.D. student in Computer Science and Engineering at the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His research interests include network security, Big Data Analytics and Blockchain. Contact him at prakash.tekchandani@research.iiit.ac.in.

Ashok Kumar Das is a full professor at International Institute of Information Technology, Hyderabad, India. He is also an adjunct professor with the Department of Computer Science and Engineering, College of Informatics, Korea University, Seoul, South Korea. His research interests include system and network security, AI/ML security and post-quantum cryptography. Das received his Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is a senior member at IEEE. Contact him at iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in.

Marimuthu Karuppiah is a Professor with the School of Computer Science and Engineering & Information Science, Presidency University, Bengaluru, India. Marimuthu received his Ph.D. degree in computer science and engineering from VIT University, Vellore, India. His research interests include cryptography and network security. He is a senior member at IEEE. Contact him at marimuthume@gmail.com.

Biplab Sikdar is a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he serves as the Head of

Department of the Department of Electrical and Computer Engineering. He received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and an Associate Editor for the IEEE Transactions on Mobile Computing from 2014 to 2017. Contact him at bsikdar@nus.edu.sg.