Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts

Salvador Pérez[1(✉)], Domenico Rotondi[2], Diego Pedone[2], Leonardo Straniero[2], María José Núñez[3], and Fernando Gigante[3]

[1] Department of Information and Communication Engineering, Computer Science Faculty, University of Murcia, Murcia, Spain
salvador.p.f@um.es
[2] FINCONS SpA, Bari, Italy
{domenico.rotondi,diego.pedone,leonardo.straniero}@finconsgroup.com
[3] AIDIMME, Valencia, Spain
{mjnunez,fgigante}@aidimme.es

Abstract. The increasing relevance of IoT in our daily life, such as healthcare and home automation, raises new concerns regarding how confidential and sensitive information is managed and privacy is assured. In this paper, we present a solution that takes into account and addresses these issues to foster adoption on IoT technologies and services by end users. We propose a novel architecture combining the flexibility and expressiveness of CP-ABE and the efficiency of symmetric key encryption techniques, with the purpose of carrying out secure data exchanges and preserving the participating entities privacy.

Keywords: Security · Privacy · Secure data exchange · Attribute-based encryption · Symmetric key encryption · CP-ABE · AES

1 Introduction

IoT and Big Data [16] are heavily impacting our lives, our environments and social habits. Lots of personal, even sensitive, data is being acquired by "sensors" (e.g., our smartphones, home appliances, wellness and health devices) and processed locally or remotely on the cloud. In this scenario, new rules and technologies are required to assure privacy would not be inappropriately affected. To this end regulatory entities [14] has provided indications on how to address IoT related privacy issues, and new normative, like the new EU GDPR[1], is being promulgated. On the technical side, the guiding principle in designing new functionalities and systems is compliance with the principles of Security/Privacy by Design, and Security/Privacy by Default, which, by the way, are recommended

[1] http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

L. Barolli and T. Enokido (eds.), *Innovative Mobile and Internet Services in Ubiquitous Computing*, Advances in Intelligent Systems and Computing 612,
DOI 10.1007/978-3-319-61542-4_93

by [14]. By-design implies to take security and/or privacy into account since the design phase of the system, while the by-default implies to use default values or configurations that assure the highest security or privacy level for the context at hand. Additionally, there is a convergence of regulation and technical approaches on protecting the full data lifecycle to preserve privacy or confidential information.

Given the dynamic and distributed nature of the IoT [13], more flexible data exchange proposals should be considered to cope with those novel contexts in which the information can be shared with a set of unknown data consumers. Starting out from this premise, the incorporation of mechanisms to guarantee that such sharing is performed securely, thus preserving the data privacy, has been raised as one of the main challenges that is being addressed by various researches within the academic and industrial area for different IoT contexts.

Following this line, full lifecycle data protection has been assured using traditional cryptographic solutions, such as *Symmetric Key Cryptography* (SKC) [8]. However, the application of this scheme is not the most suitable for contexts in which data are shared among a set of entities, due to well-known drawbacks related to the key management, distribution and revocation. In this direction, a novel cryptographic approach, known as *Attribute Based Encryption* (ABE) [5], allows encrypting the shared data by user-defined access policies that define the conditions a subject has to satisfy for succeeding in decrypting the information. In ABE systems, each subject has a personal key that is generated from its set of attributes (e.g. its role). The decryption process will be successful only if its attributes are in line with the rules in the access policy. Due to the ABE processing needs, a pure ABE approach is not suitable for IoT environments in which data are generated at a high rate or by devices with resource constraints. This work proposes a new approach for privacy-preserving data sharing that combines attribute-based cryptography, and more specifically CP-ABE [4], along with symmetric key cryptography, thus obtaining the flexibility and expressiveness of the first one and the efficiency of the second one.

The remainder of this paper is structured as follows: Sect. 2 summarizes works addressing the main challenges for privacy-preserving secure data exchanges among entities in different IoT contexts. In Sect. 3, we provide an overview of our proposed architecture, as well as the main interactions between the entities to achieve a secure data sharing while privacy is preserved. Section 4 describes a use case for which our architecture has been designed. Finally, Sect. 5 includes the conclusions of this paper and introduces some lines for future work in this area.

2 Related Work

Nowadays, IoT scenarios are intended to exchange sensitive or personal data through a central platform, such as [9], so any information leakage could violate the privacy of the participating entities. To address this issue, these scenarios use Attribute-Based Encryption (ABE), specifically CP-ABE, in order to provide privacy-preserving secure data exchange. Thus, data sources entities do not

reveal any private or confidential information, and such data will only be recovered by entities meeting the CP-ABE access policy used to encrypt them. On this line, [3] introduces an IoT security framework as an IoT Architecture Reference Model extension in order to provide privacy-preserving data exchanges. However, these papers do not consider the existence of resource-constrained devices or data sources with high data rates. Indeed, such devices have limitations in terms of processing or memory [18] to support the CP-ABE. In [1], an ABE library implementation and its application on current smartphones is presented, demonstrating that a suitable performance can be achieved in these devices. However, it is necessary to look for solutions that can be suitable for a wider set of contexts (e.g. high data rate, more constrained devices). [19] combines CP-ABE with symmetric key cryptographic to allow the secure data sharing through different kinds of repositories (private clouds, brokers, databases, etc.). In this hybrid model, data are encrypted using AES and the corresponding symmetric key is protected by the CP-ABE scheme. Nevertheless, this solution does not provide a high performance of CP-ABE operations, so that other proposals, as [17], introduce a cooperative scheme in which the expensive CP-ABE operations are delegated and performed by a set of unconstrained devices (assisting nodes), assuming that these are trusted. Thus, data are sent from a resource-constrained device to more powerful devices which encrypt them using CP-ABE. The result is returned to the originating device or is forwarded to a central platform for its sharing. The main issue of this approach is that data could be disclosed to unauthorized entities if some of the assisting nodes have been compromised. Moreover, in [11] a CP-ABE schema is proposed to obtain both constant-size ciphertexts and private keys, thus improving the usability of such scheme in resource-constrained devices. However, it is applicable only to IoT scenarios that do not require a high expressivity in access policies.

The previously mentioned investigations address different relevant issues related to the exchange of confidential or sensitive information between a wide set of heterogeneous entities, while trying to preserve their privacy. Anyway, they do not sufficiently take into account devices with resource limitations and high data generation rate, such as sensors, actuators or gateway. These works have been the basis for the proposal presented in this paper, combining both symmetric cryptography and attribute-based cryptography.

3 Our Proposed Architecture

Our architecture integrates different protocols and security mechanisms to secure data exchange that preserve privacy. Figure 1 provides a high-level view of our proposal, where the CP-ABE has been selected to protect the shared information. Thus, to solve CP-ABE issues related to speed and resource requirements, we combine the CP-ABE and AES symmetric encryption schemes. Indeed, data sources encrypt the information they provide by using AES with symmetric keys, which in turn are CP-ABE encrypted by using data owner's provided access policies. To retrieve such encrypted data, a consumer entity has to recover first the

symmetric key using the CP-ABE algorithm and its CP-ABE private key and, only in case such CP-ABE key meets the access policy specified by the data owner, the obtained symmetric key will be successful in decrypting the AES encrypted data.

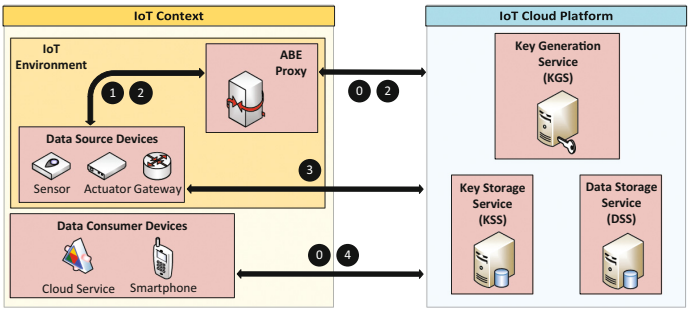

Fig. 1. Overview of our proposed architecture

As depicted in Fig. 1, the *data sources* do not directly use CP-ABE but delegate to the *ABE proxy* the execution of CP-ABE hard encryption operations. In addition, our approach takes into account other functionalities which are provided by the *IoT Cloud Platform* in order to support both the storage/retrieval of the protected data and the management of the encrypted symmetric keys. One of this is the *Key Generation Service* (KGS) that is responsible for generating CP-ABE private keys based on attributes associated with *data consumers* (e.g. to their profiles). Additionally, it provides the necessary information (i.e. the public parameters of CP-ABE approach) to the *ABE proxy* so that it can perform ABE encryption operations. Other provided functionality is the *Key Storage Service* (KSS) which stores the CP-ABE encrypted symmetric keys, in such a way that these keys can be acquired by any *data consumer*. Finally, the *Data Storage Service* (DSS) stores AES encrypted data as they are delivered by the *data sources*. Actually, the KSS and DSS represent functionalities in our architecture that can be provided by a variety of different services (e.g. DBs, publish/subscribe systems).

Following this line, our architecture envisages four phases for the privacy-preserving and secure information exchange among data sources and data consumers. Actually, a preliminary phase (**phase 0**) is assumed as necessary in which the ABE Proxy and the data consumers communicate with the KGS to acquire both the CP-ABE public parameters and their CP-ABE private keys.

Phase 1. Setup the shared symmetric key among the data source and the ABE proxy

Once the **phase 0** has been performed, the first phase can begin (Fig. 1 - ①) when a data source needs to publish data to the IoT Cloud Platform. The **phase 1** is focused on the agreement of a symmetric key among the data

source and the ABE Proxy. Firstly, both the data source and the ABE Proxy generate their ephemeral elliptic curve keys pairs using the NIST P-256 curve (secp256r1) with a key size of 256-bits, although other key sizes can be chosen (P-384, P-521). Afterwards, these entities exchange their corresponding ephemeral public keys as well as the selected ECC curve to each other according to the formats specified in *Json Web Algorithms* [6] and *Json Web Key* [7]. Subsequently, the entities execute the Elliptic Curve Diffie-Hellman Ephemeral Static [10], in combination with the Concat Key-Derivation Function [2] algorithms. Thus, at the end of this phase, the data source and the ABE Proxy have a freshly shared symmetric key.

Phase 2. Encrypt and store the shared symmetric key in the IoT cloud platform

The second phase (Fig. 1 - ②) focuses on protecting, via a data source provided CP-ABE access policy, the obtained shared symmetric key. Accordingly, the data source encrypts a set of information related to the CP-ABE access policy by the AES cryptographic algorithm using the shared symmetric key. Once the data source has protected this information, this entity sends it to the ABE Proxy in order to delegate the CP-ABE encryption operations. Such encrypted information is represented as a base64url-encoded string and it may be accompanied by a set of metadata like its encryption date or who encrypted it. The information elements are the following:

- *timestamp* indicates when the message was generated. This information is represented as UTC according to the ISO 8601.
- *device_ID* is a string which univocally identifies the data source.
- *policy* is used to provide details about the CP-ABE access policy to be used to encrypt the shared symmetric key. The CP-ABE policy can be directly specified within this data element or by indicating the information on how to retrieve it.
  - *specs* provides the CP-ABE access policy. It is represented as a tree data structure, where leaf nodes are the different attributes and intermediate nodes are the AND/OR logical operations.
  - *url* indicates the URL from which the CP-ABE attribute policy can be acquired. Note that the *specs* and *url* are mutually exclusive, i.e. only one of these should be in the message.
  - *metadata* are a set of attributes providing additional information of the CP-ABE access policy, such as its creation date, the version, a description, its author or the used CP-ABE library.
    - *name* identifies the attribute.
    - *value* contains the attribute value.
- *encrypted_symmetric_key_storages* is a data element used to specify where to store the CP-ABE encrypted shared symmetric key. It is an array that can provide different ways to store such key.
  - *type* indicates the storage type in which the encrypted shared symmetric key has to be saved. It can be a database, a pub/sub broker or a file system.

- *parameters* provides elements required by the storage type. For instance, if the *type* is a database, the parameters could be DB_connector, DB_name, table_name, etc.

When the ABE Proxy receives this information, it uses the shared symmetric key to decrypt it and it executes the CP-ABE encryption algorithm to protect such symmetric key using the obtained access policy. Furthermore, the ABE Proxy generates a unique key identifier associated with the shared symmetric key and stores both the encrypted key and its identifier in the corresponding KSS based on the storage parameters specified in the received information. Afterwards, the ABE Proxy will provide the symmetric key identifier, along with information related with the encryption process (e.g. the encryption date, who performed the encryption and the expiration date) to the data source. This identifier will complement the symmetrically encrypted data published by this source and will help data consumers in retrieving the protected key. As evident, any data element used to generate the symmetric key is removed after the shared key is generated.

Phase 3. Publish encrypted information in the IoT cloud platform

The third phase (Fig. 1 - ③) envisages the data source publishing encrypted data in the IoT cloud platform (exemplified by the DSS), using the AES algorithm and the generated symmetric key. Note that these AES encrypted data are complemented with the corresponding encrypted symmetric key identifier provided by the ABE Proxy in the previous phase.

Phase 4. Get encrypted information from the IoT cloud platform and recover it

Finally, in the fourth phase (Fig. 1 - ④), a data consumer capable to run the CP-ABE algorithm (e.g. smartphones or cloud services) acquires an encrypted data item and its encrypted symmetric key identifier from the DSS (e.g. by subscribing to the pub/sub service). Then, the consumer requests to the KSS the encrypted symmetric key associated with this identifier and it tries to decrypt it using its CP-ABE private key. Evidently, if its private key matches the access policy used in the shared symmetric key encryption process, the data consumer will be capable to acquire such symmetric key and, therefore, be able to recover the original data using the AES algorithm.

The different phases described above clearly show how our proposal overcome the concerns related to the CP-ABE use in data sources with resource constraints or high data rates thanks to the mix of CP-ABE and AES algorithms. More details on the overall architecture can be found in [12].

3.1 Security and Privacy Issues Related with Our Proposal

After this initial overview of our architecture, we now clarify some aspects of it. The generated AES symmetric keys must have a limited time-life with the purpose of defeating possible attacks, so that even if a symmetric key is acquired

by an attacker, it should only be able to retrieve the data items encrypted with that specific key. To this end, an expiration time is set for each symmetric key and when this time-life expires, it would be strongly recommended to renegotiate a new symmetric key among the data source and the ABE Proxy in order to guarantee that the communication will continue reliable and secure, and achieve the *Perfect Forward Secrecy*.

For a privacy perspective point of view, the CP-ABE algorithm offers a set of advantages over traditional data protection mechanisms:

- Access policies are explicit and formalized, so it easy demonstrating compliance to normative and laws.
- Access policies could be public so to make evident how a given information has been protected.
- Access policies govern the encryption process. Therefore, the same input data encrypted with different policies will generate different encrypted outcomes, therefore improving the resilience of the system to attacks or unauthorized access.
- There is no need to share private keys among entities. Each entity has its own CP-ABE key that will be able to decrypt the data if it meets the access policy used in the encryption process.

Furthermore, our proposed combination of CP-ABE and AES gives the following additional advantages regarding data privacy:

- The AES symmetric key generation (**phase 1**) is based on newly generated ephemeral elliptic curve keys pairs used within the ECDH protocol. Therefore, both the ECC keys pair of a data source and of the ABE Proxy will change every time our protocol is run, increasing the un-traceability of the encrypted data flow.
- The AES symmetric keys are temporary, so even if some of them would be compromised by an attacker, the privacy risk will be reduced.
- Entities accessing the encrypted data can be traced thanks to the requirement to use the entity's CP-ABE personal key and to the need to request a copy of the CP-ABE encrypted symmetric key to the KSS.

Finally, note that our design combines the flexibility, scalability and fine granularity provided by the CP-ABE cryptographic scheme with the efficiency of the AES symmetric one. Also, access to the encrypted data by authorized subjects is always guaranteed and the access constraints are always available and formalized by the provided CP-ABE access policies. Issues related to entities authentication, trust relationship and authorization are outside the scope of this paper and are addressed in other works, such as [15], that could be considered in the future to complete our design.

4 Use Case

The above architecture has been specifically conceived to address privacy issues in the H2020 PSYMBIOSYS project (see Acknowledgement), and specifically its

Furniture Industry use case[2]. PSYMBIOSYS addresses issues (named tussles in the project's documentation) related to the design and development of product-service goods. As part of this project, the *Furniture Industry* use case, led by AIDIMME, is focused on a Product-Service bundle about renovation of office environments. This scenario includes the monitoring of the office environment through the design of new smart furniture. Sensors are deployed in furniture (e.g. rooms to measure things like temperature, lighting or presence) with the aim to improve the quality of the working environment and of the worker's feeling.

The office furniture use case covers two main factors: the emotional and the physical ones. On the one hand, the emotional area is focused on the sentiment of the workers towards the furniture in use as well as the perception of the brand value in the offices. On the other hand, the physical factor is focused on the collection and analysis of two main kinds of parameters: ambience and ergonomics.

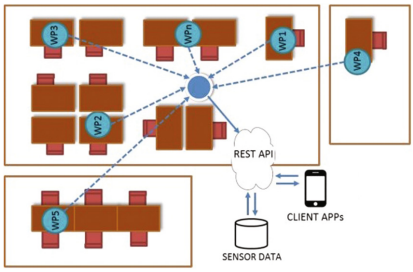

Fig. 2. Overview of the AIDIMME sensor system

As depicted in Fig. 2, sensors at each workplace are connected to microcontrollers sending data through the wireless xBee protocol to a central node that forwards them to a central server where these data are stored for subsequent analysis. The server also manages the notifications to workers about not recommended working conditions which are displayed in a client app workers use.

Ambience parameters are mainly those associated to the whole office environment such as temperature, humidity, luminosity and noise levels, while the ergonomics ones are taken from the seat at each workplace. The analysis of the ambient sensor values allows the detection of not recommended situations such as too high temperature or noise levels at the office. Moreover, ergonomics parameters are measured by using pressure sensors at the office chairs and detecting specific pressure distributions from the sensors. Some distributions are considered as wrong seating positions. Furthermore, other aspects such as long time seating at workplace are also monitored and detected.

Main objectives of this sensor system are the collection of data about the furniture use in order to improve it through the new interior decoration project, and

[2] http://www.psymbiosys.eu/furniture-industry/.

the availability of an alert system through which workers are notified regarding bad situations at the office. As stated, data from sensors are stored in an event database which also stores user notifications and profiles. Workers are enable to subscribe to personal notifications about not recommended situations at the office environment. User profiles contain sensitive anthropometric data about workers that should be carefully managed given their private nature. Also, data about worker's presence and seating habits is collected and stored in the system. Therefore, IoT data coming from the sensor at workplaces as well as database information are sensitive information from a privacy point of view that must be protected according to the Spanish and EU privacy laws. In this sense, the approach proposed in the previous sections aims at assuring compliance to these laws and to provide evidence to the involved people that their personal information is managed as required and agreed.

5 Conclusions and Future Work

The development of solutions addressing the security and privacy concerns during the full lifecycle of sensitive information, is a key challenge to achieve a full acceptance from end users, as well as to enable the large-scale services deployment in different IoT environments. In this sense, this work is based on different solutions that use the attribute-based cryptography to define a novel architecture, combining the efficiency of SKC and the flexibility and expressiveness of CP-ABE, to carry out privacy-preserving secure data exchanges. To this end, we have defined the main phases and interactions among the IoT entities of our architecture, considering the particularities of different everyday environments. In addition, we have provided details of a use case for which this proposal has been conceived. Future work focuses on assessing this mechanism in real contexts (like the AIDIMME use case) and refining and extending the architecture including authentication mechanisms.

Acknowledgments. The PSYMBIOSYS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 636804.

References

1. Ambrosin, M., Conti, M., Dargahi, T.: On the feasibility of attribute-based encryption on smartphone devices. In: Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, pp. 49–54. ACM (2015)
2. Barker, E., Chen, L., Roginsky, A., Smid, M.: Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. In: Technical Report; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2006, 2012. Citeseer (2006)
3. Bernabe, J.B., Hernández, J.L., Moreno, M.V., Gomez, A.F.S.: Privacy-preserving security framework for a social-aware internet of things. In: International Conference on Ubiquitous Computing and Ambient Intelligence, pp. 408–415. Springer (2014)

4. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, SP 2007, pp. 321–334. IEEE (2007)
5. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98. ACM (2006)
6. Jones: JSON Web Algorithms (JWA). RFC 7518, RFC Editor (2015)
7. Jones, M.: JSON Web Key (JWK). RFC 7517, RFC Editor (2015)
8. Kahate, A.: Cryptography and Network Security. Tata McGraw-Hill Education (2013)
9. Lounis, A., Hadjidj, A., Bouabdallah, A., Challal, Y.: Healing on the cloud: secure cloud architecture for medical wireless sensor networks. Fut. Gener. Comput. Syst. **55**, 266–277 (2016)
10. McGrew, D., Igoe, K., Salter, M.: Fundamental elliptic curve cryptography algorithms. RFC 6090, RFC Editor (2011)
11. Odelu, V., Das, A.K., Rao, Y.S., Kumari, S., Khan, M.K., Choo, K.K.R.: Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. Comput. Stan. Interfaces (2016)
12. Pérez Franco, S., Hérnandez-Ramos, J.L., Skarmeta, A.F., Pedone, D., Rotondi, D., Straniero, L.: A digital envelope approach using attribute-based encryption for secure data exchange in IoT scenarios. In: 2017 IEEE 1st Global Internet of Things Summit, GIoTS. IEEE (2017)
13. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comp. Netw. **57**(10), 2266–2279 (2013)
14. Ross, R., McEvilley, M., Oren, J.: Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. National Institute of Standards and Technology (2016)
15. Selander, G., Mattsson, J., Palombini, F.: Ephemeral Diffie-Hellman over cose (EDHOC). Internet-draft, IETF Secretariat (2016)
16. Tene, O., Polonetsky, J.: Big data for all: privacy and user control in the age of analytics. Nw. J. Tech. Intell. Prop. **11** (2012). xxvii
17. Touati, L., Challal, Y., Bouabdallah, A.: C-CP-ABE: cooperative ciphertext policy attribute-based encryption for the internet of things. In: 2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS), pp. 64–69. IEEE (2014)
18. Wang, X., Zhang, J., Schooler, E., Ion, M.: Performance evaluation of attribute-based encryption: toward data privacy in the IoT. In: 2014 IEEE International Conference on Communications (ICC), pp. 725–730. IEEE (2014)
19. Xiong, A., Xu, C.: Cloud storage access control scheme of ciphertext algorithm based on digital envelope. Intel. Autom. Soft Comput. **22**(2), 289–294 (2016)