A Data Protection Model for Fog Computing

Thanh Dat Dang
University of Technology Sydney, Australia
School of Computing and Communications
Thanh.D.Dang@student.uts.edu.au

Doan Hoang
University of Technology Sydney, Australia
School of Computing and Communications
Doan.Hoang@uts.edu.au

Abstract— ***Cloud computing has established itself as an alternative IT infrastructure and service model. However, as with all logically centralized resource and service provisioning infrastructures, cloud does not handle well local issues involving a large number of networked elements (IoTs) and it is not responsive enough for many applications that require immediate attention of a local controller. Fog computing preserves many benefits of cloud computing and it is also in a good position to address these local and performance issues because its resources and specific services are virtualized and located at the edge of the customer premise. However, data security is a critical challenge in fog computing especially when fog nodes and their data move frequently in its environment. This paper addresses the data protection and the performance issues by 1) proposing a Region-Based Trust-Aware (RBTA) model for trust translation among fog nodes of regions, 2) introducing a Fog-based Privacy-aware Role Based Access Control (FPRBAC) for access control at fog nodes, and 3) developing a mobility management service to handle changes of users and fog devices' locations. The implementation results demonstrate the feasibility and the efficiency of our proposed framework.***

Keywords— fog computing; cloud computing; data protection; mobility; fog security; fog location; access control

I. INTRODUCTION

Fog computing enables more processing tasks to be performed at the network edge before being moved to the core network or centralized clouds. Decisions shall be made by edge devices rather than being submitted and received from clouds. This leads to more efficient process and the ability to react more quickly to events. With the potential for billions of IoT devices creating data, data management becomes an issue at the edge network since it fails in providing adequate bandwidths for all of data to be transferred through the network. Architectures for fog are, however, in the early stage of being defined with open issues for the current research [1].

Fog resources are structured by the large number of physical devices in various locations and different type of communication and connections. Nevertheless, fog devices frequently change their locations and may request or provide nearby computing resources for faster responses. Thus, provisioning computing resources locally and allocating into regions users shall shorten the response time and enable adequately resource distributions. In fact, a location service also needs to be proposed to address frequently changes of fog devices' locations. In this paper, we introduce a local computing concept called "Region" to deal with these issues. A fog region centres on a physical location which covers services for users. It includes all fog devices such as high-end servers, smart phones, and vehicles connected each other via wire or wireless connections in a defined geo-graphic location. Some fog devices, which may share computing resources in multiple regions, move to a new region but still request and/or provide computing services.

The deployment of computing resources and data at regions shall provide users better experiences. However, the security aspects of such the architecture, if not handled correctly, could be devastating since a malicious entity may compromise the devices and cause them to make the wrong decisions at critical times. Several protection mechanisms have been well-established in cloud environments [2, 3] but find it difficult to apply to fog computing due to low-latency restrictions and mobility requirements. Furthermore, there have been only few research efforts on security and mobility for fog computing according our literature view. Thus, this paper proposes a novel data protection model for fog computing which provides region-based trust establishment, mobility service, and Fog Privacy Role Based Access Control (FPRBAC). It enables fog devices in different regions share and access resources in a secured manner. In fact, the mobility service enables clients to keep track of changes of data location among regions periodically by using a Location Register Database (LRD) as well as an enhance verification procedure at FPRBAC. As a result, it tightens security constraints while ensuring more flexibility in mobility management. FPRBAC is able to verify requests on constraints related to users' role including role, region, condition, purpose and operation. As a consequence, policies can be enriched to prevent security violations.

The contributions of this paper include: 1) We propose a new concept of "Region" where users, fog nodes, and fog devices are allocated, and a protocol to establish trust agreements among regions; 2) We introduce a mobility service for location registration, which provides efficiently location services for fog devices and enables users deploying applications with high mobility; 3) We also design a fog privacy role based access control to grant users' permission and authorize requests based on assigned roles that enables system to detect attacks based on the audit records.

978-1-5386-2859-1/17/$31.00 ©2017 IEEE

The rest of the paper is organized as follows. Section II discusses related work on security in fog computing and motivation. Section III presents the adversary model. Section IV presents the design of the proposed data protection model in fog computing. Section V presents evaluation and results for our model. The conclusion will be drawn in section VI.

II. Related work and motivation

Fog computing has become a computing model for providing real-time computing services and storage. However, few research efforts have focused on security issues which existed intrinsically in highly dynamic computing services. Clinton [4] proposed a policy-driven security management framework for fog computing which secures collaboration and enables interoperability of user-resources. Specifically, the proposed policy management mechanism supports not only virtual component interaction but also physical component interaction including fog nodes and fog instances communicating with physical devices and cloud data centers. The defined policies have focused on collaboration among components in fog computing based on policy modules. However, there is no attempt to protect resources and preserve user privacy. In fact, role-base access control was not used to define and confine the access rights of sub-systems and components in this multi-user environment. Chen [2] proposed a framework with Cloud-based Privacy-aware Role Based Access Control (CPRBAC). CPRBAC extends traditional Role Based Access Control model and include additional components such as Organizations, Conditions, Obligations and Purposes. The model, however, fails to provide low sensitive-latency verification as it is at cloud-based authorizing. Enhancing low-latency services and improving performance were studied in [5, 6], where trade-off performance approaches between fog and cloud, and allocating fog resources to applications were carried out. Nevertheless, these researches did not focus on security concerns in implementing fog systems. Consequently, users find it difficult to adopt fog computing since the adversaries may exploit the vulnerability to compromise the users' sensitive data. Studies related to potential security and privacy problems in fog computing [7, 8] have been investigated to identify types of attack on users' data. Authors have raised some potential attacks such as man-in-the-middle attack, intrusion detection, malicious detection, and malicious Fog. Nevertheless, the lack of security approaches in fog computing prevents users from adopting fog computing since the adversaries may exploit the vulnerability to compromise the users' sensitive data.

Our work is motivated by the lack of security approaches in fog computing platforms and the mobility service that enables fog devices to register and consume the current region's services. The lack of a security framework for fog computing leads to two basic challenges as follows:

Security and privacy challenges. Fog computing has been applied at the network edge to provides added computing and resources. These resources are used to serve requests on users' sensitive data. Therefore, fog devices may be compromised by many potential threats or replaced by fake ones that may expose sensitive information. Moreover, in multi-users fog computing environment, users require access to their data based on their assigned roles. Thus, strong protecting data from illegal disclosure or malicious violation will provide a basis for widespread adoption of fog computing technology either business sectors or research areas. These issues surrounding fog computing still have not been addressed with appropriate mechanisms. Consequently, fog computing has not been adopted widely yet.

Mobility management challenges. Fog devices with high mobility change frequently their locations but fog computing has not supported location registration. Thus, it is difficult to deal with tracking and tracing location requests. Without a location register service, a fog device is not able to register with a new region and allows the region to manage location records. Given that the location records are large and stored in the distributed environment, tracking and tracing of data locations are time and resource consuming. This function should be delegated to a specific mobility service.

Our work focuses on designing an important class of fog security framework and building trust among regions enabling fog's mobility. In particular, a mobility service with location registration is designed and implemented to store information about fog's devices registration, users, operations, location, and timestamp. The service addresses location issues by offering location register, location verification and traceability for all clients' requests. The security framework relies on trust among regions where fog devices are able to join and leave within relevant assigned roles. In fact, FPRBAC verifies requests to allow users accessing computing resources from fog nodes based on granting permissions based on assigned roles.

III. Adversarial model

A. Adversarial model assumptions

We present our assumptions regarding fog-based region data protection in the present of an adversary as follows: 1) *fog devices integrity:* technical and non-technical approaches to prevent such fog devices tampering have been taken to prevent the issues of device tampering to regions; 2) *physical security:* fog devices are owned by both users and service providers. These devices can be physically observed, enforced and verified through known best practice on duty management by organizations. This assumption is important for building high-level hardware and software security guarantees for the components of fog-based region infrastructure; 3) *cryptographic security:* we assume symmetric and public-key encryption schemes are semantically secure and that adversary cannot obtain plain text of encrypted data when it is sent and received by fog devices, and that the message authentication code algorithm correctly verifies message integrity and authenticity; *4) defined policies:* defined policies correctly authorize valid requests associated with users, fog nodes, fog devices and operations. The adversary cannot modify defined policies to grant and bypass FBRBAC by their own permissions.

B. Adversary capabilities

In this section, we describe specific capability for adversaries, denoted by *ADV*. We adopt the Yao-Dolev [9] threat model in which, an *ADV* can overhear and generate any requests to regions and is only limited by the constrains of cryptographic mechanisms.

We define two complementary adversarial types. One acts as a user, denoted by *ADV A*, to compromise the confidentiality and integrity of data in a region. Other type acts as a fog device, denoted by *ADV B*, has capabilities to send requests and receive responses over regions. They are able to perform the following actions: 1) Send a valid request with arbitrary roles and operations to regions it can reach; 2) Attempt to impersonate other fog devices; 3) Issue arbitrary policies within its region; 4) Use the cryptographic material to decrypt network traffic that is sent and received by other fog devices.

C. Attack vectors

From the adversary model, we identify potential attacks relevant to fog computing from fog-based regions perspective as follow: 1) *Direct access and intrusion attack*: the adversary bypasses the trust of regions and generate requests with different parameters to FPRBAC; 2) *Man-in-the-Middle Attack*: the adversary may compromise fog nodes and replace with fake ones. It then intercepts the communication among other fog nodes, and attempt to make them believe that they are communicating with each other over a correct and safe connection; 3) *Attack on policies and roles in FPRBAC*: the adversary may issue malicious policies that overwrite or disable legitimate policies already in place.

IV. THE PROPOSED ARCHITECTURE

In this paper, we focus on providing a data protection model which allows users to access securely resources based on assigned roles. The new features of our proposed model include: a region-based trust component to deal with new joined devices coming from other regions; FPRBAC for verification and authorization; Mobility management to deal with changes of fog devices' location, tracing, tracking, and triggering an alarm on any operation, data or policy violations. Figure 1 depicts the model and its three core components: 1) the Region-Based Trust-Aware component; 2) Fog-Base Privacy-Aware Role Based Access Control; and 3) the mobility management component. These components will be described in the next subsections.

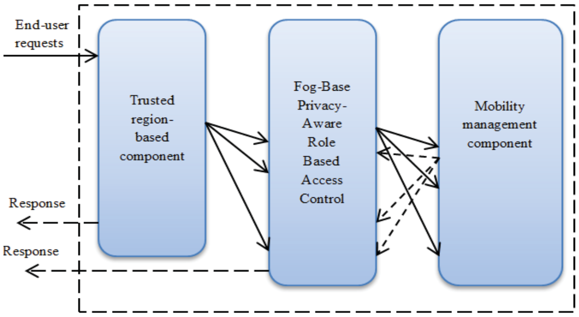

End-user requests
Trusted region-based component
Fog-Base Privacy-Aware Role Based Access Control
Mobility management component
Response
Response

Fig. 1. The design of data protection framework for fog computing

A. Region-based Trust-Aware for fog nodes

Figure 2 present the fog-based region scenario. In this design, a region can be structured by one or several fog nodes.

A fog node consists of several fog devices with weak performance which are deployed at edge network. It can provide computation, network resources and storages. The fog devices are heterogeneous raging from high-end servers to end devices such as mobile devices, wearable devices. For example, the Region 1 is structured by fog node 1 and fog node 2 while Region 2 is formed by fog node 3 and fog node 4.

Fog election: It is essential to have a fog node which delegates the management of computing resources and task executions of a region. A region has to deal with not only high frequencies of join and leave requests but also with sensitive-data protection. We use a decentralized method [10] to select the delegated fog node in the region. Each fog node sends its vote among other fog nodes and its received votes to them. so that the votes in the region finally are collected into high capacity nodes. A *heartbeat* is sent by every fog node to other fog nodes in a region periodically, at a *heartbeat interval*. Heartbeats are used by a fog node as a means to inform all fog nodes it is alive. A delegated fog also sends all fog nodes in its region every time the region changes by the detection of an event, which is either a new fog that entered the region or one that left or crashed.

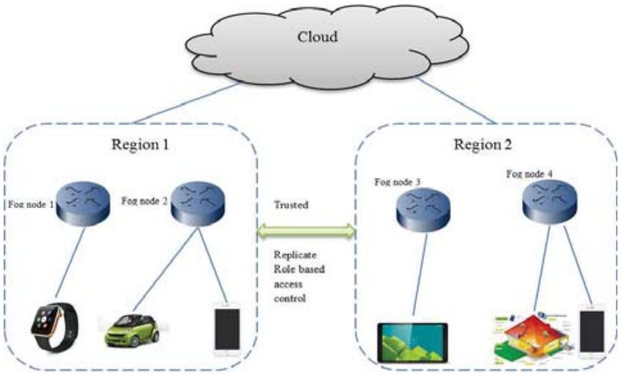


Fig. 2. The overview of Region-based Trust-Aware scenario

1) Trust establishment between two regions

When a region receives a request to establish the trust relationship with a new region, it will verify and analyze the request to obtain the destination address. A general procedure has to be executed between the two regions as request and response messages of two delegated fog nodes. The procedure is as follows: 1) The new region sends a request to the original region for establishing trust between them; 2) the original region analyses the request whether it can or cannot establish the trust and relies by a message; 3) Once two regions accepted the trust establishment, the trust relationship is updated at databases of these regions.

Two delegated fog nodes from each region carry out the Challenge/Response process [11]. Hence, Trust evaluation is performed to obtain the trust value. The delegated fog node in the requested region tests all requests from other regions and evaluates the trust degree on each region before making a decision whether to accept it and establish a trust relationship between two regions. Specifically, it raises a number of

TABLE I. SAMPLE ACCESS ROLES

Subject	Role	Object	Operation	Permission
Alice	Patient	Alice'personal info, Alice' old medical records, and Alice's summary treatment report	Read	Grant
Bob	General practitioner	Alice'personal info, Alice' old medical records, Alice' private Notes, and Alice's summary treatment report	Read/write	Grant
Alex	Invited practitioner	Alice'personal info, Alice' old medical records, and Alice's summary treatment report	Read	Grant

questions or commands which are performed by the delegated fog in other region. Based on the number of correct answers, the requested region decides whether the trust relationship is or is not established.

2) Join/leave a region

A fog with high mobility requirements switches more frequently among regions. Hence, it needs to be verified its roles in order to use computing resources in new regions. The join operations of fog devices are similar to a mobile device in mobile network [11]. When the delegated fog node receives a joined request from fog devices, it will verify and analyse the request to obtain the Fog_ID and the region. Thus, the trust relationship can be verified correctly between current region and the home region of fog devices based on this information. After the join process completes, LRD will be updated at both regions. When a fog device wants to leave the region, it notifies the fog nodes to update LRD. Sometimes, fog devices will leave the system without notice since its connections are lost. To handle abruptly leaving, fog nodes scan device status and update LRD periodically.

B. Mobility management component

Fog devices are highly dynamic and frequently switch among regions. It is vital to provide a mobility service at regions handling location requests such as update and query. The mobility management component includes the Mobility Service (MS) and the LRD.

The MS is responsible for creating queries submitted by fog nodes to the LRD. When a fog device is granted permissions in a new region, the MS updates the information about the fog in the LRD. In addition, it also supports verifying a new fog participating in the region.

The LRD provides both users and fog devices register when there is a change of location from one region to another. It stores fogs' information related to Fog_ID, Fog_location, Operations and Timestamp for monitoring purposes. Fog_ID represents entities such as users, fog nodes and fog devices. When a Fog_ID is generated for a request subscribing to a new region and, the registration procedure is performed that involves a binding location service for the data welfare including monitoring and raising an alarm. Therefore, whenever a fog device moves out of its home region, a request is submitted to the MS to extract information from the database necessary to perform registration. In addition, LRD is also served for location analysis, decision and exchange information.

C. Fog-based Privacy-aware Role Based Access Control (FPRBAC)

Role based access control (RBAC) model [12] lacks context information to satisfy sophisticated scenarios. To achieve light data protection scheme with sensitive-latency requirements, we introduce new components: *Region (Rg), Conditions (Co)*, *Obligations (Ob), Location (L)*, *Operation (Op), Purposes* and *Location (L)* to adjust policy description for the distribution of fog node concerning authorization delegation, cross-realm role assignment and privacy-aware scheme beside *Subject (S), Object (O), Role (R)*.

In the model, *Subject (S)* is an entity which accesses relevant Object. It can be a user, a fog node or a fog device, and its attribute is used to determine a specific role. *Object (O)* represents any computing resources or data relating to the identified *S*, such as fog devices or smart devices. *Role (R)* is a functional entity associated with specific authority and responsibility within a region. For instance, in Smart Traffic Lights application, Connected Vehicle can request and receives an optimum route to its destination based on the estimated time of arrival but Emergency Connected Vehicle can access and update a new route for other vehicles based on its current location. *Operation (Op)* binds *O* and consists of a set of actions that a subject can execute (such as read or write privileges). *Region (Rg)* is a domain identifier that defines *R*. In fog computing, the set of *Rgs* and *Rs* defines distributed role allocation. *Condition (Co)* is a prerequisite to be met before any *Op* can be executed, for example, school bus's route can be only disclosure to other Connected Vehicle when the current time is between 9 AM to 3 PM. *Purpose (Pu)* specifies the intended reason of the *Op*. Emergency Connected Vehicle can access the route of a Connected Vehicle only when the purpose is to respond a reported emergency. *Location (L)* is a function which must be executed before an *Op* is executed on *O* or after the execution.

We proposed the Fog-Based Region verification algorithm for the proposed model to verify requests at a region. A request is checked if it is trusted or needs a trust establishment (line 2-4). In line 3, FPRBAC is executed to verify roles in requests. The MS is performed to update LRD and notify data owners (line 8-11).

Algorithm 1. Fog-Based Region verification algorithm

Input: A set *RQ* of requests to access the data with parameters.

Output: granted or denied requests

```
1: for each request r in RQ do
2:   if r.region_id exists in Trust database then
3:       r.trust = true   // Request is trusted and passed to FPRBAC
4:   else
```

```
        trust_establishment(r) // Establish a trust relationship
    end if
    result = verify_FPRBAC(r) // verify access roles in the request
    if result = true then
        MS_Update_LRD(r) // Update LRD and notify data owner
    else
        MS_Notify_User(r) // The MS notifies data owner
    end if
end for
```

D. Use case scenarios: Healthcare applications

In this section, we introduce our use-case scenario to demonstrate the proposed model in supporting Healthcare Information System (HIS). Electric Health Records (EHRs) are integrated in the Health Information Systems (HIS) which allow patients to manage and control their health records through the internet. Patients can access their health data and share the data to physicians, health care providers, insurance practitioners, researchers and family members. We demonstrate the FPRBAC in protecting data.

A patient named Alice is recently diagnosed with gastrectomy cancer. Surgical removal of the stomach (gastrectomy) is the only curative treatment. Alice is assigned to a general practitioner, named Bob from the hospital (e.g., hospital A, located as Region A), who he regularly visits. Bob is granted full permissions to access Alice' data including read and write operations. Under Alice's health conditions, he needs to seek additional consultation regarding his treatment from different hospitals (e.g., hospital B). Alex is assigned as an invited practitioner. He is required to analyze solving the Alice' medical case and suggest a possible solution to Bob. Specifically, Alex can read a patient's EHRs for treatment purpose only if the current time is during 9AM to 6PM, however, patients and Bob will be informed by email. The above-mentioned scenario requires the FPRBAC's verification for any data operations.

V. Evaluation and results

A. Testbed

We have implemented a test bed which focuses on the data protection that includes an authorization service based on our FPRBAC model and the mobility service. We assume that applications are deployed across multiple regions. Hence, data are stored in a distributed data warehouse. A new data is generated and stored at fog nodes in buffers before synchronizing the data to its servers. Similarly, data is retrieved from clouds and stored at fog nodes to serve for requests. Hence, FPRBAC service can function as a security guard in the entire data protection model of fog computing. Requests are submitted from users and also other fog nodes. Our fog nodes are implemented on a Dell PowerEdge R730 Intel Xeon E5-2660 v3 2.6GHz 16 GB and an IBM Blade center HS20 including 8 Blades, an IBM DS400, a FC switch, and 3 Ethernet switches. We also use two Raspberry Pi 3 as the gateway located at each fog network. The LRD are deployed at fog nodes to reduce latency in serving queries from the MS. In fact, we also implemented the LRD at cloud for synchronizing among LRDs at fog nodes. Specifically, The Amazon EC2 [13] was to provide resources and the LRD as global location database. All LRD are run on MySQL. Fog nodes were built based on the fog project package [14] and deployed on two fog systems. Packages of our model were deployed on these fog instances and requests are able to access data via an RMI interface. Google Cloud Message (GCM) [15] was devised to notify users when there are any operations on the data.

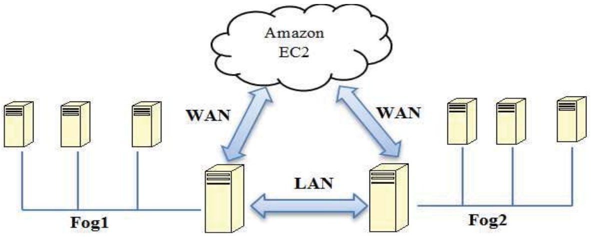


Fig. 3. Testbed setup

B. Performance evaluation

This section presents the performance evaluation for the proposed model. We investigate different aspects as follows: 1) processing time evaluation; 2) data protection evaluations; 3) mobility evaluations.

Suppose that there are *N* requests for fog resources. For each request $r \in N$, the processing time consists of elements as follows: 1) the trust establishment time from two regions, denoted as *tt*; 2) the lookup service time from client to fog node, denoted as *lt*; 3) the verification and mobility service time at fog node, denoted *vt*; 4) the response time from fog node to client, denoted *rt*. Each node of fog computing network represents for a method and an edge represents whether a method is invoked. Assume that the execution cost of a method *m* in a fog node is m_f and on cloud server m_c. So the duration of executing a request on a fog node is:

$$m_f = \sum_{\forall\, i \in N} tt_i + lt_i + vt_i + rt_i \quad (1)$$

If two regions have established the trust relationship, *tt* is set equal to 0. Regarding to the execution time of a request at cloud server in [16]. The cost of executing a request is:

$$m_c = \sum_{\forall\, i \in N} t_{lookup\ service_i} + t_{verification\ and\ data\ mobility_i} + t_{Data\ operation_i} \quad (2)$$

C. Response time performance - comparing Fog and Cloud processing times.

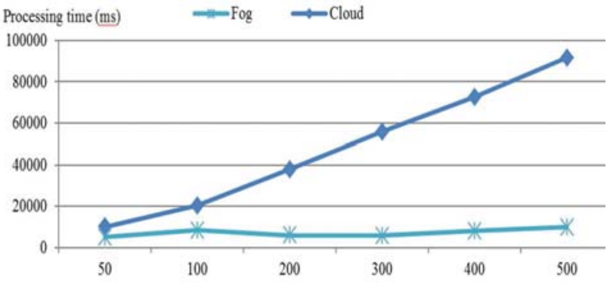


Fig. 4. Time cost of verification and mobility services for different requests

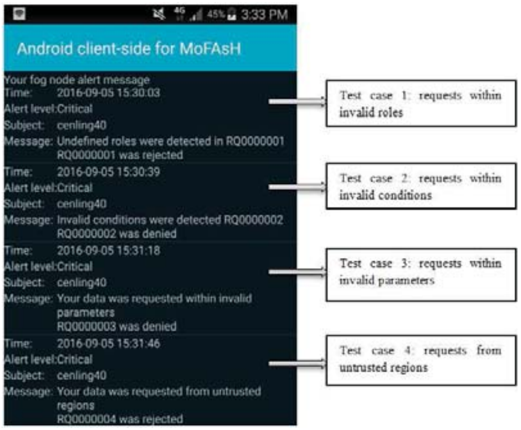
Table 1 illustrates the execution time of services for a request. It can be seen that the response time of fog node is much slower than that of cloud instance, approximately ½ execution time. Notably, the proposed model introduced small latency in the response time, approximately a quarter of the response time. Therefore, the proposed model finds it possible to integrate fog applications to protect data while still satisfying latency requirements.

Request traffic

TABLE II. EXECUTION TIME OF COMPONENTS

Execution components	Fog	Cloud
Lookup service	350 ms	651.8 ms
Verification and mobility service	160 ms	500 ms
Overall response time for a request	635 ms	3748 ms

Figure 4 illustrates the execution time of lookup and verification and mobility services for different number of requests. It can be seen that along with the increasing of the number of requests, the time cost of verification and mobility services increases obviously for our model. However, comparing to the overheads at cloud, our model only experienced slight latency due to processing many verification requests. Notably, with large IoT population, excessive traffic from the edges of the network to the Cloud affect latency severely.



Your fog node alert message
Time: 2016-09-05 15:30:03
Alert level:Critical
Subject: cenling40
Message: Undefined roles were detected in RQ0000001
RQ0000001 was rejected
Time: 2016-09-05 15:30:39
Alert level:Critical
Subject: cenling40
Message: Invalid conditions were detected RQ0000002
RQ0000002 was denied
Time: 2016-09-05 15:31:18
Alert level:Critical
Subject: cenling40
Message: Your data was requested within invalid parameters
RQ0000003 was denied
Time: 2016-09-05 15:31:46
Alert level:Critical
Subject: cenling40
Message: Your data was requested from untrusted regions
RQ0000004 was rejected

Test case 1: requests within invalid roles
Test case 2: requests within invalid conditions
Test case 3: requests within invalid parameters
Test case 4: requests from untrusted regions

Fig. 5. FPRBAC violation notification view in Samsung Galaxy Note 4

D. Data protection performance - detecting violations against access control policies

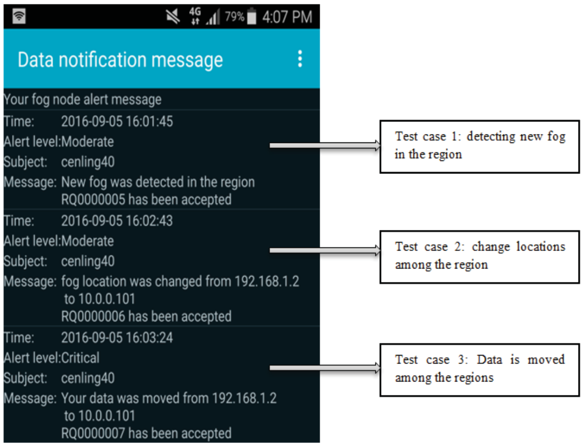
In this section, we conduct data violations against access control policies of our proposed model and trust-based region verification in order to evaluate the proposed model reacting correctly by following test cases: 1) requests try to violate the role based access control and bypass verification procedure within undefined roles; 2) clients request to access the data within insufficient conditions; 3) requests with invalid parameters attempt to gain access to the data. 4) users from untrusted regions attempt to retrieve the data at the new region. Figure 5 presents notification messages related to violations detected by the FPRBAC.

Direct access and Intrusion attacks. A request without any parameter is processed as an intrusion attack. Hence, the FPRBAC locks the source of request and invoke the MS to notify data owner or administrator. In fact, a request with correct parameters is still required to go through the verification process where FPRBAC validates each parameter. Moreover, if the verification process exceeds the configured time threshold, the FPRBAC would reject the request and terminate the process.

Attack the role based access control within undefined roles. Since FPRBAC has predefined roles associated data operations, a request is firstly verified whether it consists of roles matching with the list of roles in the system. Any inconsistent outcome created in the process would be actively detected when the FPRBAC is running and cause its termination. Retrieving these values and tampering with them to eliminate their functions are technically difficult.

Requests to access the data without valid conditions. At this checkpoint, roles and data operations are input and verified with conditions. If any inconsistent constrain occurred, requests are denied and a notification message is sent to the data owner.

Requests coming from untrusted regions. A request is only verified at FPRBAC if it comes from trusted region. to the fog system. Thus, the trust relationships need to be established among regions in other to process the request.



Your fog node alert message
Time: 2016-09-05 16:01:45
Alert level:Moderate
Subject: cenling40
Message: New fog was detected in the region
RQ0000005 has been accepted
Time: 2016-09-05 16:02:43
Alert level:Moderate
Subject: cenling40
Message: fog location was changed from 192.168.1.2 to 10.0.0.101
RQ0000006 has been accepted
Time: 2016-09-05 16:03:24
Alert level:Critical
Subject: cenling40
Message: Your data was moved from 192.168.1.2 to 10.0.0.101
RQ0000007 has been accepted

Test case 1: detecting new fog in the region
Test case 2: change locations among the region
Test case 3: Data is moved among the regions

Fig. 6. Mobility service notification related to location changes view in Samsung Galaxy Note 4

E. Mobility service operations

Figure 6 shows notification messages associated with different location changes. We established three test cases: the first one is triggering the MS when there is a request to join in current region; the second one is changing locations among regions; and the third one is triggering the MS when moving the data. All three test cases triggered the MS and then the notification message is sent to users' mobile devices immediately. The MS notifies data owner or administrator when it receives requests related to both fog locations and data locations. Then, it triggers the notification center to send a message to inform data owner about the status of request.

VI. Conclusion

This paper presented a data protection model for fog computing to protect data and handle mobility. The model features a Region-Based Trust-Aware (RBTA) model for trust translation among fog nodes of regions, a Fog-based Privacy-aware Role Based Access Control (FPRBAC) for access control at fog nodes, a mobility management service to handle location requests at a region. In order to deploy our framework in practice, providing high availability of fog services and resources and up-to-date location services need to be taken into account to address the sensitive-response requirement. The experimental outcomes demonstrated the feasibility and efficiency of the model.

References

[1] I. Consortium, S. Schrecker, H. Soroush, and J. Molina, *Industrial Internet of Things Volume G4: Security Framework*: CreateSpace Independent Publishing Platform, 2016.

[2] L. Chen and D. B. Hoang, "Active data-centric framework for data protection in cloud environment," in *ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems*, pp. 1-11, 2012.

[3] C. Liu, J. Chen, L. T. Yang, X. Zhang, C. Yang, R. Ranjan*, et al.*, "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, pp. 2234-2244, 2014.

[4] C. Dsouza, G. J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *2014 IEEE 15th International Conference on Information Reuse and Integration (IRI)*, pp. 16-23, 2014.

[5] R. Deng, R. Lu, C. Lai, T. H. Luan, and H. Liang, "Optimal Workload Allocation in Fog-Cloud Computing Towards Balanced Delay and Power Consumption," *IEEE Internet of Things Journal,* vol. PP, pp. 1-1, 2016.

[6] M. A. Hassan, M. Xiao, Q. Wei, and S. Chen, "Help your mobile applications with fog computing," in *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking - Workshops (SECON Workshops)*, pp. 1-6, 2015.

[7] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," in *2015 6th International Conference on the Network of the Future (NOF)*, pp. 1-3, 2015.

[8] Y. Wang, T. Uehara, and R. Sasaki, "Fog Computing: Issues and Challenges in Security and Forensics," in *2015 IEEE 39th Annual Computer Software and Applications Conference (COMPSAC)*, pp. 53-59, 2015.

[9] D. Dolev and A. C. Yao, "On the security of public key protocols," presented at the Proceedings of the 22nd Annual Symposium on Foundations of Computer Science, 1981.

[10] G. Liu, H. Shen, and L. Ward, "An Efficient and Trustworthy P2P and Social Network Integrated File Sharing System," *IEEE Transactions on Computers,* vol. 64, pp. 54-70, 2015.

[11] T. Nguyen, D. Hoang, and A. Seneviratne, "Challenge-response trust assessment model for personal space IoT," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pp. 1-6, 2016.

[12] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *Computer,* vol. 29, pp. 38-47, 1996.

[13] A. EC2. (2014). *Amazon Elastic Compute Cloud.* Available: http://aws.amazon.com/

[14] fogproject. (2016). *fogproject.* Available: https://fogproject.org/

[15] GCM. (2014). *Google Cloud Messaging for Android.* Available: https://developer.android.com/google/gcm/index.html

[16] T. D. Dang, D. Hoang, and P. Nanda, "Data Mobility Management Model for Active Data Cubes," in *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 750-757, 2015.