Secure Authentication Solution for Cloud-based Smart City Surveillance System

Yosra Ben Dhief, Yacine Djemaiel, Slim Rekhis and Noureddine Boudriga
Communication Networks and Security Research Lab, University of Carthage, Tunisia

Keywords: Smart City, Physical Unclonable Functions, Sensor Authentication, Cloud, Virtual Sensor.

Abstract: With the emergence of physical monitoring systems and their use for smart cities, new security concerns arise due to the sensitive nature of the data produced by the sensor devices of these systems, which makes the smart city applications a prime target for cyber attacks. However, securing these devices is very challenging given the fact that they are resource-constrained, and deployed in physically unsecured environments. In this paper, we propose a secure scheme for cloud-based smart city surveillance system providing a lightweight sensor authentication protocol based on Physical Unclonable Functions and securing the exchanged data through the different components of this infrastructure.

1 INTRODUCTION

With the emergence of smart cities over the world, there is a great need for services that ensure the protection of citizens and cities' assets. In fact, these services run in a dynamic environment containing sets of physical supervisory systems, which in turn can be managed by different providers to serve several actors. However, the inherent complexities of such environments raise several challenges for the implementation of smart city applications. These challenges are mostly caused by the massive amount of data that are generated by the sensors. The cloud technology presents an attractive solution to face this challenge since it provides powerful computing resources and elastic storage capacities (Schleicher, et al., 2016).

Despite the benefits of the cloud, the smart city applications are still suffering from security threats given the fact that the sensitive nature of sensor data makes them a prime target for cyber attacks. Therefore, implementing security solutions is very crucial to ensure efficient and reliable services for smart cities. In particular, authentication and encryption services are required to provide both device and data exchange security. However, the sensor devices are endowed with limited processing, memory, and energy resources which make them unable to support complex security mechanisms (Wallrabenstein, 2016). In this context, several works considered Elliptic Curve Cryptography (ECC) as an effective solution for resource-constrained devices that requires lower computational and storage capabilities. In (Kalra & Sood, 2015), the authors presented an ECC based mutual authentication protocol for secure communication between embedded devices and cloud servers. In (Hu, et al., 2017), the authors proposed a secure cloud-based architecture for health monitoring using IoT devices which achieves authentication and data security using ECC digital signature.

However, the aforecited schemes call for the storage of the secret key inside the Non-Volatile Memory (NVM) of devices, while the sensors can be deployed in a hostile environment and be the target of many physical attacks. To thwart these attacks, the sensor devices can be equipped with tamper resistant hardware. However, theses solutions can be too expensive to be practical in many smart city applications. Several researches were proposed (Lao, et al., 2017), (Wallrabenstein, 2015), (Aman, et al., 2017) and (Wallrabenstein, 2016) focusing on the use of a low-cost solutions to protect sensor devices from tampering. These solutions are based on the use of a Physical Unclonable Function (PUF) which consists in an on-demand extraction of secrets from complex properties of hardware, rather than storing them in a NVM. In fact, a PUF produces to a given input (or challenge) an output (or response) which is unique due to inter-chip variation that is difficult or impossible to model. The challenge and response

Dhief, Y., Djemaiel, Y., Rekhis, S. and Boudriga, N.
Secure Authentication Solution for Cloud-based Smart City Surveillance System.
DOI: 10.5220/0006867005020507
In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT*, pages 502-507
ISBN: 978-989-758-319-3

pairs (CRPs) of a PUF are used to generate chip-unique signatures for an authentication system (Lao, et al., 2017).

In this work, we propose a security scheme for cloud-based smart city surveillance architecture leveraging an extension of the PUF-based authentication system proposed in (Wallrabenstein, 2016). The architecture was presented by our work in (Yosra, et al., 2018) that provides global monitoring services (GMS) for smart cities built on virtual sensors (vs), which are created by different brokers. A vs provides an indirect measurements by processing data collected by physical sensors (ps) deployed by different physical supervisory systems ($PSSs$). The main goal of this paper is to design a lightweight scheme involving more than two actors (i.e., sensor devices, broker and provider) to perform secure authentication and key management for sensors in cloud-based environment, in addition to guaranteeing sensors' anonymity. The proposal exploits, firstly, the ECC to enable the sensor device to generate pair of asymmetric key and the PUF hardware to secure the private key from tampering, and then the Zero knowledge Proof (ZKP) to prove the authenticity of the generated public key. The generated asymmetric keys are used to encrypt and sign the exchanged data.

The main contribution of this paper is four fold: 1) A lightweight authentication scheme for sensor devices that preserves their anonymity in cloud environment; 2) A low cost tamper resistance solution for sensor devices based on the use of unclonable function; 3) The proof of the real involvement of sensors in data collection; and 4) The integrity and confidentiality of the exchanged data in a cloud sensor based architecture.

The remaining part of the paper is organized as follows. Section 2 discusses the security requirements for cloud-based smart city surveillance system. Section 3 details the proposed architecture and the functions ensured by its components. Section 4 presents our proposed authentication and key distribution scheme. The next section provides a security analysis and validation of the proposed scheme. Section 6 concludes the paper.

2 SECURITY REQUREMENTS FOR CLOUD-BASED SMART CITY SURVEILLANCE

In this section, we detail the security requirement to design sensor authentication scheme in cloud-based smart city surveillance system.

Anonymous Sensor Authentication. The virtualization enables GMS to make use of different ps without knowing their identity. However, it is required to prove that the used data are collected by a trusted sensor. Thus, sensor devices should be authenticated anonymously.

Low Computational and Energy Operation. The computation power and the battery capacity of sensor are limited and may be insufficient for the processing of security algorithms. Therefore, a security scheme for sensor devices should involve low resource and energy consumption.

Tamper Resistance. Given the fact that the sensor devices can be deployed in remote unattended places, security solution should be able to detect any attempt to tamper with them.

Freshness and Integrity of Sensing Data. The surveillance applications requires firstly, the freshness of the used data to guarantee that it is very much recent and no old data have been replayed. Secondly, the integrity of the used data to guarantee that it has not been altered in transit.

3 CLOUD-BASED SMART CITY SURVEILLANCE SYSTEM ARHITECTURE

The proposed cloud-based smart city surveillance architecture is composed of three actors: i) Physical Supervisory System (PSS) /provider ii) A broker of vs and iii) A Logical Supervisory System (LSS). An architectural map of the proposed architecture is shown in Figure 1. In the following we detail the role of each actor.

Physical Supervisory System / Provider

A typical PSS is a centralized system that ensures real-time monitoring of an infrastructure process using a set of heterogeneous sensors. The PSS acts as a provider that allows the reuse of its ps by different external systems with different configurations. It also interacts with a trusted Authentication System (AS) to enroll and to authenticate its ps. The AS is composed of enrollment servers that ensure the authentication of PSS and the generation of shared keys to be used to secure the data exchange.

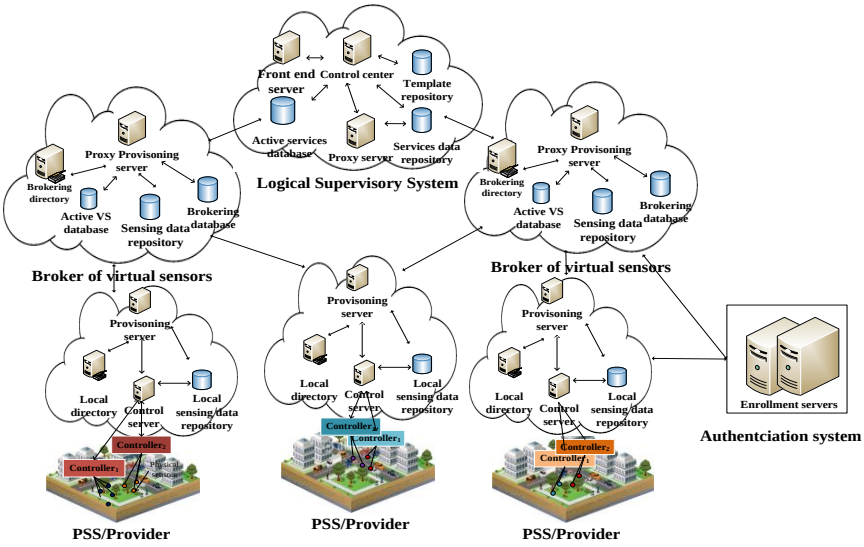

Figure 1: Cloud-based smart city surveillance architecture.

Broker of Virtual Sensors

The broker of vs is the intermediary between the PSS/providers and the LSS. According to the request of LSS, the broker selects providers to use their ps with the appropriate configurations. It creates a vs enabling the processing of the data generated by the selected ps. The broker also maintains an archive of the sensed data collected from the different PSSs.

Logical Supervisory System

The LSS provides GMSs for heterogeneous and distributed infrastructures making the use of vs provided by different brokers of vs. The supervision ensured by this GMS is based on the analysis and the processing of data produced by a set of vs.

4 SECURE DATA EXCHANGE IN CLOUD-BASED SMART CITY SYSTEM

This section describes the proposed PUF-based authentication and key distribution scheme for cloud-based smart city surveillance, in addition to an overview about the PUFs concept.

4.1 Physical Unclonable Function Overview

The PUF performs a mapping from a challenge to a unique response which depends on the unique characteristics of the physical hardware on which it is executed. Several authentication schemes have been proposed based on the PUF (Aman, et al., 2017). They use the fact that only a user and a sensor device know a CRP. To authenticate a sensor, the user has to tell the device in clear his challenge so that it can get the response. Thus a man in the middle can hear the challenge, get the response from the PUF device and use it to spoof the PUF device. The Controlled PUF (Dijk, et al., 2008) (CPUF), which is a combination of a PUF and an Integrated Circuit (IC) bound together such that an attacker has no access to the communication between the PUF and the IC. Any attempt to force them apart will damage the PUF. The IC completely governs the PUF input and output and reveals only indirect information derived from the output.

4.2 PUF-based Authentication and Key Distribution Scheme

The proposed scheme is based on ECC which is a suitable solution for resource-constrained sensors. We define an elliptic curve E over a field F_p of prime order p, and a base point G of order q, where $p = 2q + 1$. The proposed scheme is also based on a CPUF implemented by the used sensor devices and a hash function denoted by H. We assume that the ES is a trusted entity that authenticates the actors of

our architecture and that generates the secret keys to be used during the data exchange. In addition, each provider has a pair of keys (k_{pub}, k_{priv}) generated by the ES and to be used during the exchange of data with sensors.

4.2.1 Enrollment Phase

This phase is executed in a secure environment by the AS. The sensors are pre-configured with a virtual identity idv_{dev}. Once the enrollment phase is finished, the device deletes idv_{dev} from its memory. Figure 2 shows the steps of this phase, which are detailed in the following:

1. The ES generates a Pre-challenge C_{pre} and sends $H(C_{pre})$ to the sensor device.
2. The sensor selects rand from F_p and calculates a challenge $C = rand \oplus H(C_{pre})$ and $n = H(C, E, G, p, q)$ which is used as input to the PUF to generate the response R. Next, it generates a public key $A = r.G \bmod p$, where the private key r is selected from F_p. It applies an Error Correction Code (ECC) over the private key, and blinds this value with R, in a way that the final helper value $P = R \oplus ECC(r)$ leaks no information about the private key. The device stores C and P in the NVM, and sends to the ES the public key A, the rand and its idv_{dev}.
3. The ES saves the public key A and rand with the correspondent idv_{dev} and the identity of its provider id_p.

4.2.2 Sensor Authentication Phase

The device authentication is performed through a ZKP protocol. In this phase, the ES verifies whether the sensor can re-generate the private key involving its PUF. Figure 3 shows the steps of this phase, which are detailed in the following:

1. The ES recovers the relevant public key A, C_{pre} and $rand$ using idv_{dev}. It generates a nonce N and r_1 and calculates $H(C_{pre})$ and $Q = H(N|\, r_1 |\, H(C_{pre}) \,| rand)$. Next, the ES encrypts r_1, idv_{dev}, N, $rand$ and Q using a secret key K_{Ep}, which is shared between the ES and the provider that owns the sensor device.
2. The PSS decrypts the received message with K_{EP} and transfers to the relevant device r_1, N, $rand$ and Q.
3. The device reads from its memory C and P. It calculates $H(C_{pre}) = C \oplus rand$ and verifies the received Q. This enables the sensor device to authenticate the ES, given that it is the only entity that knows the C_{pre} and $rand$. Then, the device calculates $n = H(C, E, G, p, q)$ and gets its correspondent response R from its PUF. It re-generates its private key r using an error decoding, $r = D(P \oplus R)$. It also calculates its public key $A = r.G \bmod p$.

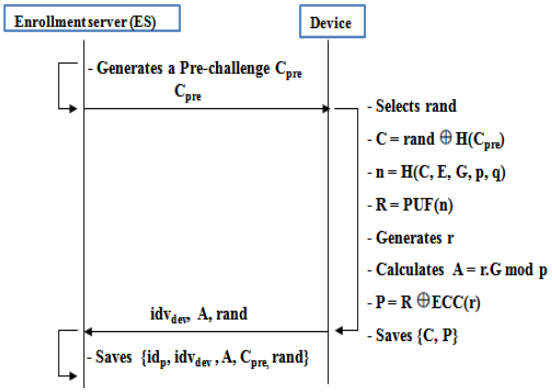

Figure 2: Enrollment phase.

4. After re-generating the asymmetric key pair, the device selects x from F_q and calculates $y = x.G \bmod p$. Then, It calculates $c' = H(G, A, t, N)$ and $z = y + c'.r \bmod q$. It also calculates $Q_1 = H(y|z|N\,|H(C_{pre}))$ and generates r_2. Finally, it sends r_2, Q_1, y, z to the PSS/Provider.
5. The PSS adds its identity id_P and the idv_{dev} to the received message and encrypts them with K_{EP}. It adds to the encrypted message in clear its id_P and sends them to the ES.
6. Using id_P, the ES retrieves K_{EP} and decrypts the message. Then, it verifies Q_1 and calculates $c" = H(G, A, y, N)$ and $y' = z.G - c".A \bmod p$. The ES compares y and y'. If they are equal, it sends an acknowledge to the provider. Else, it refuses to authenticate the device.

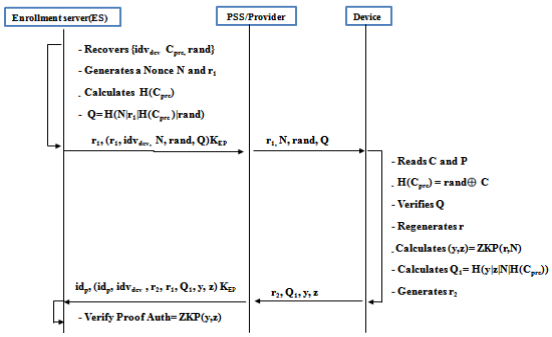

Figure 3: Device authentication phase.

Once a sensor is authenticated, the parameters used for sensor authentication can be renewed.

4.2.3 Data Transfer Phase

The data collected by a sensor are transferred to the broker without revealing the sensor identity. However, the broker should make sure that the received data are collected from an involved and an authentic sensor. To this end, we proposed a protocol that enables a broker to authenticate a sensor through a digital signature without revealing its identity. The sensor signs data with its private key r that it re-generates using its PUF. In the other hand, the broker verifies the sensor's signature using a public key A provided by the ES. The validity of the key pair (A, r) is verified by the ES through the sensor authentication described above.

The proposed signature protocol is based on the ElGamal digital signature algorithm described by (Wallrabenstein, 2016). Figure 4 shows the steps of this phase, which are detailed in the following:

1. The device reads from its memory C and P and re-generates its private key r and public A as described at step 3 in the authentication phase. It selects a random curve point from F_p $k = \{(G_x.k, G_y.k)\}$. Next, it sets $R = (k)_x = G_x.k$ where $(k)_x$ denotes the $x-$coordinate of the point k. It also sets $S = k^{-1}(Hash\,(data|SeqN°) + R.r)$ where $SeqN°$ is a sequence number which is initially synchronized between the broker and the device. The device creates the message M_4 starting from R, S and data. It encypts the message M_4 and a random value r_1 using the public key k_{pub} of the provider. It adds to the encrypted message r_1 in clear and sends them to its provider.

2. The provider decrypts the message its k_{priv} and adds $ReqN°$ and its identity id_p to the decrypted message. Then, it encrypts them with the secret key K_{PB} shared with the concerned broker. It also adds in clear its identity id_p. Finally, it sends them to the broker.

3. Using id_p, it selects the appropriate K_{PB} and decrypts the message. Then, it retrieves the public key A using idv_{dev} and verifies the signature by calculating $R = G.H(data|SeqN°).S^{-1} + z^{-1}$.

5 SECURITY ANALYSIS AND SYSTEM VALIDATION

In this section, we will analyze and validate the robustness of the proposed scheme against a set of attacks.

- **Low Cost Tamper Resistant.** The device uses C and P with its PUF to regenerate its private key r instead of stored it in the NVM. Hence, r is physically obfuscated and only exists in memory when needed for a cryptographic operation. Besides, we use a CPUF that makes an inseparable link between an IC and a PUF's input-output mapping, an attacker that attempts to probe the circuit will irreversibly modify the physical variations in the IC, which in turn changes the PUF mapping and prevents regeneration of the private key. Thus, PUF circuits are a low-cost solution for tamper resistance to resource-constrained devices.

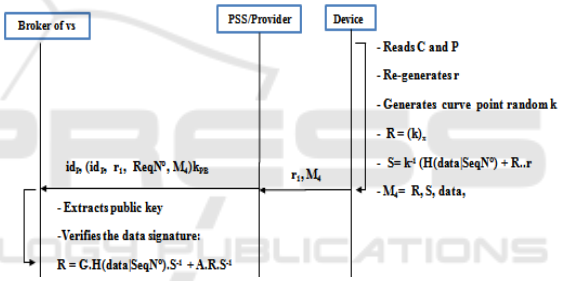

Figure 4: PUF-based signature protocol.

- **Sensor Anonymous Authentication.** The broker authenticates a sensor device through the verification of its signature using the public key A sent by the ES. A is generated based on a private key r which is only known by the sensor device given that the regeneration of r requires the involvement of its unique function PUF. Based on this fact, the ES authenticates the sensor using ZKP protocol. Besides, the sensor device is identified by a virtual identity idv_{dev} which is only known by the provider and the enrollment server. Thus, the broker authenticates the sensor device without knowing its identity and its physical specifications.

- **Resistance to Replay Attack.** An attacker can replay previous messages exchanged by the sensor device to the broker. But, the broker can detect the invalidity of the message because messages are signed using the private key r that

can be generated only by the sensor using its PUF and contain new sequence number generated for new message. Besides, to prevent replay attacks on the message exchanged between actors, new nonces are generated to guarantee the freshness of each session.

- **Resistance to Impersonation Attack.** The proposed scheme implements ZKP protocol to authenticate a sensor device which allows the ES to verify that the sensor knows the private key r without disclosing it. A sensor can prove that it knows the correct r by re-generating it involving its implemented PUF. Given that the PUF is unique for each device, an adversary cannot re-generate r to impersonate the S .

- **Resistance to Man In the Middle Attack.** an attacker cannot perform a MITM attack in the communication between the ES and a sensor because at each time each one checks that the other knows the $rand$ and the $Pre-challenge$ used to generate the challenge C saved by the sensor. An attacker is not also able to decrypt several messages because they are encrypted by a secret key already calculated by the ES. On top of that, our scheme is based on CPUF which prevents an attacker, even though he determined the challenge saved by the sensor, to probe the device and get the response.

6 CONCLUSION

We proposed in this paper a secure authentication scheme for cloud-based smart city surveillance system. The proposal solution exploits, firstly, ECC to enable the sensor device to generate a pair of asymmetric key and the PUF hardware to secure the private key from tampering, and then ZKP to prove the authenticity of the generated public key. Moreover, the generated asymmetric keys are leveraged to provide encryption and signature mechanism to protect exchanged data with sensors while coping with their resources-limitations. In addition, our proposed solution enables to authenticate anonymously a sensor in the cloud environment. In a future work, we will extend our proposed scheme to support the authentication of virtual sensors created starting from a dynamic set of mobile and heterogeneous sensor devices.

REFERENCES

Aman, M. N., Chua, K. C. & Sikdar, B., 2017. *Secure Data Provenance for the Internet of Things.* In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, IoTPTS'17, pp. 11-14, Abu Dhabi, United Arab Emirates.

Dijk, B. G. a. M. V. et al., 2008. Controlled Physical Random Functions and Applications. *ACM Transactions on Information and System Security (TISSEC),* 10(4), pp. 3:1--3:22.

Dijk, B. G. a. M. V. et al., 2008. Controlled Physical Random Functions and Applications. *ACM Transactions on Information and System Security (TISSEC),* 10(4).

Hofer, C. B. a. M., 2012. *Physical Unclonable Functions in Theory and Practice.* 1 ed. New York, USA: Springer Publishing Company.

Hu, J.-X., Chen, C.-L., Fan, C.-L. & Wang, K.-h., 2017. An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing. *Sensors,* Volume 2017, p. 11.

Kalra, S. & Sood, S. K., 2015. Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile Computing,* 24(C), pp. 210 - 223.

Lao, Y., Yuan, B., Kim, C. H. & Parhi, K. K., 2017. Reliable PUF-Based Local Authentication With Self-Correction. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 36(2), pp. 201-213.

Schleicher, M. V. a. J. M., Inzinger, C., Dustdar, S. & Ranjan, R., 2016. Migrating Smart City Applications to the Cloud. *IEEE Cloud Computing,* 3(2), pp. 72-79.

Suárez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P. & Castedo, L., 2017. A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications. *Sensors,* 17(9).

Wallrabenstein, J. R., 2015. *Implementing Authentication Systems Based on Physical Unclonable Functions.* In Proceedings of the 14th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, TrustCom-15, pp. 790-796, Helsinki, Finland.

Wallrabenstein, J. R., 2016. *Practical and Secure IoT Device Authentication Using Physical Unclonable Functions.* In Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016), pp. 99-106, Vienna, Austria.

Yosra, B. D., Yacine, D., Slim, R. & Noureddine, B., 2018. *Cloud-based Global Monitoring System for Smart Cities.* In Proccedings of the 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2018, Cracow, Poland.