EHR ATTRIBUTE-BASED ACCESS CONTROL (ABAC) FOR FOG COMPUTING ENVIRONMENT

Aisha Mohmmed Alshiky, Seyed M. Buhari and Ahmed Barnawi

King Abdulaziz University, KSA, Jeddah

ABSTRACT

Cisco recently proposed a new computing environment called fog computing to support latency-sensitive and real time applications. It is a connection of billions of devices nearest to the network edge. This computing will be appropriate for Electronic Medical Record (EMR) systems that are latency-sensitive in nature. In this paper, we aim to achieve two goals: (1) Managing and sharing Electronic Health Records (EHRs) between multiple fog nodes and cloud, (2) Focusing on security of EHR, which contains highly confidential information. So, we will secure access into EHR on Fog computing without effecting the performance of fog nodes. We will cater different users based on their attributes and thus providing Attribute Based Access Control ABAC into the EHR in fog to prevent unauthorized access. We focus on reducing the storing and processes in fog nodes to support low capabilities of storage and computing of fog nodes and improve its performance.

KEYWORDS

Fog computing, Electronic Medical Record (EMR), Electronic Health Record (HER)

1. INTRODUCTION

The explosive increase in the use of sensors and sensing information leads to the scope of producing plenty of future applications. The most important requirement in these applications is low-latency processing and as known centralizing of services at the core of the Internet in the cloud computing may lead to high latency which is rejected. While there are numerous economic advantages of cloud, there is a problem for latency-sensitive applications due to frequent movements of huge data from the source to the server/cloud [1].

The latency-sensitive and real time applications require nodes in the vicinity to provide fast responses. A new platform is needed to achieve these requirements; [2] Cisco recently proposed a new computing environment called fog computing, call it “Fog”, simply because fog is a cloud close to the ground. It is a connection of billions of devices (called as fog nodes) around the globe. It's different from Cloud Computing: distribution of processing in distributed nodes with mobility. In fog computing environment, the generic application runs logic on resources throughout the network, including dedicated computing nodes and routers [3]. "The emerging

Jae-Kwang Lee et al. (Eds) : CCSEA, AIFU, DKMP, CLOUD, EMSA, SEA, SIPRO - 2017
pp. 87– 95, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70209

Fog Computing architecture 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 the network" [4].

However, developing applications using fog computing resources is critical because it includes heterogeneous resources at different levels of network hierarchy to provide low latency and scalability requirement for new applications [3]. In this research, the Fog environment is considered to be an appropriate platform to implement Electronic Health Records (EHR). Nowadays, in modern healthcare environments, healthcare providers are shifting their electronic medical record systems to clouds [5]. But as the cloud is not good choice for real time and latency sensitive applications, we propose that the Fog computing is appropriate for EHR. EHR contains private and sensitive patient health information which are needed to be secured and the privacy of the patient must be ensured. Security in Fog Computing Environment will eventually become an issue; with security embedded into the Fog Computing environment, we envision, in this research, to provide appropriate security solutions without effecting on performance. With the proposal of Attribute Based Access Control which is a flexible and logical mechanism [6], we will cater different users based on their attributes, object (information and resources) attributes and environment conditions (time and location). Thus, providing secure access mechanism into the EHR fog to prevent unauthorized access to fog and also prevent leaks of information; user-based attributes might be related to a targeted application.

In this paper, we introduce an innovative ABAC architecture for EHR in fog computing environment as an alternative that provides inherent advantages that will improve the security measures related to EHR. In addition to that, we exhibit that the introduction of fog computing will outperform the cloud based alternatives. This paper is organized as follows, in Section 2, we review the literature and present related work in cloud computing access control architecture. In Section 3, we list few applications for Fog Computing with emphasis on Healthcare sector. In Section 4, we describe our ABAC Fog computing architecture. In Section 5, we propose a location based Fog Computing ABAC architecture and analyze the proposed system against security threats and risks. In Section 6, we conclude and summarize our future work.

2. LITERATURE REVIEW

Instead of cannibalizing Cloud Computing, Fog Computing allows a new type of applications and services, and that there is a rich interplay between the Cloud and the Fog, mainly when it comes to data management and analytics. This review is mostly related to work and deals with the potential risks of privacy exposure to the healthcare system and implement electronic health record (EHR) in fog computing [1]. Security in Fog Computing Environment will eventually become an issue; this issue is not being investigated yet and it seems to be completely absent in the literature. For that, this section discusses a number of related and similar researches that provide security of cloud system especially for EHR.

One of studies [7] explains that patients' records must be accessible only by authorized users and they justified that patients should have the opportunity to exert the control over their own data. For that, they proposed a cryptographic access control scheme allowing patients to grant medical teams authorizations to access their medical data. They proposed a schema consists of decentralized hierarchical key agreement protocol to securely establish a hierarchy of crypto keys in agreement with the privilege levels of the team members. The scheme provides data

confidentiality, but it must be guaranteed that hierarchical keys are unique and "fresh" for each run of the protocol which require high computation.

As multiple entities will interact with the data, the authors in [8] explain that access to sensitive resources should be provided only to authorized users and tenants. They adapt Task-Role-Based Access Control, which considers the task in hand and the role of the user. They support both workflow based and non-workflow based tasks and authorize subjects to access necessary objects only during the execution of the task. Classification of tasks and activities has been done on the basis of active and passive access control and inheritable and non-inheritable tasks. Each user is assigned a role, roles are assigned to workflow or non-workflow tasks, and tasks are assigned to permissions. This model only supports the scenarios when the roles are defined within a single healthcare organization. It is designed to support healthcare service provided in a single healthcare organization. So, the access should be restricted and provided only during the execution of a specific task.

In [5] and [9], the authors mainly focuses on access control issues when EHRs are shared with various health care providers in cloud computing environments. In [5], they proposed a unified access control scheme which supports patient-centric selective sharing of virtual composite EHRs using different levels of granularity, accommodating data combination and various privacy defense requirements. However, this approach assumes that all health care providers adopt a unified EHR schema, which is not applicable in cloud environments. In [9], the authors try to overcome this limitation by supporting EHRs aggregation from various health care providers considering different EHR data schemas in cloud environments. They propose a systematic access control mechanism to support selective sharing of composite electronic health records aggregated from various health care providers in the cloud. They present algorithms for EHRs data schema composition and cross-domain EHR aggregation.

In [10], the authors explain that Attribute-Based Encryption ABE (data can only be read by a user with certain attributes [10] suitable for electronic health records system in the cloud, in which many users can retrieve the same EHR while each user can only decrypt the parts that they are allowed to read. The authors here try to handle some problems such as when a user with multiple roles might cause information leakage and computational overhead on EHR owners. Hence, they adopt both ABE and Identity Based Encryption IBE (a type of public-key encryption in which the public key of a user is unique user identity) and integrate them into their hierarchical framework. ABE is used to achieve fine-grained access control while IBE is used to securely transmit ABE keys. EHRs are encrypted on the Trusted Server and then are uploaded to the cloud. Decryption keys are also generated on trusted server and are distributed to domain servers that are then responsible for distributing the decryption keys to authorized entities. This framework addresses only the case of read access. This solution was suitable for an environment which has large number of users (subject) because it depends on their attributes which need not be predefined for each user.

Many research works proposed important and useful concepts of the EHR security [5, 7, 8, 9, and 10]. However, there are several uncertain issues. One of those issues is how to manage information of PHR and bring it near the user to support quick access of these information in timely manner. Therefore, allowing a hospital staff to access patient information (EHRs) in short period is essential. Information stored in the patient’s EHR may help a medical staff to make better decisions. In some emergency healthcare situations, immediate exchange of patient's EHRs is crucial to save lives. In our research, we try to handle the EHR near to the medical staff and

provide quick response for patient needs. We will support that by implementing part of EHR in suitable and nearest fog nodes and we propose that Attribute Based Access Control (ABAC) that depends on attributes of subject (who want to access), object (services or information), action attributes (view or delete patient information) and environment conditions (time and location). This approach is flexible and it decreases the administrative overhead [6].

3. FOG COMPUTING APPLICATION IN HEALTHCARE

In this section, we will review some of studies that applied fog computing in health care system. How to develop real-world fog computing-based universal health monitoring system is still an open question.

In [11], pervasive fall detection is employed for stroke mitigation. There were four major contributions in this study: (1) they examined and developed a set of new fall detection algorithms built on acceleration magnitude values and non-linear time series analysis techniques, (2) they designed and employed a real–time fall detection system employing fog computing paradigm, which distributes the analytics through the network by splitting the detection tasks between the edge nodes (e.g., smart phones attached to the user) and the server (e.g., cloud), (3) they examine the special needs and constraints of stroke patients and they proposed patient centered design that is minimal intrusive to patients and (4) their experiments with real-world data displayed that their proposed system achieves the high specificity (low false alarm rate) while it also achieves high sensitivity. Depend on researchers knowledge, their proposed system is the first large scale, real-world pervasive health monitoring system that employs the fog computing paradigm and distributed analytics.

Ultraviolet (UV) radiation has a great effect on human health. Since sensors in mobile phone cameras are very sensitive to UV, mobile phones have the potential to be an ideal equipment to measure UV radiance. The research [12] investigated theoretical foundations that control mobile phone cameras without any add-on to measure solar UV in open environment. Theoretical foundations accomplished to a procedure that can be deployed to any mobile phone with a camera. In addition, by utilizing fog computing, results can be collected and edited locally through fog server to provide accurate UV measurement. Furthermore, an Android app called UV Meter was established based on the procedure that can be implemented in mobile phones. Verification was conducted under unlike weather conditions and their results showed that the procedure is valid and can be implemented onto mobile phones for everyday UV measurement.

In another study [13], efficient IoT-enabled healthcare system architecture which benefits from the concept of fog computing is presented. The effectiveness of fog computing in IoT-based healthcare systems in terms of bandwidth utilization and emergency notification is demonstrated. In addition, they utilized ECG feature extraction at the edge of the network in their implementation as a case study. They proposed that to perform functionalities of gateways, the smart gateway should have the ability to offer a high level of advanced services in the fog computing platform. The smart gateway architecture including physical and operational structures is elaborately designed and described.

4. ABAC IN FOG COMPUTING ENVIRONMENT

Our policy framework adopts attribute-based security framework where in all users are authenticated and identified based on a set of attributes which are associated to each request. In our proposed framework, the ABAC is implemented and enforced at fog node which receives user access request. Each fog node which received requested action will analyze the attributes that is associated with the request. Then, based on these retrieved attributes and policies schema, the permission will be granted to user.

Our proposed solution used the recommended architecture of ABAC [14] as shown in Figure 1. As mentioned above, this architecture implemented in the edge of network (fog nodes). For that, authenticated and authorized access into EHR is applied on request at the nearest fog instead of at the core of the network (cloud).

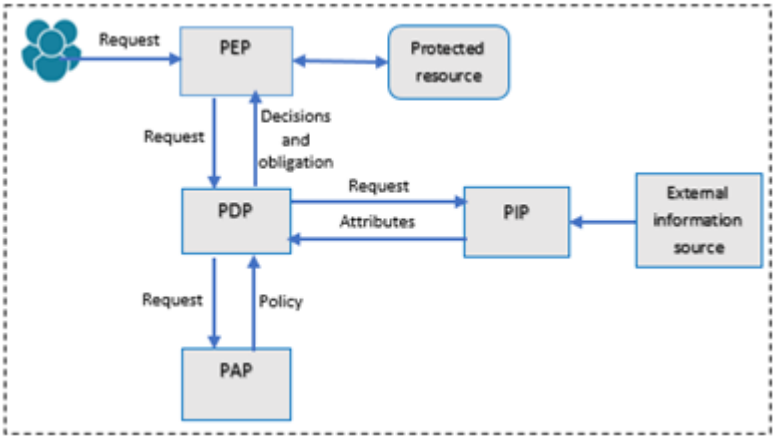

Figure 1. ABAC Architecture

- The PEP or Policy Enforcement Point examines the request and produces an authorization request and sends to the PDP.

- The PDP or Policy Decision Point evaluates incoming requests against policies that has been constructed. The PDP returns a Permit / Deny decision.

- The PAP or Policy Administration Point maintaines the policies and bridges PDP to policies statements. The administrator of host (fog nodes/cloud) is responsible to defines policises of its host. The multi-tenant nature of the fog computing model raises the requirement for an administrator to define policies that bind a user to healthcare system and implement policy schema. Each fog node has specific polices which are applied only to its users.

- The PIP or Policy Information Point maintains descriptive attributes and bridges the PDP to external sources of attributes e.g. databases. The administrator of host (fog nodes/cloud) is responsible to define PIP of its host. He prepares data schema that specifies a set of defined attributes associated with a physical or virtual component. Each

fog has data schema of its users only to avoid unused stored database. The attributes considered in our proposed ABAC are:

- Subject attributes (department, role and job title)
- Action attributes (view or delete patient information)
- Object attributes (object type, sensitivity of data)
- Environment attributes (time and location)

Simple use case of requested action (user 7 view patient 12 record) from Dr Khaled to medicine department fog is presented in Figure 2 below.

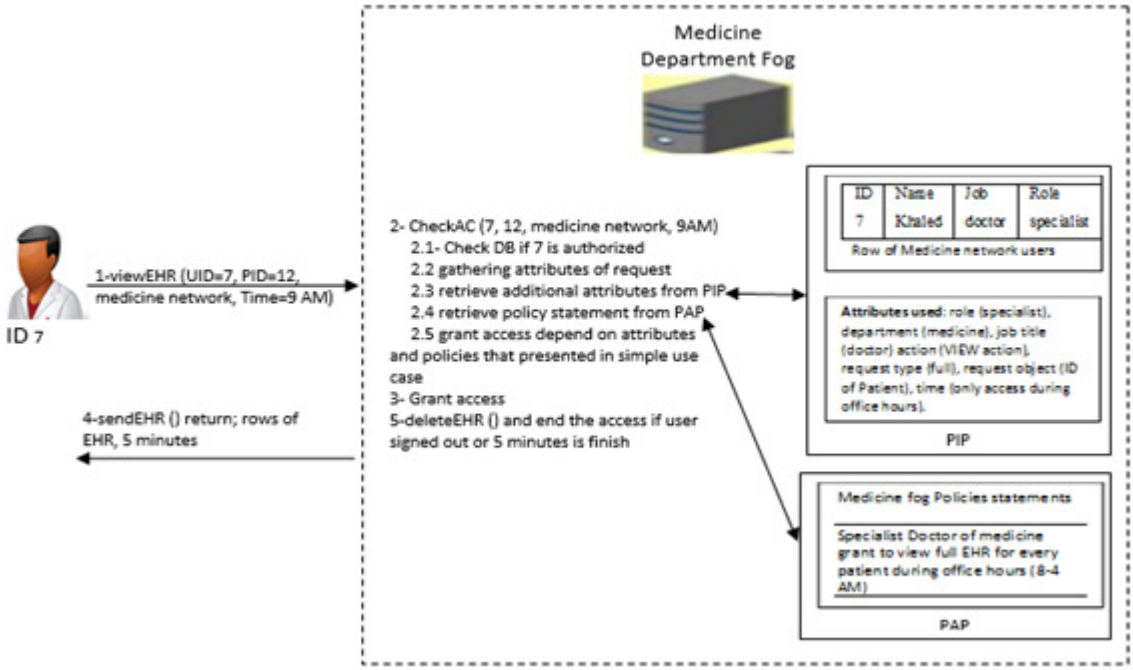

Figure 2. Simple use case of ABAC

5. LOCATION BASED ABAC FOG COMPUTING ARCHITECTURE

Depending upon location of fog device, the managing and sharing of EHRs between multiple fog nodes and cloud is maintained. The important issue that we considered in our solution is the low capabilities of storage and computing of fog nodes. We focus on reducing the storing and processes in fog nodes to serve the availability of fog, to improve its performance and efficiency. To achieve these goals we proposed that:

- All hospital information and needs are maintained in Cloud (data center)
  - Full version of Electronic Medical System (EMR) which contain EHRs of all patients in hospital are implemented in cloud (data center).
  - It serves all the hospital department's users.

- There is a fog device for every single hospital department
  - Part of EMR is implemented in fog, which provide only services that are needed by department's users to do their job.
  - Contains information and attributes of department network user and predefined access policies.
  - Fog applies ABAC into incoming request for each attempted access.
  - Fog maintains temporary and timely storage of EHR.
- Scheduling of EHR sharing between cloud and specific fog in specific location.
  - Movement timeline of visiting patient in hospital is estimated first. This estimation is assigned once patient visits reception department and reception user tries to access to patient information in cloud.
  - After first access of the patient record in cloud by the receptionist, scheduling of EHR sharing between cloud and specific fog in specific location occurred depends on proposed estimation. For example, patient Khaled will be directed to laboratory department after reception department within 5 minutes. So, depending upon proposed estimation, the cloud will send copy of visiting patient EHR into specific location of fog within 5 minutes.
  - Timing of patient services in specific department is estimated. Once patient arrives and user in this location (department) starts to serve him/her, the timer is started and after the timer ends, the EHR is deleted from the temporary storage of fog.

Simple scenario is presented in Figure 3 to explain simple patient workflow from reception to laboratory and time of EHR sharing between cloud and specific fog in specific location (laboratory). It is estimated that patient after 6 minutes (360 s) will go to laboratory department. Before the patients' arrival to laboratory department, the cloud will send copy of visiting patient EHR to specific location (laboratory department).

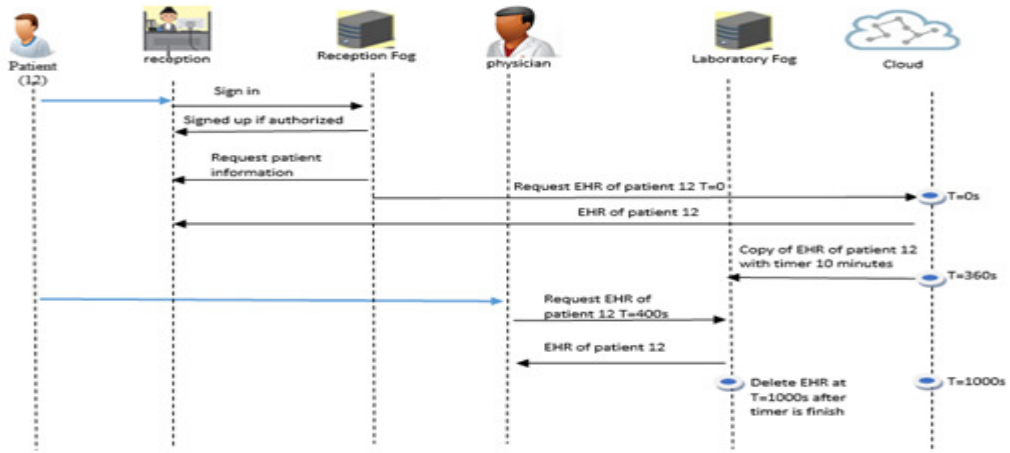

Figure 3. EHR sharing between cloud and fog

6. CONCLUSION AND FUTURE WORK

We provided ABAC into the EHR in fog to prevent unauthorized access. Also, we considered in our solution the low capabilities of storage and computing of fog nodes by focusing on reducing the storing and processes in fog nodes to serve the availability of fog, to improve its performance and efficiency.

In our future work, we will simulate our solution by using iFogSim tool and we will evaluate the results of our solution.

REFERENCES

[1] Hong K, Lillethun D, Ramachandran U, Ottenwälder B, Koldehofe B, editors. Opportunistic spatio-temporal event processing for mobile situation awareness. Proceedings of the 7th ACM international conference on Distributed event-based systems; 2013: ACM.

[2] Zhu J, Chan DS, Prabhu MS, Natarajan P, Hu H, Bonomi F, editors. Improving web sites performance using edge servers in fog computing architecture. Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on; 2013: IEEE.

[3] Hong K, Lillethun D, Ramachandran U, Ottenwälder B, Koldehofe B, editors. Mobile fog: A programming model for large-scale applications on the internet of things. Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing; 2013: ACM.

[4] Bonomi F, Milito R, Zhu J, Addepalli S, editors. Fog computing and its role in the internet of things. Proceedings of the first edition of the MCC workshop on Mobile cloud computing; 2012: ACM.

[5] Wu R, Ahn G-J, Hu H, editors. Secure sharing of electronic health records in clouds. Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on; 2012: IEEE.

[6] NIST GS, Goguen A, Fringa A. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. 2002.

[7] Boyd C, Mathuria A. Protocols for authentication and key establishment: Springer Science & Business Media; 2013.

[8] Narayanan HAJ, Güneş MH, editors. Ensuring access control in cloud provisioned healthcare systems. 2011 IEEE Consumer Communications and Networking Conference (CCNC); 2011: IEEE.

[9] Jin J, Ahn G-J, Hu H, Covington MJ, Zhang X. Patient-centric authorization framework for electronic healthcare services. computers & security. 2011;30(2):116-27.

[10] Huang J, Sharaf M, Huang C-T, editors. A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud. 2012 41st International Conference on Parallel Processing Workshops; 2012: IEEE.

[11] Cao Y, Chen S, Hou P, Brown D, editors. FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation. Networking, Architecture and Storage (NAS), 2015 IEEE International Conference on; 2015: IEEE.

[12] Mei B, Cheng W, Cheng X, editors. Fog Computing Based Ultraviolet Radiation Measurement via Smartphones. Hot Topics in Web Systems and Technologies (HotWeb), 2015 Third IEEE Workshop on; 2015: IEEE.

[13] Gia TN, Jiang M, Rahmani A-M, Westerlund T, Liljeberg P, Tenhunen H, editors. Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction. Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on; 2015: IEEE.

[14] Coyne E, Weil TR. ABAC and RBAC: scalable, flexible, and auditable access management. IT Professional. 2013;15(3):0014-16.