International Journal of Innovative Research in Scientific Engineering and Technology-ijirset
VOLUME 1 ISSUE 1, MAY 2018 ISSN: 2XXX-XXXX
WWW.IJIRSET.ORG

Fog Challenges KMIP Solutions

[1]Aarshiya Khandelwal,
[2]Arti Harde,
[3]Bhuvaneshwari Iyer,
[4]Kajal Shirsath,
[5]Yashi Gupta
Cummins College of Engineering for Women,
Savitribai Phule Pune University Pune, India.[1,2,3,4,5]

Abstract : Fog is an attractive target for cyber-criminals due to high volumes of data throughput and the likelihood of being able to acquire sensitive data from both Cloud and IoT devices. Fog Computing today has many challenges out of which for communication, data security and wireless security challenges, encrypted communication and secure key management can be a possible solution. Some of the fog challenges which can be solved using KMIP are presented in this paper. This paper also investigates an application scenario and conducts IOT device authentication, F2F Communication and Task Scheduling of Fog Nodes. This paper generates more use-case scenarios for Fog Computing with secure and faster experience.

I. INTRODUCTION

Cloud computing technologies are becoming increasingly important since they provide a wide range of beneficial properties such as on-demand self-services, resource pooling, rapid elasticity, etc. Over the years, the cloud technology has matured enough with its increased popularity. But this increase in its popularity is increasing its challenges like Security, Communication with other clouds, Huge Data, Resource Management leading to increased latency[1]. In order to overcome these challenges new technologies, fog and edge[2] have been proposed. Fog Computing is a virtualized platform that provides compute, storage, and networking services between the end devices. and it has some striking advantages like Low latency and location awareness, Mobility. Inspite of these benefits due to fog computing , there are certain challenges like [3] Device Authentication on Fog Level, Interoperability between different fog vendors , Scheluding tasks, Trust Management.All of these challenges can be solved by the use of Key management interoperability protocol (KMIP). The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. [4] This paper is organized as follows. In the second section we introduce how some of the challenges of Fog Computing paradigm can be solved using KMIP. The following section takes a close look at a few issuesof Fog computing. In the fourth section we have taken up a use case scenario of Bus Transport system to depict the association of KMIP to solve fog computing challenges.

II. LITERATURE REVIEW

2.1 SECRET-KEY CRYPTOGRAPH

In secret-key cryptograh,both the communicating parties use the same key to encrpyt and decrpyt the message.Before encrypted data can be sent both the parties must agree on the cryptographic algorithm that will be used by them for encryption and decryption.

2.2 PUBLIC-KEY CRYPTOGRAPH

It is a scheme that consists of two unidentical keys namely : Public and Private Key.Each of them performs a unique function. Generally,Public key is used for encryption and private key is used for decryption.Public keys are shared,since they are too big to managed, they are stored on Digital certificates for secure transport and sharing.

2.3 DIGITAL CERTIFICATE

A digital certificate is an electronic passport that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate is sometimes also referred as public key certificate.

2.4 KMIP

The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol.It defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. KMIP also allows for clients to ask a server to encrypt or decrypt data, without needing direct access to the key.

2.5 FOG COMPUTING

Fog computing, also known as fog networking or fogging, is a decentralized computing infrastructure in which data, compute, storage and applications are distributed in the most logical, efficient place between the data source and the cloud.It extends the cloud services to the edge of network, and makes computation, communication and storage closer to edge devices and end-users, which aims to enhance low-latency, mobility, network bandwidth, security and privacy.

II. CHALLENGES IN FOG AND THEIR KMIP SOLUTIONS

The KMIP Server will be on cloud and each fog node belonging to that cloud will have its own Public and Private Keys. Using these keys, KMIP Server will generate unique identifier for each fog which will be stored on cloud. This identifier will be used for Fog-to-Cloud(F2C) as well as Fog-to-Fog(F2F) Communication. Following are some of the challenges that can be solved using KMIP.

3.1 DEVICE AUTHENTICATION ON FOG LEVEL

Authentication of IOT device trying to connect a fog needs to be done at fog level[3]. In current senario any device can be added in fog without any kind of authentication for that device. Key Management Interoperability Protocol(KMIP) will provide authorized access for devices when they try to connect with fog. When new device tries to connect a fog, fog will check whether Signature key from Digital certificate of that device, which is issued by a Certification Authority (CA) is stored in the cloud or not , if it is already present it means access through that particular device is authenticated i.e it has an authorized access . But if it is not there in cloud then fog will first authenticate the device by checking its digital certificate

3.2 IINTEROPERABILITY BETWEEN DIFFERENT FOG VENDORS

The devices used by different IOT devices getting connected to the fog network will be different having different security protocols. Different device models from same vendor may also have different security protocols. Interoperability protocol is needed for all the devices to run on Fog. KMIP can manage different Key Server of same or different vendors from it. [5] shows KMIP Server Test Results as of Jan 2017.

3.3 SCHEDULING TASKS

Scheduling tasks in fog computing is complex and difficult [6]. This problem can also be solved using KMIP. The KMIP server will be on cloud. And the fog node which needs dividing and scheduling tasks among different fog nodes needs to send request to cloud. Upon which the KMIP server will schedule the tasks for different fog nodes.

3.4 TRUST MANAGEMENT

Whether an unknown fog is trying to access the cloud is a situation where Trust Management is required as described in [7]. This can be detected using KMIP. KMIP server has a unique identifier stored for each of its recognized fogs. When an unknown fog will try to access the cloud, its identifier can be obtained using its keys and can be determined that it is not authorized to access the cloud. Necessary methods can be taken to stop that fog.

IV. EXAMPLE SCENARIO

This section presents a scenario in Fog Computing on Local Bus Transport within a city. Under the proposed network shown in Fig. 1, we will investigate the model of task scheduling, device authentication and F2F Communication. In the scenario, a city is divided into multiple fog network areas and the fixed bus route and schedule of all the buses traveling in the city is already stored in the cloud. And as soon as a bus starts from its first station, the route of that bus is loaded in the corresponding fog network area. Its location, speed, etc information is sent to that fog which verifies whether the bus is on time or if it has stopped due to some failure. As the bus moves, from one fog area to another, its information should also be sent to corresponding fog area which will check its details and communicate it to the nest fog node as per route. If the bus reached successfully to its location i.e. last fog node on

checking found journey successful, then only the required information to be sent to cloud for storage. In case of failures, the passengers waiting in the next fog area for the bus, should get information about the bus status and also the information to be sent to the Bus Transport Authority. And then the required information to be stored on cloud. Here, When the bus starts, its starting information will be sent from the bus' device to its fog node after shared key authentication of device at fog level itself. Then from the fog the request data is encrypted after its public key cryptography and sent to cloud where it will be decrypted. The cloud will then load the bus' route, schedule and other information onto the fog node ,after its public key encryption, which requested for the data. All this keying is managed by the KMIP Server. After this, the KMIP server, using this information, will schedule, the fog nodes that will act in that journey. When bus during its journey travels through one fog node area and enters into next fog node(as scheduled by the KIMP Server) area, the previous fog node returns its task status as completed. The previous node will send the bus data to its next node to do the process and will delete the data from itself. If a bus does not reach required destination within time due to some reason, the fog node will return failure and the situation can be analyzed. Depending upon the bus failure reason, the required information can be sent to the users waiting on all the next bus stops, by sending the information to next scheduled fogs after its public key encryption.

V. CONCLUSION

This paper has focused on Security and interoperability challenges in fog computing like device authentication on Fog Level, Interoperability between different fog vendors , Scheduling tasks, Trust Management and how these challenges can be solved by the use of Key management interoperability protocol (KMIP). In addition, we have given a case scenario of Bus Transport system to depict the association of KMIP to solve fog computing challenges. This framework can also be used in manufacturing industries, product-based industries and small organizations.

REFERENCES

[1] A. Shawish and M. Salama, Cloud Computing: Paradigms and Technologies. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 39–67. [Online]. Available: https://doi.org/10.1007/978-3-642-35016-0 2

[2] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, "Edge-centric computing: Vision and challenges," SIGCOMM Comput. Commun. Rev., vol. 45, no. 5, pp. 37–42, Sep. 2015. [Online]. Available: http://doi.acm.org/10.1145/2831347.2831354

[3] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective," IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586–2595, Nov 2017.

[4] Wikipedia, Key Management Inetroperability Protocol, https://en.wikipedia. org/wiki/Key Management Interoperability Protocol.

[5] Oasis, KMIP Key Management Inetroperability Protocol, 2017, https://www.oasis-open.org/committees/download.php/60192/ RSAc2017-KMIP.pdf.

[6] Z. Hao, E. Novak, S. Yi, and Q. Li, "Challenges and software architecture for fog computing," IEEE Internet Computing, vol. 21, no. 2, pp. 44–53, Mar 2017.

[7] T. S. Dybedokken, Trust Management in Fog Computing, 2017, https://brage.bibsys.no/xmlui/bitstream/handle/11250/2454375/ 16996 FULLTEXT.pdf?sequence=1.