Brief Report
Volume 16:01, 2025

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

A Biometric and PUF-based Privacy Framework for Integration of Internet of Things in Smart Cities

David Daniel*

Department of Biometry and Data Management, University of Zurich, Zurich, Switzerland

Introduction

As smart cities evolve through the integration Of Internet of Things (IoT) technologies, the need for robust, scalable, and privacy-preserving authentication mechanisms becomes paramount. IoT devices used in smart city infrastructure such as traffic sensors, energy meters, surveillance systems, and healthcare monitors are often resource-constrained and deployed in environments that are vulnerable to physical and cyber-attacks. Traditional password-based authentication is not only impractical in such settings but also fails to meet the high-security standards required for citizen data protection. To address these challenges, researchers and developers are increasingly turning to innovative combinations of biometric authentication and Physically Inclinable Functions (PUFs) to ensure both strong identity verification and device-level uniqueness without compromising privacy. This framework offers a promising path forward for secure, user-friendly authentication in large-scale, heterogeneous IoT environments [1].

Description

The proposed biometric and PUF-based privacy framework leverages the inherent advantages of both technologies. Biometric systems (such as fingerprint, facial recognition, or iris scans) provide a convenient and user-specific means of identity authentication. Meanwhile, PUFs exploit manufacturing variations in hardware components to produce device-specific digital fingerprints that are nearly impossible to replicate or forge. The combination of these two techniques creates a dual-layered security approach: biometrics authenticates the user, and PUFs authenticate the device. The authentication process begins with the capture of a user's biometric input, which is securely encrypted and matched against previously enrolled templates. Simultaneously, a PUF challenge-response protocol is executed on the device to verify its hardware authenticity. Because PUFs do not store any secret keys but instead generate them dynamically from the hardware's physical characteristics, they eliminate the risk of key extraction in case of physical tampering. Moreover, to preserve privacy, the framework includes cryptographic hash functions and secure key exchange protocols to ensure that neither biometric data nor PUF responses are transmitted in raw form. This reduces the attack surface for potential intruders [2].

The rapid deployment of Internet of Things (IoT) devices in smart cities ranging from public surveillance systems and traffic control sensors to healthcare monitoring devices and smart utility meters has amplified the demand for secure, efficient, and privacy-conscious authentication mechanisms. Traditional methods such as password-based login or centralized identity verification are not only inadequate in handling the scale and heterogeneity of smart city infrastructure but also pose significant privacy and cybersecurity risks. This has led to the development of integrated security frameworks that combine biometric authentication and Physically Unclonable Functions (PUFs) to provide a dual-layered and decentralized approach to authentication. Biometrics offer a non-transferable, user-specific identity marker, leveraging physical or behavioral characteristics like fingerprints, facial patterns, or voice recognition. These traits are difficult to replicate and provide a seamless user experience without the need for memorized credentials. However, biometric systems alone may be vulnerable if raw data is compromised. To overcome this, the proposed framework does not store biometric data in its original form. Instead, it uses biometric feature extraction combined with homomorphic encryption or secure sketch techniques to ensure that biometric data remains private and is never directly transmitted or stored [3].

Complementing the biometric layer, PUFs provide hardware-level security. Each PUF generates a unique and repeatable response to a given input challenge based on intrinsic manufacturing differences in microelectronic components. These differences are practically impossible to clone, even by the manufacturer, making each device uniquely identifiable. In the proposed authentication scheme, when a device is first enrolled, a set of challenge-response pairs is securely stored in a tamper-resistant server. During authentication, the device is sent a challenge; it uses its PUF to generate a response, which is verified against the stored data. This process confirms the physical authenticity of the device without relying on stored cryptographic keys, which are vulnerable to theft or compromise. To preserve end-to-end privacy and security, the framework incorporates additional cryptographic measures such as zero-knowledge proofs, lightweight symmetric encryption, and Hash-Based Message Authentication Codes (HMACs). These tools ensure that even in the event of intercepted communications, no meaningful information can be extracted or reverse-engineered. Moreover, the system architecture is designed to be scalable and energy-efficient, making it ideal for constrained IoT devices with limited processing power and memory [4].

The integration of PUFs and biometrics in smart city contexts facilitates multiple critical applications. For instance, in smart healthcare, patients can be authenticated to access their medical records through biometric inputs, while the PUF ensures the medical device in use is legitimate and untampered. In public safety, citywide cameras and sensors can use PUF-based authentication to confirm the legitimacy of incoming data streams, while law enforcement agents access these systems via biometric credentials. In smart transportation systems, biometric-PUF combinations can ensure that only verified drivers operate autonomous or semi-autonomous vehicles and that real-time vehicle data originates from genuine, authenticated sources. Furthermore, the framework supports decentralized identity management, potentially through integration with blockchain or Distributed Ledger Technologies (DLT), allowing for transparent and tamper-proof auditing of authentication events without relying on a single authority. This significantly reduces the risks of identity theft, unauthorized access, and data spoofing critical concerns in urban infrastructures dealing with sensitive citizen and city data [5].

***Address for Correspondence:** David Daniel, Department of Biometry and Data Management, University of Zurich, Zurich, Switzerland, E-mail: david@daniel.ce*

Received: 01 February, 2025, Manuscript No. jbmbs-25-166971; **Editor assigned:** 03 February, 2025, Pre QC No. P-166971; **Reviewed:** 15 February, 2025, QC No. Q-166971; **Revised:** 20 February, 2025, Manuscript No. R-166971; **Published:** 27 February, 2025, DOI: 10.37421/2155-6180.2025.16.251

Conclusion

The integration of biometric authentication with PUF technology presents a powerful solution to the complex security challenges facing IoT-enabled smart cities. This dual-authentication framework ensures not only that users are who they claim to be but also that the devices they use are trustworthy and unique. By minimizing reliance on passwords and central databases, and by dynamically generating device-specific credentials, the system enhances both privacy and security. As smart city ecosystems continue to expand, implementing such privacy-preserving authentication mechanisms will be crucial for protecting sensitive data, ensuring public trust, and enabling the seamless operation of interconnected urban infrastructure.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Anderson, Jeffrey. "An ensemble adjustment Kalman filter for data assimilation." *Mon Wea Rev* 129 (2001): 2884–2898.
2. Andersson, Erik, John Haseler, Peter Undén and Courtier, Claude, et al. "The ECMWF implementation of three-dimensional variational assimilation (3D-Var). III: Experimental results." *Q J R Meteorol Soc* 124 (1998): 1831–1860
3. Andrews, Alan. "A square root formulation of the Kalman covariance equations." *AIAA J* 6 (1968): 1165–1169.
4. Beck, Alexander and Michael Ehrendorfer. "Singular-vector-based covariance propagation in a quasi-geostrophic assimilation system." *Mon Wea Rev* 133 (2005): 1295–1310.
5. Zupanski, Milija. "Maximum likelihood ensemble filter: Theoretical aspects." *Mon Wea Rev* 133 (2005): 1710–1726.

How to cite this article: Daniel, David. “A Biometric and PUF-based Privacy Framework for Integration of Internet of Things in Smart Cities.” *J Biom Biosta* 16 (2025): 251.