International Journal of Engineering Technology and Management Sciences[IJETMS]

Website: ijetms.in Issue:1, Volume No.2, January 2018

# Novel Perspective on Security And Privacy Mechanisms in Fog Computing

Manas Kumar Yogi[1] , Mahesh Reddy[2], Himatej[3]

[1] Asst. Prof.,Department Of CSE,Pragati Engineering College

[2,3] B.Tech III Year Student,Dept. Of CSE,Pragati Engineering College

Surampalem,Dist:East Godavari,A.P.

[1]manas.yogi.@gmail.com

[2] mahesh36453reddy@gmail.com

[3] himatejy@yahoo.com

***Abstract*— This paper sincerely attempts to summarize the current technological perspective of security challenges posed in the domain of fog computing. Our paper discusses the operational intricacies of security as well as privacy concern due to the highly flexible nature of fog nodes. In such an dynamic nature providing sustainable security requires quite a effort while designing the security principles. We have presented a novel review of existing techniques and also advocated a modified approach for access control. We have additionally presented the mechanism of authentication and privacy control for the fog users by deployment of trust management system.**

***Keywords*—, Access Control, Authentication, Fog, IOT, Privacy, Security**

## I. INTRODUCTION

Fog computing is taken into account as associate extension of the cloud computing paradigm from the core of network to the sting of the network. it's an extremely virtualized platform that has computation, storage, and networking services between end devices and traditional cloud servers. Fog computing is defined as "a situation wherever a large range of different (wireless and generally autonomous) omnipresent and decentralized devices communicate and cooperate among them and with the network to perform storage and process tasks without the involvement of third parties. These tasks are for supporting basic network functions or new services and applications that run during a sandboxed atmosphere. Users leasing a part of their devices to host these services get incentives for doing therefore. Though this definition continues to be debatable, we have a tendency to powerfully agree that we want a definition to differ fog computing from connected technologies since anyone of these underlying techniques could cover a false read on fog computing.

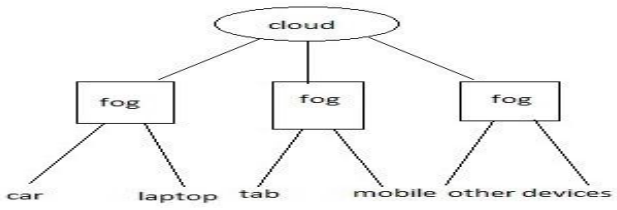


Fig. 1. Representing cloud and fog

Due to set at the edge of net, fog network is heterogeneous. The duty of fog network is to attach each element of the fog. However, managing such a network, maintaining connection and providing services upon that, particularly within the eventualities of the internet of Things (IoT) at massive scale, isn't simple.

## II.SECURITY ASPECTS IN FOG

### A. Authentication

Current trusty Platform Modules (TPMs) are ill suited for cross-device situations in trustworthy mobile applications as they hinder the seamless sharing of information across multiple devices.By design, TPMs provide a hardware root of-trust certain to one, standalone device. TPMs return equipped with secret writing keys whose private parts never leave the TPM hardware chip, reducing the chance those keys could also be compromised. the strain between single-device TPM guarantees and also the would like for cross-device sharing makes it tough for trustworthy applications to deal with multi-device eventualities. This paper reviews one, easy style amendment to the TPM,

referred to as cTPM.At producing time, TPM chips are provisioned with some of public/private key-pairs for cryptography (i.e., digital signatures and uneven encryption). The TPM style guarantees that the non-public keys of those root key-pairs never leave the TPM, thereby reducing the possibility of compromise. TPMs also can generate public/private key-pairs with non-public keys keep within the TPM's NV storage. However, TPMs have restricted NV storage and therefore cannot store several such key-pairs.

Limitation 1: Cross-Device information Sharing

Limitation 2: Trust Clock

Limitation 3: NV Storage

To address these limitations, we tend to propose cTPM, a modification to the TPM style that has an extra cloud management domain. This domain offers a similar practicality because the owner domain except that its primary seed is additionally shared with the cloud. Sharing the seed with the cloud permits each cTPM and also the cloud to come up with a similar cloud root key.

Combining the cloud root key with remote storage lets cTPM:

1) higher share information via the cloud,

2) have access to a sure period of time clock, and

3) have access to remote NV storage that supports an outsized amount of storage, and high frequency writes. cTPM's style facilitates information sharing. The preshared primary seed lets the cloud effectively act as a PKI. The cloud and also the device's TPM will use this shared secret to inscribe and evidence their messages to every different. The identity drawback has currently been "pushed" to making sure that the cloud primary seed is shared firmly between cTPM and also the cloud. this primary sharing step ought to be done at cTPM producing time once the cTPM's 3 different primary seeds square measure provisioned.

B. Architecture :

cTPM consists of 2 totally different parts, one running on the device and also the different within the cloud. each parts implement the total TPM a pair of.0 software package stack with the extra cTPM options. This ensures that every one cloud operations created to the cTPM strictly follow TPM linguistics, and therefore we tend to don't have to be compelled to re-verify their security properties. On the device-side, the cTPM software package stack runs within the TPM chip, whereas the cloud runs the cTPM software package within a VM. On the cloud-side, the NV storage is regular cloud storage, and also the timer offers a period of time clock operate. The cloud-side cTPM software package reads the civil time upon each initialisation and uses NTP to synchronize with a reference clock. once running within the cloud, cTPM resources (e.g., storage, clock) needn't be encapsulated in hardware as a result of the OS running within the VM is assumed to be sure. In distinction, the device's OS is untrusted, and therefore the cTPM chip itself should be ready to provide these resources in isolation from the OS.

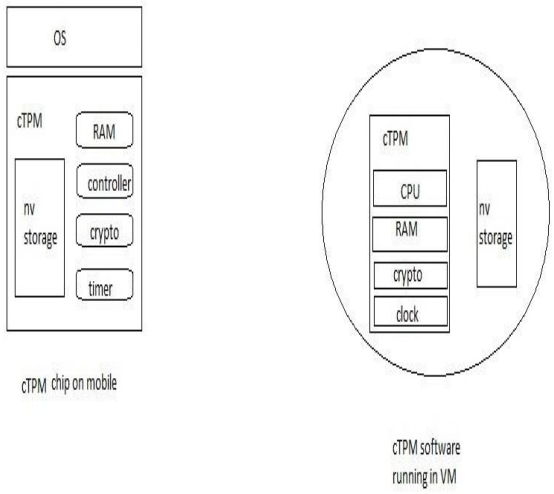


Fig. 2. cTPM Architecture

C.Access Control Mechanism In Fog Computing:

The design principles for operational aspects of access control have dependency with the service level agreements (SLA's). For cloud computing these SLAs are so designed to be neutral for all parties in concern. The degree upto which SLAs are in compliance matters much in fog computing due to the reason that fog users might not have complete trust in service providers. Hence to increase the level of trust and for trust level management activities a third party initiative can be considered to reasonably handle the trust management issue.

TABLE I . Representing access control issues

| | |
|---|---|
| Privacy violation | Fog decentralization may require data interchange between administrative domains |
| Coherency | A unique and coherent access control system |
| Context-awareness | support access control decisions |
| Resource restriction | Access control system should not drain power or resources from devices |
| Network availability | Access control should be able to provide a level of functionality even in case of network unavailability |
| Decision latency | The system should minimize time required to grant or deny a request |
| Management | Policy management, which includes the ability to create, update and delete policies |
| Accountability | Tracks concerning malicious activity should not be lost across administrative domains |

D. Modified Attribute-Based Access Control (Abac) Approach :

Attributes are characteristics, defined as name-value pairs, which can contain information about subjects, objects and context. Context attributes, or environmental conditions, allow ABAC implementations to be context-aware, thus making it an ideal candidate for fog applications, where context is a factor that affects the entire system behavior. Identity-based authentication is not a prerequisite for ABAC. In case, when needed identities can be used provided they have been assigned to subjects as attributes.To ensure certified exchanging of attributes, the utilization of proper attribute certificates has already been proposed in previous work. In an attribute-based access control system, authorization is performed according to a security policy that is mainly defined on the basis of subject and object attributes instead of any identities. Security policy refers to the set of rules, laws and practices that regulate how an organization manages, protects, and distributes sensitive information. Modified ABAC utilizes 3 sets of policies. Digital Policies (DP), Meta Policies (MP) Fog Trust Level Policy(FP). DPs signal the access control rules that access control system enforces. MPs are used for managing DPs. An example of MP is the definition of priorities that should be assigned for the case of conflicting DPs. Fog Trust Level Policy (FP) can supersede MP if the trust level reduces for a participating fog node.

The Fog Reference monitor (FRM) includes the Policy Resolution Point (PRP) and the Policy Imposition Point (PIP). Access decisions are made in PRP and are then injected into the PIP that applies them, thereby permitting or rejecting user access requests against objects. These decisions are based on DPs and corresponding MPs, FPs.

In the proposed modified ABAC implementation, fog security administrators initialize policies that are saved in a logical Policy Data Point (PDP). Policies can be initialized with the help of User Interface (UI) or any other technique (e.g. via a web service). We indicate PIP as logical policy as it is represented as a single component even though it can be implemented in a distributed way within the fog area. PDP comprises of all policy and attribute information for one or multiple domains and propagates policies to PRPs deployed mainly in fog area. A PIP applies access decisions and can be executed on every single device. For example, PIP can reside on a network switch, where it disables a port if attributes of a requestor user leads to a reject decision by a PRP located in a fog server. PIP does not need more computing resources to consume, since most of the required computation takes place in the PRP. At the fog node level, a hash table is used to store the id of PDPs along with linked list of corresponding PRPs.

For the sake of fog environment continuance and backup, PIPs can be attached to one or more PRPs. This can only be operational when all PRPs are simultaneously informed of any policy change. PRP policy synchronization requires a proper policy propagation control method. As mentioned above, MPs contain information for managing DPs. All policies are created, changed or removed by policy managers under the supervision of an administrative FP. In case of a single PRP, all changes in policies stored in a PIP can directly be spread to the PRP and then in no time be effective for the whole system. However, in case of distributed PRPs, where communication networks may impose delays due to outages or breakdowns, a change in the policy set (PIP) should be spread on basis of particular rules that consider factors like the current network

conditions as well as the changing level of fog trust. For instance, it may be decided not to send policy updates to any PRP unless all required PRPs are reachable and the fog trust level has a specific trust value.

To face such issues, we advocate the fair use of propagation rules represented by a hybrid policy set, called Propagation Policies (HPP). HPPs are policies that define how FP policies are constructed along with the procedure of updation of PIP policies, propagation to PRPs and exchange of access requests between PRPs. Apart from the initialization of the propagation of policies, proper care should be taken to securely transmit and verify the DPs and MPs. For this purpose, active research has already begun at scaling the definition and deployment of access rule certificates.

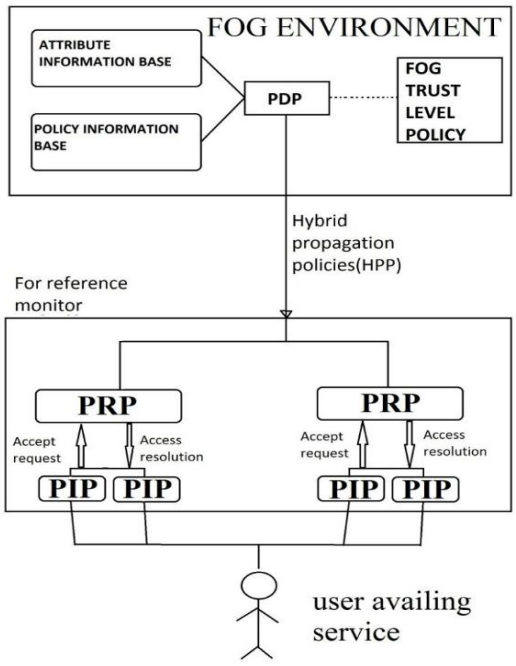


Fig. 3. Block diagram of modified ABAC method

## III. CONCLUSION

We conclude this paper by advocating the policy of fog security through distributed trust management and noting that the degree of security, privacy to enhance is a research challenge attributed to the diverse nature of participating elements in a fog environment. Fog computing is here to stay as well as leverage the societal needs which is a way towards revolutionizing the paradigm of distributed computing.

*References*

[1] C. Chen, H. Raj, S. Saroiu, and A. Wolman. ctpm: a cloud tpm for cross-device trusted applications. In NSDI, 2014.

[2] C. Dwork. Differential privacy. In Encyclopedia of Cryptography and Security. 2011.

[3] S. Kosta, A. Aucinas, P. Hui, R. Mortier, and X. Zhang. Think air: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In INFOCOM. IEEE, 2012.

[4] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen. Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. TPDS, 2012.

[5] H. Takabi, J. B. Joshi, and G.-J. Ahn. Security and privacy challenges in cloud computing environments. IEEE Security and Privacy, 2010.

[6] S. Yu, C. Wang, K. Ren, and W. Lou. Achieving secure, scalable, and fine grained data access control in cloud computing. In INFOCOM, 2010.