# Using ABE for Medical Data Protection in Fog Computing

Abdelghani Krinah[1], Yacine Challal[2], Mawloud Omar[3] and Omar Nouali[1]
[1]*Computing Security Division, Cerist, Algiers, Algeria*
[2]*ESI, Algiers, Algeria*
[3]*Bejaia University, Bejaia, Algeria*

Keywords: Fog Computing, e-Health Applications, Data Confidentiality, Attribute based Encryption.

Abstract: Fog is an extension of the cloud computing paradigm, developed to fix the clouds latency, especially for applications requiring a very short response time, such as e-health applications. However, these applications also require a high level of data confidentiality, hence the need to apply appropriate encryption techniques, which can ensure security needs, while respecting the characteristics of the infrastructures devices. In this article, we will focus on ABE encryption, through the work done to study its applicability in the cloud and the Internet of things, as well as the improvements that can be made to adapt it to the fog computing environment.

## 1 INTRODUCTION

Fog Computing has been introduced to address the cloud architecture's latency issue by bringing the processing and storage units at the edge of the network, closer to end users where data is produced and consumed, especially in applications requiring a very short response time such as e-health applications. However, like any computer paradigm, it must meet certain requirements, especially in terms of security and confidentiality.

Among the promising techniques for data encryption, the attribute-based encryption (ABE) approach is an interesting solution, which has proved its effectiveness in various environments, such as Cloud computing (Ambrosin et al., 2016) (Moffat et al., 2017). The advantage of ABE is that we do not need to rely on the storage server to prevent unauthorized data access since the access policy is embedded into the encrypted text, or into the decryption key.

The integration of ABE into healthcare systems is a challenge. Many studies have been conducted on the feasibility of ABE on IoT devices, mobile devices or smartphones (Ambrosin et al., 2015) (Ambrosin et al., 2016). Our study aims to go further, by considering the effectiveness of ABE not only on separate devices, but in a Fog computing infrastructure, gathering multiple nodes with different characteristics, and achieving different tasks.

In this paper we first introduce the concepts of fog computing and ABE encryption. We then explore related works, by gathering them into 3 main topics; namely security in e-health, security in Fog and ABE in Fog. After that we present a discussion on previous works. We finish by a conclusion and perspectives.

## 2 BACKGROUNDS

**Fog Computing** is considered as an extension of the cloud computing paradigm from the core of network to the edge of network (Yi et al., 2015). It is a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing Data Centers, typically, but not exclusively located at the edge of network (Bonomi et al., 2012).

So the Fog is an infrastructure composed of nodes at the edge of the network, each node must be able to perform processing locally, and act as a router for its neighbors, to convey the information to the end user, or to a remote cloud server.

It is important to note that the Fog is not an alternative to the Cloud. In reality there is interoperability between the Fog and the Cloud. A typical Fog architecture consists of 3 levels: the IoT devices at the bottom, Cloud datacenters at the top and in the middle are the Fog nodes. While Fog nodes provide localization, allowing low latency and context awareness, the cloud provides global centralization. Many applications require both localization and real time processing of the Fog, as well as the globalization and



Krinah, A., Challal, Y., Omar, M. and Nouali, O.
Using ABE for Medical Data Protection in Fog Computing.
DOI: 10.5220/0007424601550161
In *Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS 2019)*, pages 155-161
ISBN: 978-989-758-372-8

the long-term storage of the Cloud, especially in the field of e-health, which perfectly illustrates the complementarity between the two technologies.

**Attribute-Based Encryption (ABE)** is a public key encryption scheme first introduced in 2005 by Sahai and Waters (Sahai and Waters, 2005). It is a class of control systems that extends identity-based encryption to allow expressive access policies and fine grained access to encrypted data. ABE uses attributes to define user access keys and policies. There are two main types of ABE systems: KP-ABE (Key-Policy ABE) and CP-ABE (Ciphertext-Policy ABE).

Because of its complexity and resourcefulness, the ABE scheme has left researchers skeptical about its implementation on small devices such as wireless sensors and RFID devices. Indeed, the Internet of Things interconnects devices with limited resources in terms of energy, storage and computing capacity. These limited devices are not capable of performing the heavy operations of ABE.

Nevertheless, and given the added value of ABE access control in IoT, many techniques and solutions are proposed to reduce the costs of ABE systems, such as compute offloading, compression, optimization of energy consumption. Etc.

# 3 RELATED WORKS

Several studies were conducted on the protection of confidentiality in the fog. We classified them in 3 categories.

## 3.1 Security in Fog

In order to identify the security issues in fog computing, we first relied on the recommendations of the OpenFog Consortium, founded by Intel, ARM, Princeton University, Dell, Cisco and Microsoft to accelerate fogs adoption, and define Fogs architecture requirements. Indeed, in (Martin et al., 2017) the OpenFog Consortium states that Information security and service trustworthiness have long been identified as the preeminent issues of our heavy dependency on the global information infrastructure, mainly in a Cloud/Fog/IoT environment. This is particularly important when the Fog Node was deployed in a hostile environment where it may be physically tampered. Once an entity has been registered with an OpenFog System, it must be provided with a cryptographically strong credential. A common technique is to use public-key ciphers to certify the digital identity of the entity. However, devices with limited resources may be incapable to perform strong authentication and access control; in those cases, these functions shall be delegated to their associated Fog Nodes as their proxies.

Meanwhile, using a well-known systematic literature review (SLR) approach, Dasgupta and Gill conducted a survey on Fog Computing Challenges (Dasgupta and Gill, 2017). They concluded that Fog inherits some of the problem of cloud computing with a number of studies (76 %) highlighting the lack of security in fog devices, making security the most important concern in Fog Computing.

As stated by Rani and Kumar (Rani and Kumar, 2015) the problem is even severe in mobile cloud computing because mobile devices often lack of computing power to execute sophisticated security algorithms. Moreover, it is difficult to enforce a standardized credential protection mechanism due to the variety of mobile devices (both IoT and Fog devices).

In the same perspective Petac et al (Petac and Petac, 2016) noticed that it may be difficult to protect the communication between Fog nodes and the IOT devices using encryption methods. This is due to the fact that encryption and decryption methods consume large amount of battery on mobile devices. So Petac proposed an Adoptive Fog Computing Node Security Profile (AFCNSP). The functional requirements that appear in this approach include the following security services: Authentication, Authorization and Accounting (AAA), Role and Rule Access Based Control, Symmetric and Asymmetric Encryption. All these rich features should be included in an improved security fog node.

Going from the principle that Cloud computing cannot apply the traditional access control models to achieve access control because of its characters, Sun et al (Sun et al., 2014) introduced Semantic access control (SAC) model, which considers semantic relations among different entities. It complements the use of attributes with the use of metadata to represent the semantics different elements. They assume that this solution provides an appropriate solution, especially for heterogeneous, distributed and large environments such as cloud computing, which can be applied to Fog computing as long as it has the same characteristics.

On the other hand, Koo and Hur (Koo and Hur, 2018) pointed out that in a fog computing environment, privacy issues surrounding outsourced data become more critical due to its complicated innards of the system. They proposed the first privacy-preserving deduplication protocol capable of efficient ownership management in fog computing. To obtain plausible and reliable experimental results, they made use of different kinds of equipment under differenti-

ated network conditions. They concluded that deduplication is able to utilize space efficiently by storing only a single copy of duplicate data and providing owners with a link to it.

Finally, with aim to find out and emphasize security related problems that arise with the employment of fog computing by IoT, Butun et al (Butun et al., 2019) underlined that a remedy is needed to enhance the privacy needs of the users in these services (IOT and Cloud) and fog computing is a strong candidate to provide this. Since early detection is important to stop ill effects of intrusions, they stated that fog computing would bring early detection opportunities to IDS algorithms working on IoT. In conclusion, they suggested that to improve privacy, a wiser solution would be keeping the private data on the edge while sending the just necessary data to the cloud.

In this section we presented a sample of studies and solutions related to security in Fog computing in general manner, regardless of the field of application. In what follows, we will focus more specifically on e-health applications at first, then on solutions involving the use of ABE, in Fog/Cloud computing environment.

## 3.2 Security in e-Health

Privacy concerns may impede, or at least slow down, the diffusion of new e-health services. Therefore it would be important to review the various security solutions in the field of healthcare.

Authors in (Rani and Kumar, 2015) proposed a scenario where the Home Node Base station (HNB) is connected to the cloud through a security gateway. To provide health data security in cloud, a user id and password are generated when for the first time the data are received from the user. The generated user id and password are sent to the user so that the user can access the data on cloud. The id of the healthcare centre which first accesses the data of the patient is attached to patient information stored in the cloud. As except the intended healthcare centre and the user no one can access the data. Privacy, authentication and integrity are guaranteed from the view point of both the user and the health center.

Following the principle of Keep it Simple and Secure Kaur and Mahajan (Kaur and Mahajan, 2015) presented a key management technique adaptable for the HMSNs by making it energy efficient, for the purpose of assuring both confidentiality and performance. Because these nodes (HMSN) are connected through wireless network with each other and base stations, they argued that it becomes a highly prone network to the hacking attacks. Moreover, cryptographic key distribution and management techniques usually consume larger amount of energy and put high computational overheads on Wireless Sensor Nodes. They concluded that the key verification policy must be quick, which is only possible using the small or mid length security keys.

Alshiky et al study (Alshiky et al., 2017) focused on Electronic Health Record, since EHR contains private and sensitive patient health information which is needed to be secured, without affecting the performance of fog nodes. Authors provided an Attribute Based Access Control ABAC into the EHR in fog to prevent unauthorized access, where different users are described based on their attributes, object (information and resources) attributes and environment conditions (time and location). In this scenario, each fog node which received requested action will analyze the attributes that are associated with the request. Then, based on these retrieved attributes and policies schema, the permission will be granted to user. Authenticated and authorized access into EHR is applied on request at the nearest fog instead of at the core of the network (cloud).

Dubey et al works (Dubey et al., 2015) (Dubey et al., 2017) were motivated by the fact that Heart diseases are one of the major chronic illness with a dramatic impact on productivity of affected individuals and related healthcare expenses. Hereby an ECG subsystem is considerably for more out-of-hospital applications. Moreover, such Telehealth application is a typical example of big data application that collects a large volume of data with a variety of information requiring real time and fast processing to provide the best healthcare. Therefore, they proposed Fog Data architecture , which main feature is its ability to carry out onsite data analytics to reduce the amount of data to be stored and transmitted to the cloud. They performed experiments on ECG signal containing 2160 samples (MIT-BIH Arrhythmia data), data reduction is carried using Dynamic time warping (DTW) and GNU zip compression. DTW reduces ECG data by more than 98% in most of the cases, and takes 1 second of processing time on Intel Edison Fog computer. Thus, authors concluded that Fog Data (also called Smart data) architecture is well suited for real-time ECG monitoring.

Because of urgent need to develop an effective health monitoring system, which can detect abnormalities of health conditions in time and make diagnoses according to the gleaned data, Deshpande and Kulkarni (Deshpande and Kulkarni, 2017) developed a new method for ECG monitoring based on Cypress Wireless Internet Connectivity for Embedded Devices (WICED) Internet of Things (IoT) platform. They no-

ticed that existing portable wireless ECG monitoring systems cannot work without a mobile application, which is responsible for data collection and passing on the messages to doctors. This solution consists of an IoT-based ECG monitoring system which is implemented using the advanced techniques of mobile sensing, cloud computing and Web. ECG data are gathered using a wearable monitoring node and are transmitted directly to the cloud using Wi-Fi. The two driving factors of this technology are the IoT-based data collection and cloud-based analytics.

While in (Barik et al., 2017) Barik et al proposed SoA-Fog, a three-tier secure fog computing based solution for smart health applications. This framework allows communication between client layer, fog layers nodes and cloud layer for enhanced security features for health data sharing by using win-win spiral model. Health data could be analyzed for locating the area with critical issues of diseases so that proper healthcare facilities could be provided. In SoA-Fog framework, confidentiality can be achieved by SSL based security integration. Role based security is meant to focus on integrity of services whereas database security is to focus on the availability of the data to the authenticated user.

Finally, Barni et al (Barni et al., 2011) presented a Privacy-preserving system where a server can classify an ElectroCardioGram (ECG) signal without learning any information about the ECG signal and the client is prevented from gaining knowledge about the classification algorithm used by the server. In the proposed system wireless body sensor networks are attached to clients body to collect physiological data like Breathing Rate (BR), Blood Pressure (BP), Blood Glucose and Electrocardiogram (ECG), these data are then sent to a remote cloud server for processing and storage. Authors proposed the use of generic secure two-party computation protocols (2PC). The problem of enforcing access control policies over multiple parties involved in this mobile health monitoring is also solved by using attribute based encryption (ABE).

As shown in the two previous sections, security is a huge concern in Fog computing application, especially healthcare applications. Now we will emphasize on studies involving the use of ABE, as one of the most promising solution for data encryption and access control.

### 3.3 ABE in Fog

Fog Computing could be useful in E-Health applications, where real-time processing and quick response to events are essential. An intelligent Fog-based healthcare system is characterized by low latency, mobility support, as well as privacy support. Since the cloud server is not always fully trusted, the fine-grained access control on the encrypted data is quite desired from the viewpoint of users. Attribute-based encryption (ABE) is a promising solution for this requirement.

However, Zuo et al (Zuo et al., 2016) noticed that the size of ABE ciphertext and decryption cost are usually proportional to the complexity of the access policy. This impedes the use of ABE in IoT devices due to the limited resources. So they proposed Attribute-based encryption with outsourced decryption (OD-ABE), where it allows a proxy with a transformation key to transform ABE ciphertexts into simple and constant size ciphertexts, while the proxy cannot obtain the corresponding plaintext. By using OD-ABE, the most of the decryption cost on ABE ciphertexts can be moved from the IoT devices to the proxy (a fog node). Moreover, to fill the gap between the security requirements of fog computing and the security of OD-ABE, authors proposed the CCA security for OD-ABE by following the spirit of the traditional CCA security as close as possible.

Similar to previous work, Moffat et al (Moffat et al., 2017) found that whether the research into mobile devices has been translated to the application of attribute-based encryption in IoT where the challenges to support complex computation and data transmission are potentially more complex given the much greater heterogeneity and resource restrictions of IoT devices. They proposed ABE encryption and decryption to be delegated from the mobile device to the Cloud server. ABE encryption (resp decryption) is de-constructed into pre-encryption (resp pre-decryption) and then to distribute computation costs. Limiting the computation impact of extensive attribute lists defining the access policy (resp sets of individuals) through constant-size ciphertexts (resp secret keys), depending on whether CP-ABE or KP-ABE is used.

While in (Tan et al., 2013) Tan et al made a comparison between the two types of ABE. They noticed that KP-ABE allows higher flexibility and efficiency in the modification of access control towards any authorized personnel compared to CP-ABE. This is because the updates made on the descriptive attributes are much simpler than updates made on access structure. Experiments performed by authors showed that KP-ABE encryption time is shorter than CP-ABE. KP-ABE scheme is able to realize the lightweight encryption and producing smaller ciphertext size than CP-ABE in a resource constraint device. Moreover, medical information is being encrypted at a continuous basis, while key generation for each authorized

users is being generated once. Therefore, they concluded that KP-ABE encryption scheme is more appropriate to be implemented to secure medical information.

On another side Cha et al (Cha et al., 2016) introduced fog computing based rule violation monitoring system based on Attribute-based Proxy re-encryption (ABPRE), where only users with the necessary access privileges are able to decrypt the ciphertext. The proposed system encrypts the sensor (device) data gathered from vehicles, and the proxy quickly performs re-encryption (ABPRE). Authors found that gathering data from countless moving vehicles at the central server and summarizing and indexing them into a searchable form would be extremely difficult, when the problem can be addressed by extracting only the important data and processing them at the network edge, which would reduce the amount of data on the network and only the important metadata would need to be delivered. The setup and the key generation are a step performed by the institute that manages keys and access privileges, while the generation of re-encryption keys is a step performed by an administrative agency that owns the data. The encryption step is performed by the data generator, while the re-encryption is performed by the proxy. Finally, decryption is a step performed by a secondary user.

We end this section with the studies of Ambrosin et al on the Feasibility of Attribute-Based Encryption on Smartphone Devices (Ambrosin et al., 2015) and IoT devices (Ambrosin et al., 2016). In the first work authors studied the feasibility of applying ABE on smartphones devices. In particular, they implemented AndrABEn, an ABE library for Android operating system. Based on the results of the experiments performed, they concluded that using ABE on Android smartphones and similar devices is feasible with satisfactory performances. While in the second study, authors implemented a prototype wireless healthcare data reader system for remote monitoring, data collection and processing. In this system, measurements from medical sensors are collected, encrypted with CP-ABE, and sent to a data collection server. Most of the traffic in this scenario consists of ECG data. They finally concluded that CP-ABE can be used in such scenario supporting up to 5 attributes with 80 bits security.

# 4 DISCUSSION

From all above, we noticed that although ABE is a very useful cryptographic tool to realize fine-grained access control, and privacy preserving of health data in a Fog environment (Cloud-Fog-IoT architecture), the inefficient performance is its Achilles heel, especially when it comes to capacity limited devices. Several studies (see section 3.3) that have been conducted to adapt the use of ABE in the context of constrained environment, especially Fog computing, and improve its performance. From our point of view these improvements can be made at 3 levels.

## 4.1 Algorithmic Level

ABE suffers from high computational overhead. The heavy operations (exponentiation, pairing) of ABE scheme cause its lack of efficiency on resource-constrained devices. The main goal is to reduce ABE computational complexity without altering the security level.

First, we conducted tests to determine which features have the most impact on ABE encryption performance (see section 5), in terms of execution time, memory and CPU usage. The measurements made us realize that the most influential factors are the number of attributes and the size of the encryption and decryption keys.

As long as we could not freely modify these two criteria (the number of attributes depends on the application field and the size of the keys determines the level of security required), it would be wiser to lighten the operations acting on this data, which opens the way to a lot of research topics in terms of re-encryption, optimization of cipher texts, key cutting, reformulation of attributes . . . etc.

## 4.2 Data (Input) Level

One of the biggest obstacles to the development of Fog computing is the huge volume of information requiring a real-time processing. Thus, the second manner to improve ABE performance in the Fog is to reduce the input data size.

Just like the ECG signal can be significantly reduced by using DTW compression, we can apply similar and suitable techniques for different types of input data to minimize its size, as long as the following two rules are respected: The reduction must not alter the value and the meaning of the information (especially in the case of sensitive medical data), the processing performed on the data must not increase the cost of global encryption in terms of resources consumption.

These operations can be performed by the IoT devices themselves, as well as the Fog nodes located in the lower level of the infrastructure, just near the sensors, depending on the complexity of the processing, and the capacity of the device. Filtering can also be

performed to determine which data need to be processed locally, and which one has to be encrypted before being transmitted to the higher nodes of the hierarchy, including the Cloud servers.

### 4.3 Deployment Level

Applying public key cryptography to all layers of Fog environment is inadequate due to the high computing power consumption requirements. By providing an optimal deployment model, in which computation may be divided and offloaded to peer node, Kattepur et al (Kattepur et al., 2016) demonstrated 77.8% latency and 54% battery usage improvements over large computation tasks, by applying this optimal offloading.

This offloading has been applied to various computational tasks. We can apply similar scenario to cryptographic operations within an optimal deployment scheme. Medical data collected by HBSN is light encrypted if necessary and sent to lower level Fog nodes, where it is analyzed, filtered and response is sent back to end-users if necessary. Data then is restructured, classified, and each part is routed to the adequate upper node in order to be encrypted with suitable algorithm, and so on until it reaches the Cloud servers level where it will be stored for later analysis, after being decrypted by only authorized users.

This scenario meets the requirements of the OpenFog Consortium, which states that Fog nodes connected directly to the end devices mostly work as data concentrators, compressors and pre-processors. Fog nodes in the upper tiers are often endowed more capability and bestowed with data analytic and modeling tasks. On the other hand, reactive real-time computing and cyber-physical control often take place in the Fog Nodes close to the end devices while the data-to-knowledge conversion may be performed closer to the Cloud.

## 5 EXPERIMENTATION

In order to know what factors affect the performance of ABE encryption, we performed tests on two resource constraint devices (which will act as Fog nodes), namely a Smartphone Samsung S3 (1GHz ST-Ericsson U8420 CPU, 1,4 GB RAM) and a Raspberry Pi Zero (1GHz single-core CPU, 512MB RAM). We carried our tests (CP-ABE encryption) on medical datasets consisting of Diabetes patient records [1].

[1] http://archive.ics.uci.edu/ml/datasets/Diabetes

In both environments, we varied the encryption key size, the number of attributes, and the size of the data to be encrypted. And we measured the resulting ciphertext size, the execution time of the encryption operation, as well as the CPU and RAM consumption.

The results obtained were almost similar in both environments, namely that the two most influential factors are the key size and the number of attributes. Indeed, the more you increase the size of the encryption keys and the number of attributes (that constitute the access tree), the more the encryption operation will consume CPU, RAM and last longer. On the other hand, the size of the input data has no influence on the performances.

## 6 CONCLUSION AND PERSPECTIVES

Fog computing seems to be the missing link to the rise of the Internet of Things, and the development of new applications, especially in the field of e-health. Indeed, the contribution of the Fog infrastructure can solve a lot of problems. Firstly, because of its position close to the end user, it makes it possible to optimize decision-making and response time, compared to the latency of the Cloud. But also by the capacities of its peripherals, the Fog allowed treatments that were impossible to perform on IoT resource constrained devices. Cryptographic operations, quite resource intensive, are part of these treatments.

According to the study done in this paper, the use of attribute-based encryption within Fog nodes seems to be an interesting solution to meet the requirements of data protection while maintaining satisfactory performance, especially in healthcare field which requires real-time processing, and privacy preserving of medical data.

But this involves proposing optimal deployment schemes that meet the standard requirements, where each node performs a specific task according to its capabilities and its location in the overall infrastructure hierarchy, and contributes to achieving the objectives of the business application.

In our future works, we will take advantage of the tests performed and the results obtained, by acting on the factors that have the greatest impact, namely the key size and the number of attributes.

We will propose a Fog e-health application that performs ECG signal collection and analysis, with distributive variable-size keys management, as well as an access tree optimization mechanism based on the use of profiles, to reduce the number of attributes.

# REFERENCES


Alshiky, A. M., Buhari, S. M., and Barnawi, A. (2017). Ehr attribute-based access control (abac) for fog computing environment. In *Seventh International Conference on Computer Science CSIT*.

Ambrosin, M., Anzanpour, A., and Conti, M. (2016). On the feasibility of attribute-based encryption on internet of things devices. In *IEEE Micro Magazine, vol. 36, no. 6*, pages 25–35.

Ambrosin, M., Conti, M., and Dargahi, T. (2015). On the feasibility of attribute-based encryption on smartphone devices. In *IoT-Sys 2015*, Florence, Italy.

Barik, R. K., Dubey, H., and Mankodiya, K. (2017). Soafog: Secure service-oriented edge computing architecture for smart health big data analytics. In *5th IEEE Global Conference on Signal and In-formation Processing GlobalSIP 2017*, Montreal, Canada.

Barni, M., Failla, P., and Lazzeretti, R. (2011). Privacy-preserving ecg classification with branching programs and neural networks. In *IEEE Trans. Inf. Forensics Security*.

Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, pages 13–16. MCC12. ACM.

Butun, I., Sari, A., and Osterberg, P. (2019). Security implications of fog computing on the internet of things. In *to appear in Proceedings of the ICCE 2019*, Las Vegas, NV, USA.

Cha, H.-J., Yang, H.-K., Kim, J.-M., and Song, Y.-J. (2016). Design of monitoring system of rule violation using abpre in the fog computing environment. In *Asia-pacific Journal of Applied Science and Engineering for Better Human Life, Vol.6*, pages 29–31.

Dasgupta, A. and Gill, A. Q. (2017). Fog computing challenges: A systematic review. In *Australasian Conference on Information Systems*, Hobart, Australia.

Deshpande, U. and Kulkarni, M. A. (2017). Iot based real time ecg monitoring system using cypress wiced. In *International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, Vol. 6, Issue 2*.

Dubey, H., Montero, A., and Constant, N. (2017). Fog computing in medical internet-of-things: Architecture, implementation, and applications. In *Handbook of Large-Scale Distributed Computing in Smart Healthcare*.

Dubey, H., Yang, J., and Constant, N. (2015). Fog data: Enhancing telehealth big data through fog computing. In *Proceedings of the ASE BigData & SocialInformatics 2015*, page 14.

Kattepur, A., Dohare, H., and Mushunuri, V. (2016). Resource constrained offloading in fog computing. In *MECC 16*, Trento, Italy.

Kaur, L. and Mahajan, M. (2015). Cryptographic key exchange scheme for cloud based healthcare monitoring. In *International Journal of Advanced Research in Computer Science, Volume 6, No. 5*.

Koo, D. and Hur, J. (2018). Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing. In *Future Generation Computer Systems*, pages 739–752.

Martin, B. A., Michaud, F., Banks, D., and Mosenia, A. (2017). Openfog security requirements and approaches. In *IEEE Communications Society Invited Paper*.

Moffat, S., Hammoudeh, M., and Hegarty, R. (2017). A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot. In *Proceedings of the International Conference on Future Networks and Distributed Systems ICFNDS*, Cambridge, United Kingdom.

Petac, E. and Petac, A.-O. (2016). About security solutions in fog computing. In *Economic Sciences Series, Ovidius University Annals*.

Rani, S. and Kumar, P. (2015). A survey of research on health monitoring system using mobile cloud computing by home node base station. In *IJRITCC*.

Sahai, A. and Waters, B. (2005). Fuzzy identity-based encryption. In *EUROCRYPT'05*, pages 457–473.

Sun, L., Yong, J., and Soar, J. (2014). Access control management for e-healthcare in cloud environment. In *EAI Endorsed Transactions on Scalable Information Systems*.

Tan, Y.-L., Goi, B.-M., Komiya, R., and Phan, R. (2013). Design and implementation of key-policy attribute-based encryption in body sensor network. In *International Journal of Cryptology Research 4(1): 84 - 101*.

Yi, S., Li, C., and Li, Q. (2015). A survey of fog computing: Concepts, applications and issues. In *Mobidata15*, Hangzhou, China.

Zuo, C., Shao, J., and Wei, G. (2016). Cca-secure abe with outsourced decryption for fog computing. In *Future Generation Computer Systems*.