Volume 4, Issue 4, April 2019 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

Securing Fog Computing Using Shibboleth Identity Provider

Rushikesh B. Dhangare
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Prasad D. Joshi
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Dinesh E. Mali
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Pavan D. Manwar
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Ratan D. Deokar
Dept.of Information Technology
MET's Institute of Engineering, Nashik

Abstract- ***Fog Computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end users. We discuss the state-of-the-art of Fog computing and similar work under the same umbrella. Security and privacy issues are further disclosed according to current Fog computing paradigm. As an example, we study a typical attack, man-in the-middle attack, for the discussion of security in Fog computing. This paper is basically focusing on overcoming the security issues encountered during the data outsourcing from fog client to fog node. Advantages of Fog computing, and analyses its applications in ma series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks***.

Keywords— Cloud, Security, fog, privacy, Compute, Accountability Safe Management of Identity, Data Privacy

I. INTRODUCTION

CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things (IoT), to run directly at the network edge. In Fog computing, services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the „ground", creates automated response that drives the value. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.

Internet of Things is basically physically inter-connected objects. All physical objects connected with each other forms an IoT network. The connected physical devices are also embedded with different software, sensors and also have network connectivity which makes them able to share and access the information. Today's technology-oriented world has revolutionized the IoT network as each and every physical device is connected with each other. We have added Shibboleth also known as security and cross domain access control protocol between fog client and fog node for improved and secure communication between the fog client and fog node.

NEED OF FOG

In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current "pay-as-you-go" Cloud computing model becomes an efficient alternative to owning and managing private data centers for customers facing Web applications and batch processing .Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomes a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements. When techniques and devices of IoT are getting more involved in people's life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location awareness and low latency. Fog computing is proposed to address the above problem. As Fog computing is implemented at the edge of the network, it provides low latency, location awareness, and improves quality-of-services (QoS) for streaming and real time applications [2].

Shibboleth Protocol

Shibboleth frame work basically defines a set of collaboration between its providers in order to facilitate its users with Single-sign-On and attribute exchange processes. Shibboleth system includes two basic components: (a) Service Provider (SP), and (b) Identity Provider (IdP). Service provide and Identity providers are the architectural components of Shibboleth. The aforesaid shibboleth components are also referred as Target site and Origin site respectively.

The Shibboleth components mutually form a federation and facilitate the user in accessing the web resources securely . In order to develop the trust between service provider and identity provider, a public key is exchanged between them. User attributes that are provided by origin site are used on the target site. The decision is then made about all owing the user to access the desired source or not.

II. LITERATURE SURVEY

Variety of work has been done in IoT network and Fog computing for ensuring its security like, in. Huang et al. has proposed and implemented a model for fog computing to ensure the privacy of data in different applications. The implementation is done by using Raspberry Pi. Abdo has proposed a method for the reduction of latency in a mobile cloud environment where they have made the user authentication faster to decrease the delay. Different security and privacy challenges have been discussed and the author has also proposed a scheme for focusing these security issues using bloom filters and certificates. Fog computing has played an emerging role in IOT network. Its emergence has been discussed. A survey has been done on different concepts, applications and issues in Fog computing.

Nowadays Cross-domain access is gaining popularity andit's different pro- tocols are deployed in different organizations . To ensure that the intended purpose of protocols are being fulfilled, the cross domain access protocols must be checked against their envisioned properties. In order to check the protocol's correctness we take help of formal verification. Formal verification is an effective method to prove the protocol correctness, against some properties. In case of any issues in the system, formal verification is also aimed to target the issues to be known. Many of the protocols have been exposed with different security flaws ,Auth has been verified formally to check security issues if any. Formal methods basically involve modelling, analysis, and verification of the system. Formal verification has been used in finding out the flaws and thus improving the system. In work related to rule-based frame work has been done which is dedicated to the policies of RBAC model. Needham-Schroeder, Kerberos, and TNM protocol shave been analysed by the authors.

A Tool which issued in is Mur-phi which is used to analyse net- work having a large number of topologies. Malik et al. has used HLPN to model and analyse different VM based cloud management platforms .Miculan and Urban have given protocol formalization

in Alice-Bob notation and also in High-Level Protocol Specification Language (HLPSL). To check security flaws and attacks author has used AVISPA which is a verification tool for the analysis of security protocols. In another study Akhawe et al. has used Alloy model checker to formally verify the web security and authentication protocols. To discover out some identified or unidentified vulnerabilities of CSRF attacks author has modelled web authentication protocols which is a Kerberos based SSO web solution. The method tracked in is limited to only HTTP communication. Shibboleth framework basically defines a set of collaboration between its providers in order to facilitate its users with Single-sign-On and attribute exchange processes. Shibbole the system includes two basic components: (a) Service Provider (SP), and (b) Identity Provider (IdP).

Shibboleth framework basically defines a set of collaboration between its providers in order to facilitate its users with Single-sign-On and attribute exchange processes. Shibboleth system includes two basic components: (a) Service Provider (SP), and (b) Identity Provider (IdP). Service provide and Identity providers are the architectural components of Shibboleth. The afore- said shibboleth components are also referred as Target site and Origin site respectively. The Shibboleth components mutually form a federation and facilitate the user in accessing the web resources securely.

III. PROPOSED SYSTEM

Our proposed system to improve and secure communication and over- coming the security issues encountered during the data outsourcing from fog client to fog node. This system provide features for fog client such as location awareness, low latency, mobility support and To enhance interoperability by using different platforms by fog client.

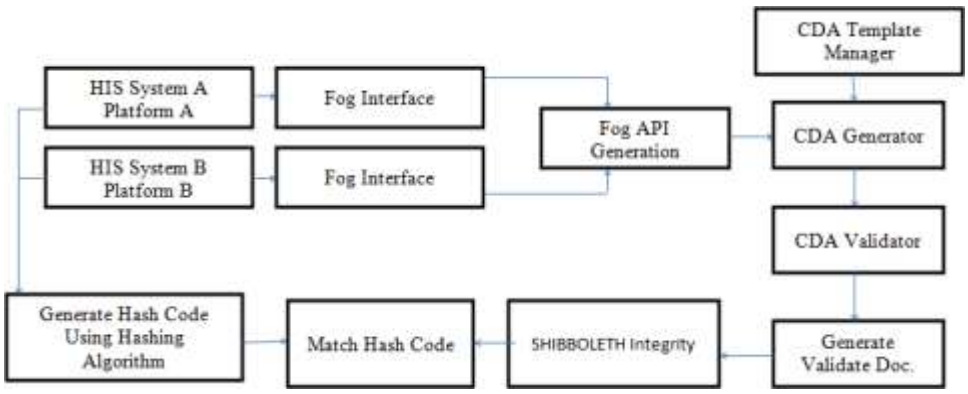
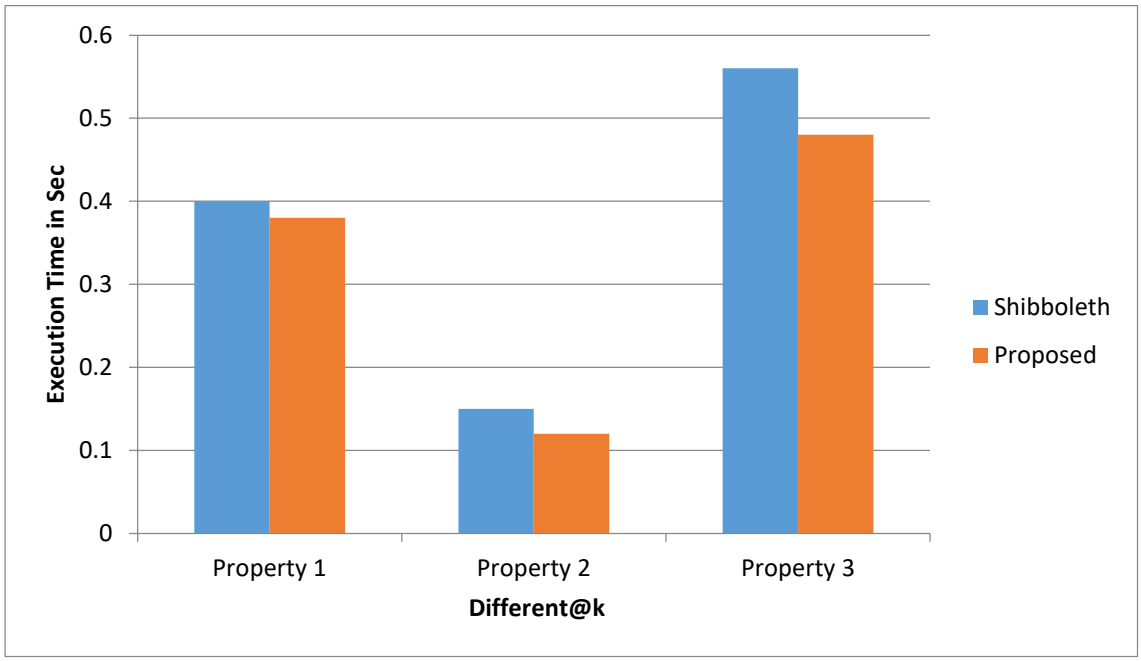


Fig -1: Proposed System

Security monitoring on the cloud is important, because computers sharing data are most readily available to an attacker. Without mechanisms in place to detect attacks as they occur, an system may not realize its security. There- fore it is vitally important that computers residing in the cloud are carefully monitored for a wide range of audit events. The auditing in a system con- sists of three steps. The first step is the attack has attempted on any node in system, secondly the attack is detected by the system by hashing algorithm after detection of attack the notifications are send to data owner. Due to this security is improved

IV. RESULTS



	Shibboleth	Proposed
Property 1	0.4	0.38
Property 2	0.15	0.12
Property 3	0.56	0.48

CONCLUSION

In this paper we have critically analyzed the Shibboleth protocol which is a widely used security protocol. This critical study has made us to propose 'Shibboleth based FogIoT network' which includes Shibboleth for ensuring security between Fog Client and Fog Node. As the number of HIE based on CDA documents increases, interoperability is achieved, but it also brings a problem where managing various CDA documents per patient becomes inconvenient as the clinical information for each patient is scattered in different documents. The CDA document integration service from our cloud server adequately addresses this issue by integrating multiple CDA documents that have been generated for individual patients.

REFERENCES

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ''Wireless sensor networks: A survey,'' Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002.
2. M. Chui, M. Löffler, and R. Roberts, ''The Internet of Things,'' McKinsey Quart., vol. 2, no. 2010, pp. 1–9, 2010.
3. S.Yi,C.Li,andQ.Li,''Asurveyoffogcomputing:Concepts,applications and issues,'' in Proc. Workshop Mobile Big Data, 2015, pp. 37–42.
4. J. B. Abdo, ''Authentication proxy as a service,'' in Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC), 2017, pp. 45–49.
5. L. Catuogno and C. Galdi, ''Interoperability between federated authentication systems,'' in Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), 2014, pp. 493–498.
6. T. Komura, H. Sano, N. Demizu, and K. Makimura, ''Design and implementationofWebforwardproxywithshibbolethauthentication,''inProc. IEEE/IPSJ11thInt.Symp.Appl.Internet(SAINT),Jul.2011,pp.321–326.
7. J.-L. A. Manan, Z. A. Khattak, and S. Sulaiman, ''Practicable unified security, trust and privacy (STP) framework for federated access management(FAM),''inProc.IEEE11thInt.Conf.Trust,Secur.PrivacyComput. Commun., Jun. 2012, pp. 1411–1416.

8. D.R.Cok,A.Stump,andT.Weber,‘‘The2013evaluationofSMT-COMP and SMT-LIB,’’ J. Autom. Reasoning, vol. 55, no. 1, pp. 61–90, 2015.

9. D. Chistikov, R. Dimitrova, and R. Majumdar, ‘‘Approximate counting in SMT and value estimation for probabilistic programs,’’ in Tools and Algorithms for the Construction and Analysis of Systems. Springer, 2015, pp. 320–334.

10. K. Ashton, ‘‘That ‘Internet of Things’ thing,’’ RFiD J., vol. 22, no. 7, pp. 97–114, 2009. [11] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, ‘‘Smart objects as building blocks for the Internet of Things,’’ IEEE Internet Comput., vol. 14, no. 1, pp. 44–51, Jan./Feb. 2010.

11. J. A. Stankovic, ‘‘Research directions for the Internet of Things,’’ IEEE Internet Things J., vol. 1, no. 1, pp. 3–9, Feb. 2014.

12. R. Want, B. N. Schilit, and S. Jenson, ‘‘Enabling the Internet of Things,’’ Computer, vol. 48, no. 1, pp. 28–35, 2015.

13. L. Coetzee and J. Eksteen, ‘‘The Internet of Things—Promise for the future? An introduction,’’ in Proc. IST-Africa Conf., 2011, pp. 1–9.

14. A. Botta, W. De Donato, V. Persico, and A. Pescapé, ‘‘On the integration of cloud computing and Internet of Things,’’ in Proc. Int. Conf. Future Internet Things Cloud (FiCloud), 2014, pp. 23–30.

15. A.Nenadic,N.Zhang,J.Chin,andC.Goble,‘‘FAME:Addingmulti-level authentication to shibboleth,’’ in Proc. 2nd IEEE Int. Conf. Grid Comput. e-Sci., Dec. 2006, p. 157. [17] X. D. Wang et al., ‘‘Shibboleth access for resources on the national grid service (sarongs),’’ in Proc. 5th Int. Conf. Inf. Assurance Secur. (IAS), vol. 2. 2009, pp. 338–341.

16. M. Hatala, T. M. T. Eap, and A. Shah, ‘‘Federated security: Lightweight security infrastructure for object repositories and Web services,’’ in Proc. Int. Conf. Next Generat. Web Services Pract. (NWeSP), 2005, p. 6.

17. W. Ying, ‘‘Research on multi-level security of shibboleth authentication mechanism,’’ in Proc. 3rd Int. Symp. Inf. Process. (ISIP), 2010, pp. 450–453.

18. H. Wang and F. Shen, ‘‘Negotiation-based trust establishment for shibboleth,’’ in Proc. 1st Int. Conf. Inf. Sci. Eng. (ICISE), 2009, pp. 1773–1776.

19. S. U. R. Malik, S. U. Khan, and S. K. Srinivasan, ‘‘Modeling and analysis of state-of-the-art VM-based cloud management Platforms,’’ IEEE Trans. Cloud Comput., vol. 1, no. 1, p. 1, Jan. 2013.

20. K.JensenandL.M.Kristensen,‘‘ColoredPetrinets:Agraphicallanguage for formal modeling and validation of concurrent systems,’’ Commun. ACM, vol. 58, no. 6, pp. 61–70, 2015.

21. M. V. Bharti and S. Kumar, ‘‘Survey of network protocol verification techniques,’’ Int. J. Sci. Res., vol. 2, no. 4, pp. 228–231, 2012.

22. W. Mao and C. Boyd, ‘‘Towards formal analysis of security protocols,’’ in Proc. Comput. Secur. Found. Workshop VI, 1993, pp. 147–158.