SURVEY ON SECURITY ISSUE IN FOG COMPUTING FOR IOT ENVIRONMENT

[1]M .Sundarababu, [2]TD Ravi Kiran
[1,2]Assistant Professor,
[1] Department of Information Technology,
[1]PVP Siddhartha Institute of Technology, AP, India.

Abstract : Fog computing has been acquainted as an innovation with conquer any hindrance between remote server farms and Internet of Things (IOT) gadgets. Engaging an extensive variety of focal points, including enhanced security, diminished data transmission, and lessened inertness, haze is a fitting worldview for some IOT administrations. Here proposition is one of the security issue in IOT Environment is Authentication. Authentication in IOT has a few difficulties, for example, versatility and effectiveness. Customary confirmation is wasteful, and there is a requirement for a safe, adaptable, productive, and easy to understand answer for adapt to asset compelled IoT gadgets. Encouraged by Fog, a lightweight encryption algorithm can be connected between fog nodes and IOT gadgets to enhance the proficiency of the verification procedure. Moreover, fog could make an open door for validation in IOT gadgets, especially wearable gadgets.

***Index Terms* – Fog node, IOT, EU.**

I. INTRODUCTION

IOT networks are expected to provide reliable and secure services to the EUs. This requires all devices that are part of the fog network to have a certain level of trust on one another. Authentication plays a major role in establishing initial set of relations between IOT devices and fog nodes in the network. But this is not sufficient as devices can always malfunction or are also susceptible to malicious attacks. In such a scenario, trust plays a major role in fostering relations based on previous interactions. Trust should play a two-way role in a fog network. That is, the fog nodes that offer services to IOT devices should be able to validate whether the devices requesting services are genuine. On the other hand, the IOT devices that sends data and other valued processing

Requests should be able to verify whether the intended fog nodes are indeed secure. This requires a robust trust model in place to ensure reliability and security in fog network.Several works [1], [2] have been carried out to address the issue of trust in cloud computing environment. However, the unique challenges posed by fog computing environment necessitate revisiting this problem. Contrary to cloud computing environment, the need for a fog node to quantify past interactions with IOT devices in the form of trust/reputation is to be addressed.

Trust of a Fog Service: A potential EU in fog computing needs to ensure trust-level provided by the fog service providers. Therefore, it becomes necessary to answer:

How do we measure trust in a fog service and what are the main attributes that define the trust of the fog service?

The well-established trust models in cloud computing can be directly applied to fog computing due to lack of centralized management and mobility issues. Even though fog service provider offers attributes to measure trust of a service, at the same time, following question will arise as who will verify and monitor these attributes?

Among several trust-management models in cloud computing, reputation-based trust model is widely used in E-commerce services. Sometimes, reputation of a service provider is useful to choose among several service providers. As this service model strongly depends on overall opinion, it is not well well-suited in fog computing due to dynamic nature of EU devices and fog nodes in the fog layers. In addition, although, opinion-based model is helpful to choose a fog service, the reliability will become an important factor to be considered. Service Level Agreement (SLA) between a cloud service and EU has gained a significant attention in designing trust model in cloud computing. However, this SLA verification is limited when a user directly uses the cloud service, if the service is processed in the fog layer, a professional and licensed third-party should monitor SLA verification for the EUs and small organization that lack in technical capability.

II. B. AUTHENTICATION

Authentication of networked devices subscribed to fog ser-vices is one of the foremost requirements in fog network. To access the services of a fog network, a device has to_rst become part of the network by authenticating itself to the fog network. This is essential to prevent the entry of unauthorized nodes. It becomes a formidable challenge as the devices involved in the network are constrained in various ways including power, processing and storage. Traditional authentication mechanisms using certificates and Public-Key Infrastructure (PKI) are not suitable due to the resource constraints of IOT devices. Alternatively, authentication protocols like [2] have been proposed that is based on public-key infrastructure using multicast authentication for secure communications. In essence, like storage and processing services, authentication also needs to be offered as a service

whereby a device that needs them would have to get authenticated to the fog node with the help of the intermediary that may be the Certifying Authority (CA). This model of operations would prevent unauthorized nodes from becoming part of the fog network. In addition, this would also allow the fog nodes to restrict service requests from malicious/compromised nodes.
Dynamic fog nodes and EUs: Similar to mobility issue in EUs, the fog nodes also frequently join and leave the fog layer. It is required to ensure the uninterrupted service to the registered end users when a new fog node joins (or leaves) the fog layer. The EU must be able to authenticate themselves to the newly formed fog layer mutually. From EUs perspective, the complexity of registration and re-authentication phase without huge overhead.

III. SECURE COMMUNICATIONS IN FOG COMPUTING

The way processing and storage requirements can be offloaded to fog nodes, security requirements cannot be offloaded. Even IoT devices need to implement the minimum security requirements. Communications between IOT devices are considered to be taken care of the security practices in place for IOT communications. IOT devices interact with fog nodes only when they need to offload a processing or storage request. Any other interactions would not be considered as part of the fog environment as such communications would happen as part of the network. These fog nodes interact with each other when they need to effectively manage network resources or to manage network itself. They may even operate in distributed manner to perform a specific task. To secure communications in a fog computing environment the follow-ing communications between these devices are to be secured:

1) Communications between constrained-IOT devices and fog nodes and
2) Communications between fog nodes.

Usually, an IOT device can initiate communication with any of the fog nodes in the fog network requesting for a processing or storage requirement. In fact the IOT device may not even be aware of the existence of the fog network; therefore messages sent by such a device cannot be secured by using symmetric cryptographic techniques. Alternatively, asymmetric key cryptography has its set of challenges that are unique to IOT environment. Maintaining the PKI that is required to facilitate secure communication is one of the major challenges. Other challenges include minimizing the Message overhead keeping in mind the constrained environment in which the IOT devices operate. Communications among fog nodes requires end-to-end security as nodes involved in multi-hop path may not be trust worthy.

IV. D. END USER'S PRIVACY

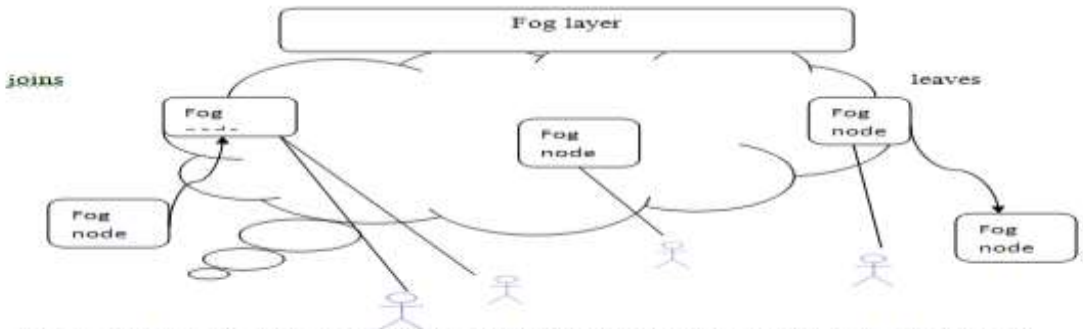
Fog computing lies on the computational power of distributed nodes for reducing the total pressure of the data centre. In fog computing, privacy preservation is more challenging since fog nodes that are in vicinity with EUs may collect sensitive data concerning the identity, usage of utilities, e.g. smart grid or location of end users compared to the remote cloud server that lies in the core network. Moreover, since fog nodes are scattered in large areas, centralized control is becoming difficult. The compromise of an poorly secured edge node can be the entry point for an intruder to the network. The intruder once inside the network can mine and steal user's privacy data that is exchanged among entities. Increased communication among the three layers that constitute the fog architecture can also lead to privacy leakage. Location privacy, as discussed in [1], is one of the most important models for privacy, since the place of equipment can be linked to the owners. Since fog clients offload its tasks to nearest fog nodes, location, trajectory and even mobility habits can be revealed from an adversary. User habits can also be revealed from an adversary by analyzing his/her usage habits of fog services, e.g. smart grid. Smart meters' readings can disclose information about the time that the house is empty or even the TV programs that the EU prefers to watch. As new systems that are based on fog computing are pro-posed, new privacy challenges also arise. Ni et al. [2] pro-pose the idea of Fog-based Vehicular Crowd Sensing (FVCS).
In this system vehicular fog nodes can temporarily store and analyze all sensing data, that is ploaded by vehicles, in order to provide local services, taking the role of central cloud servers. By exchanging data about local situation, e.g. traffic jam, each car can help in optimizing several parameters of the vehicle network, exposing on the same time sensitive data about their owners regarding their location, trajectory etc. The anonymization of the information and the tasks of different entities that need to be done for each task could put a heavy burden on pseudonym management for both customers and the cloud [2].Even if systems are well designed and securely implemented, they can expose critical information through their side channels. Possibilities of information leakage via side channels are pointed out in the literature and include electromagnetic radiation, observably timing of certain activities, power consumption of certain devices and even light acoustic or heat emanations from equipment All these privacy issues arise the need for more sophisticated solutions and countermeasures. Existing recent works are presented in the following sections.

V. MALICIOUS ATTACKS

Fog computing environment can be subjected to several malicious attacks and without proper security measures in place may severely undermine the capabilities of the network. One such malicious attack that can be launched is a Denial-of-Service (DoS) attack. Since majority of the devices connected to the networks are not mutually authenticated, launching a DoS attack becomes straight forward. The attack may be launched when devices that are connected to IOT network request for innate processing/storage services. That is a compromised or malfunctioning node can make repeated processing/storage requests to a fog node thereby stalling requests made by legitimate devices. The intensity of such an attack raises manifold when a set of nodes simultaneously launch this attack. Another way to launch this attack is to spoof addresses of multiple devices and send fake Processing/storage requests. Existing defense strategies of other types of networks are not suited for fog computing environment mainly due to the openness of the network. The first major challenge is the size of the network. Potentially, hundreds and thousands of nodes forming an IOT network avail the services of fog/cloud to overcome computation and storage limitations and also enhance performance. Since all these devices cannot be authenticated by fog nodes, they may rely on trusted third party like a certification authority that issues some form of credentials to ensure device authentication. But, the existence of such credentials only allows the processing fog node to verify whether the request has been generated by a legitimate node. Since a compromised node is a legitimate part of the network, all such requests would be entertained. On the other hand, restricting connectivity to the network or _altering the requests made by IOT devices nullify the motivation of existence of fog nodes. Spoofing of addresses is also relatively easier as the address space.

VI. PRAPOSED PROBLEM STATEMENT

Here proposal is one of the security issue in IOT Environment is Authentication .Authentication in IOT has several challenges such as scalability and efficiency. Traditional authentication is inefficient, and there is a need for a secure, scalable, efficient, and user-friendly solution to cope with resource-constrained IOT devices. Mutual authentication among dynamic fog nodes and EUs is one of the research challenges in fog computing environment. The EUs roam randomly over the network. Besides a fog node also frequently join and leave the fog layer. Thus mutual authentication EU and fog node is challenging issue.
My primary focus on how the EU is able to mutually authenticate with new fog node that joins the network without any significant increase in overhead. My contribution is an efficient and secure authentication scheme that allows any EU and any fog node to authenticate each other. The EU stores only one long live master secrete key, by which the EU mutually authenticates with any fog node managed by the cloud service provider.



How to design a low complexity based authentication and key management between end users and fog node in a scalable fog network.

VII. CONCLUSION

Fog computing has been acquainted as an innovation with conquer any hindrance between remote server farms and Internet of Things (IOT) gadgets. Engaging an extensive variety of focal points, including enhanced security, diminished data transmission, and lessened inertness, haze is a fitting worldview for some IOT administrations. Here proposition is one of the security issue in IOT Environment is Authentication. Authentication in IOT has a few difficulties, for example, versatility and effectiveness. Customary confirmation is wasteful, and there is a requirement for a safe, adaptable, productive, and easy to understand answer for adapt to asset compelled IoT gadgets. Encouraged by Fog, a lightweight encryption algorithm can be connected between fog nodes and IOT gadgets to enhance the proficiency of the verification procedure. Moreover, fog could make an open door for validation in IOT gadgets, especially wearable gadgets.

REFERENCES

[1].”Fog Computing for the Internet of Things: Security and Privacy Issues” by Arwa Alrawais,Abdulrahman Alhothaily,Chunqiang Hu, and Xiuzhen Cheng George Washington University, Published by the IEEE Computer Society 1089-7801/17/$33.00 © 2017 IEEE ,IEEE INTERNET COMPUTING.

[2]. "Security and Privacy in Fog Computing: Challenges" by Mithun Mukherjee,Rakesh Matam,, Lei Shu, Eandros Maglaras,Mohamed Amine Ferrag, Inhumane Choudhury,And Vikas Kumar published in IEEE Access oct-2017 ,Vol5,2017.

[3]. Saad Khan, Simon Parkinson and Yongrui Qin published paper "Fog computing security: a review of current applications and security solutions" in Journal of Cloud Computing: Advances, Systems and Applications.

[4]. Data Center Companies. Accessed: Jul. 23, 2017. [Online]. Available: https://www.datacenters.com/directory/companies.