Maintaining Fog Trust Through Continuous Assessment

Hasan Ali Khattak[1(✉)], Muhammad Imran[1], Assad Abbas[1], and Samee U. Khan[2]

[1] Department of Computer Science, COMSATS University Islamabad, Islamabad 44550, Pakistan
{hasan.alikhattak, mimran, assad.abbas}@comsats.edu.pk
[2] Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58105, USA
samee.khan@ndsu.edu

Abstract. Cloud computing continues to provide flexible and efficient way for delivery of services, meeting user requirements and challenges of the time. Software, Infrastructures, and Platforms are provided as services in cloud and fog computing in a cost-effective manner. Migration towards fog instigate new aspects of research for security & privacy. Trust is dependent on measures taken for availability, security, and privacy of users' services as well as data in fog as well as sharing of these statistics with stakeholders. Any type of lapses in measures for security & privacy shatter user's trust. In order to provide a trust worthy security and privacy system, we have conducted a thorough survey of existing techniques. A generic model for trustworthiness is proposed in this paper. This model yields a comprehensive component-based architecture of a trust management system to aid fog service providers to preserve users' Trust in a fog computing environment.

Keywords: Fog computing · Security and privacy · Trust management · Trustworthiness

1 Introduction

Internet is constituting as a significant driving force in development of future smart cities. Among major developments in distributed computing the most significant one has been provision of Software as a service (SAAS) to provide online services, Infrastructure as a service (IAAS) for reducing administration and maintenance cost, and Platform as a service (PAAS) to improve the overall provision of the development configurations. Besides availability, privacy as well information security is the basic requirement for a user's Trust [1]. Fog computing has been proposed as a future direction for provision of services and overall service enhancement [2]. Fog Computing otherwise known as edge computing basically leverages edge nodes for hosting the computational powers hence improving the quality of service as well as reducing latency. Key responsibilities of fog service providers are safety, physical security, and reliable availability of computing resources. Trust management performs a key role and

Y. Xia and L.-J. Zhang (Eds.): SERVICES 2019, LNCS 11517, pp. 129–137, 2019.
https://doi.org/10.1007/978-3-030-23381-5_10

effects utilization, services reliability, and infrastructure as well in a fog computing environment [3].

Organizations are stimulating in the direction of fog computing as it is cost effective, manageable for different time critical requirements and relocating their conventional systems on fog. Different fog deployment models such public, private as well as hybrid fog computing architectures along with on-site and off-site fog computing is a popular model for latency prone computing applications [4].

The fundamental characteristics of a secure computing system include confidentiality, integrity, availability, non-repudiation and authentication [5, 6]. Availability of application security systems and standards in the cloud anticipates ease of use to its end users. However, they do not serve as the only feature of a fog computing trust provisioning system.

A trustable Trust Provisioning System ought to anticipate the vital characteristics for inception of trust along with Trustworthiness [7]. A user's trust can be acclaimed by supplying an invariant availability, privacy and security management techniques in fog environment. Smart city application scenario leveraging fog computing are controlled remotely thus providing service providers ease of access and management. Availability can be achieved by surplus resources on these surrogate servers. Similarly, providing legitimate and secure authentication as well as authorization to obscure users is laborious feat in itself [8, 9]. Significant contributions of this work are as mentioned below:

1. Overview of Existing Trust Management Models
2. Requirements for Trust Management in Fog
3. Proposing Generic Trust Management Model
4. Research Issues and Questions for Trustworthiness

The organization of rest of the manuscript is structured in following these notable sections, that are as follows; In Sect. 2, the paper discusses background and basic terminologies of fog as well as cloud computing. Threats and vulnerabilities affecting fog computing are covered in Sect. 3. Related work on Trust and Trustworthiness establishment is covered in Sect. 3.1. Brief discussion of components of fog computing and trust in fog is carried out in Sect. 5.1. Research questions and related work are described in the Sects. 4 and 5, respectively. Proposed framework is concluded in Sect. 6 along with future directions.

2 Background

Delivery of application and softwares through cloud computing is done via Software as a Service (SaaS) for end users [10]. Online compilers, online image manipulation tools, Online Office suits are all famous examples of SaaS. The users, through their authorized credentials are able to connect to the services and use according to their respective agreements. Here the users don't having any kind of authority on fog or cloud authorizations.

Platform as a Service (PaaS) can be described as allocation of an operating system and clusters of programming languages and their development tools to create and deploy customized applications and services. Microsoft Azure and Google Compute

Cloud are some of the significant examples. Similarly, PaaS permits end-users to have command on application design. However, it doesn't provide them the complete authority over the fog or its physical infrastructure [11].

Infrastructure as a Service (IaaS) provides consumers with the straight access to storage, processing, and other similar computing resources, also permitting them to configure these resources and then run operating systems and software on them. Few other notable examples of IaaS are IBM 's Blue cloud and Amazon's elastic compute cloud (Fig. 1).

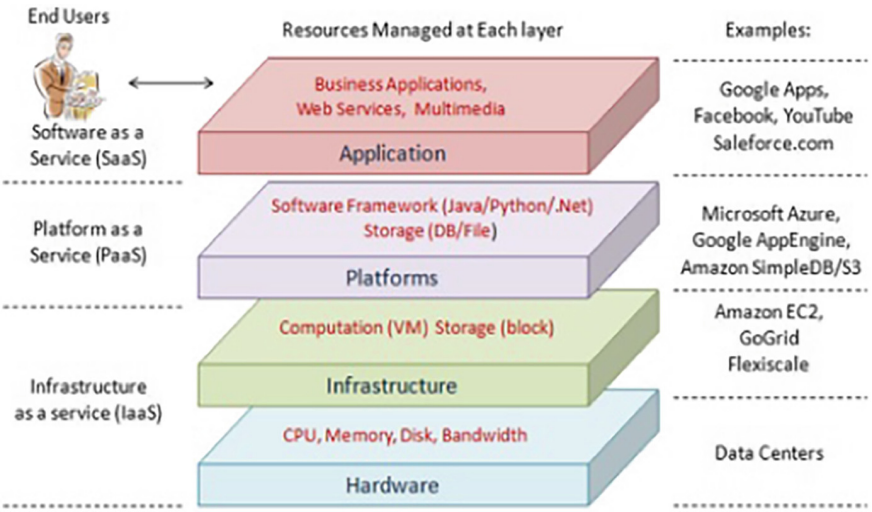

Fig. 1. Fog architectures and services [12]

Fog computing based services are being rendered by a distinct CSPs (Cloud Service Providers). Table 1 contains the list of services and their providers.

Table 1. Cloud services and providers

SaaS	CVM Solutions, Google Apps, Gageln, Host Analytics, Knowledge Tree, Reval, Exoprise Systems, Taleo, NetSuite, Microsoft Office 365, Salesforce.com, Rackspace, Antenna Software, Cloud9 Analytics, IBM and LiveOps
PaaS	Amazon AWS, IBM, Google Apps, Microsoft Azure, Intuit, Netsuite, SAP, SalesForce, WorkXpress, and Joyent
IaaS	OpenStack, Amazon Elastic Compute Cloud EC2, Rackspace, Bluelock, CSC, IBM, Savvis, GoGrid, VMware, Citrix, Terremark, BluePoint and Joyent

3 Fog Computing Security Phenomenon

Fog computing environments contains many components including hardware as well as software which are utilized in order to process huge amounts of data. These can be classified into services or applications, devices and their respective communications as shown in Fig. 2.

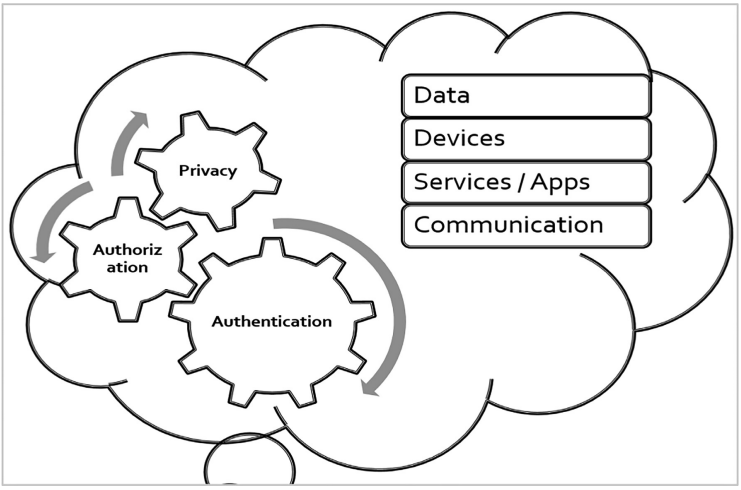

Fig. 2. Fog security phenomenon

Similarly, trust can be attained only by contributing in information security and privacy expedients, i.e., authorization, authentication and privacy [10, 13]. A trustable trust can be gained by pertaining means for Authorization, Authentication, and Privacy (AAP) at every step and about all the components in the environment. A trustable trust will be delivered even if a person is in a LAN, IoT, WoT, distributed computing and even in fog computing environment [14].

3.1 Trust Concepts

Trust: Trust is an individual's goal for acquiring vulnerability of a trustee, based upon the positive expectancy of their actions.

Trust Establishment: Trust establishment is a procedure and has responsibility of evaluation, maintenance, representation, and distribution of the trust between nodes.

Trust Management: Now, Trust management is presented by Blaze et al. [15] as a consolidated process to specify and interpret security policy guidelines, relationships and their respective credentials that permit uninterrupted authorization of security oriented actions.

Trustworthiness. Trustworthiness on the other hand is an acquired attribute because of the parameters revealed by the respected trustees in a specific environment. Mayer et al. [16], have pointed out 3 significant characteristics which helps us in establishment of the basis for expansion of a trust framework [17]. In the trust development process, integrity, ability, and good will have been highlighted as the key roles of a trustees.

4 Research Questions

Fog computing encourages its stakeholders in many dimensions such as, time and space by achieving reliable connectivity and desirable latency. Flexibility and expandability regarding hardware resources are the main characteristics of fog computing. Efforts and economy of resources are well organized in fog computing. Attraction of users concerning fog computing infrastructure is based on the trust on the fog. The basic research queries to analyze users trust in fog are outlined as follows:

- Measuring Achieved User's trust
- Significance of system feedback on trust management.
- Advantages of sharing statistics affecting user's trust
- Tradeoffs between Trustable trust and Achievable trust
- Tactile Trustworthiness Establishment Matrices
- Feasibility of sharing the information regarding affected users' trust
- Relationship among Trust and Trustworthiness

5 Trust Management System Model

Trustable trust between applications, devices and their users is attained through reinforcing a basic trust management infrastructure. Trust Management Systems (TMS) can be classified into two functions i.e., trustworthiness establishment and most importantly trust establishment of fog modules.

Trust in fog is one of the most important characteristics however, it is also one of the difficult ones and hence, opening doors to many research domains. This paper introduces trust in general and then identifies trustworthiness in fog computing. Diverse cloud computing models are dispensed along with threats and vulnerabilities which each of them may experience. Moreover, a comprehensive list of research questions has been put forward, which results in main subsidy of this paper in form of a proposed Fog Trust Management System model which not only caters those research questions but also sets stone for future research in directions of establishing Trust as well as Trust Management.

Mainly trust in fog is dependent on the user's perception and acceptance of trust and on that trustworthiness of a fog resource can be judged. Trustworthiness of a system is established by means of generating statistics related to trust governance, trust assessment, trust evaluation, event logging and assessment sharing. User Feedback plays a vital role in not only gaining trust but also trustworthiness of any service provided. Trust Assessment sharing enhances the trustworthiness and will enable users to keep track of the services provided and as well as the trust level which service providers are offering. Though cloud service providers are obliged to ensure the availability of these statistics always, otherwise the whole trust phenomenon would be considered incomplete. Next comes the question how much trust will be considered trustable trust, which can be summed up to the top most level of possible achievable trust offered by the system and this is directly measured by the parameters of trust itself namely, Availability, Security and Privacy.

5.1 Trustworthiness

Trustworthiness is to be considered as the ability, benevolence, and therefore integrity of a trustee [18]. The procedures convoluted to inaugurate trustworthiness is outlined as follows:

Trust Governance. A central trust governance characteristic will yield a technique to establish procedures, policies, certification and decertification of artefacts in the cloud [19].

Trust Evaluation. Trust evaluation is the main component for developing trustworthiness of items that are being utilized in fog i.e., software along with hardware and their communication mediums.

Event Logging. The cloud monitoring can be gained successfully by event logging means which are held to manage and govern trust in the fog. Evaluation and recording of fog actions generated events are utilized in developing trustworthiness.

Trust Assessment. Trust assessment is sustained based on the event monitoring and trust evaluation. Dispensing of trust assessment outcomes with the Fog users is the force multiplier in developing trustworthiness.

Psychological Factors. Fog service providers always obtain some good or bad repute from their users. Reputation relies on the satisfaction of users regarding Service Level Agreements (SLAs) [20]. User's trust can easily be transfigured and rectified by these psychological factors.

Assessment Sharing. Finally Trust assessment is dispensed effortlessly through continuous dissemination of statistics on the overall trust situations. Trust assessment outcomes are handed out with the users of the fog, and validation procedure is held based on the feedback of users. When user satisfaction level is attained, and an honorable reputation is developed, trustworthiness is issued to the world (Fig. 3).

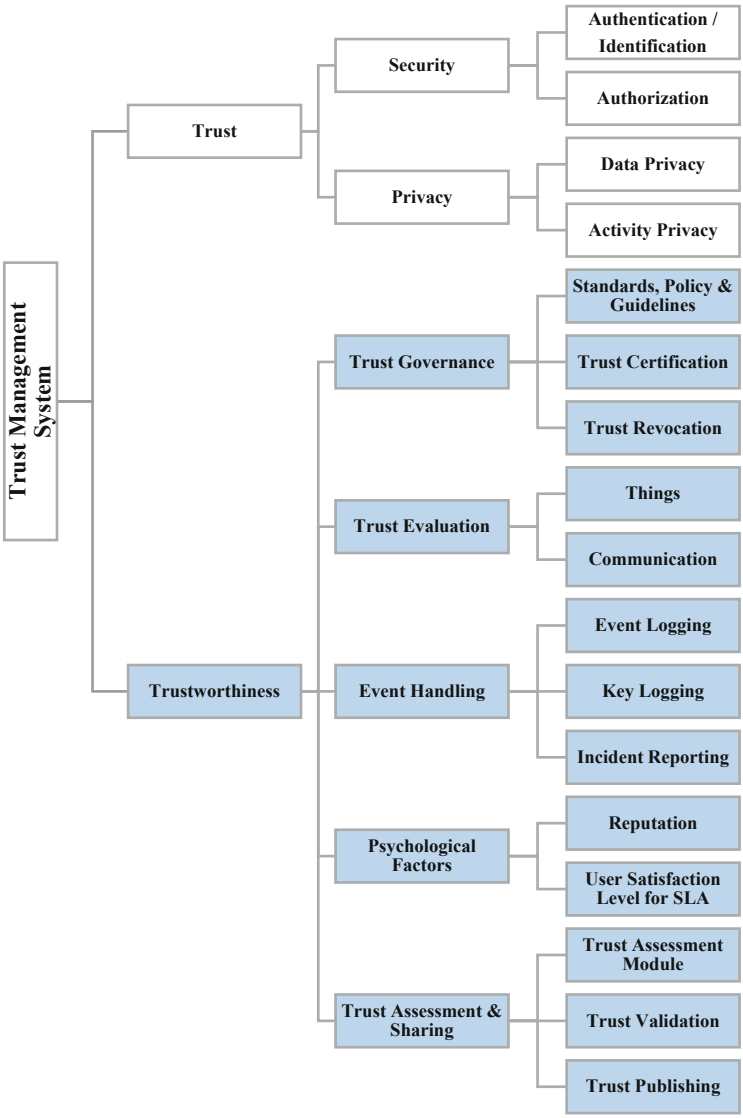

Fig. 3. Basic components of the proposed trust management system for fog

6 Conclusion and Future Directions

The model proposed for Trust Management System emphasizes the total functionality on the trustworthiness subsystem. This module covers all the basic components of the proposed system which are responsible for trust enabled governance, trust establishment, trust assessments, event logging as well as statistics sharing. Fog computing is often on public internet, which makes it essential to offer necessary privacy while

sharing these user statistics, one of many ways to implement this is anonymization of the events and data which is used in these statistics.

Though literature mentions trust and trustworthiness as the same thing but we consider then to be complementing each other, trustworthiness is something which needs a continuous assessment and enable fog users to choose to trust certain fog providers based on the prior experience of the existing users. The proposed model attempts to provide basis for a model trust management system which is responsible for providing trust as well as trustworthiness of a fog system. In future, we plan to offer the model workflow for this system by establishing the necessary technological aspects as well as a model implementation of the system.

Acknowledgements. This work has been partially supported through Startup Research Grant Projects No. (21 – 1122/SRGP/R&D/HEC/2016) by the Higher Education Commission (HEC) Pakistan. We also thankfully acknowledge the services from COMSATS University, Islamabad and would like to thank Dr. M. Ahmad, Dr. A Khan for supporting us in valuable technical and scientific aid.

The work of Samee U. Khan is based upon works supported by (while serving at) the National Science Foundation. Any opinions, findings, and conclusions or suggestions expressed in this manuscript are those of the authors and do not necessarily reflect the view of National Science Foundation.

References

1. Firdhous, M., Ghazali, O., Hassan, S.: Trust management in cloud computing: a critical review. arXiv Prepr. arXiv:1211.3979 (2012)
2. Cisco Systems. Fog computing and the internet of things: extend the cloud to where the things are, p. 6 (2016). Www.Cisco.Com
3. Arshad, H., Khattak, H.A., Shah, M.A., Abbas, A., Zoobia, A.: Evaluation and analysis of bio-inspired optimization techniques for bill estimation in fog computing. Int. J. Adv. Comput. Sci. Appl. **9**(7), 191–198 (2018)
4. Salman, O., Elhajj, I., Kayssi, A., Chehab, A.: Edge computing enabling the Internet of Things. In: Proceedings of IEEE World Forum on Internet of Things, WF-IoT 2015, pp. 603–608 (2016)
5. Rabai, L.B.A., Jouini, M., Ben Aissa, A., Mili, A.: A cybersecurity model in cloud computing environments. J. King Saud Univ. Inf. Sci. **25**(1), 63–75 (2013)
6. Almulla, S.A., Yeun, C.Y.: Cloud computing security management. In: 2010 Second International Conference on Engineering Systems Management and Its Applications (ICESMA), pp. 1–7 (2010)
7. Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G.: A subjective model for trustworthiness evaluation in the social internet of things. In: 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC), pp. 18–23 (2012)
8. Martucci, L.A., Zuccato, A., Smeets, B., Habib, S.M., Johansson, T., Shahmehri, N.: Privacy, security and trust in cloud computing: the perspective of the telecommunication industry. In: 2012 9th International Conference on Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), pp. 627–632 (2012)

9. Li, X., Du, J.: Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. IET Inf. Secur. **7**(1), 39–50 (2013)
10. Stojmenovic, I., Wen, S., Huang, X., Luan, H.: An overview of fog computing and its security issues. Concurrency Comput. Pract. Exp. **28**(10), 2991–3005 (2015)
11. Liang, G.: Automatic traffic accident detection based on the internet of things and support vector machine. Int. J. Smart Home **9**(4), 97–106 (2015)
12. Stojmenovic, I., Wen, S.: The fog computing paradigm: scenarios and security issues. In: Proceedings of 2014 Federated Conference on Computer Science and Information Systems, vol. 2, pp. 1–8 (2014)
13. Khan, S.U., Khan, R.: Content-location based key management scheme for content centric networks. In: Proceedings of 6th International Conference on Security of Information and Networks - SIN 2013, pp. 376–379 (2013)
14. Muzammal, S.M., et al.: Counter measuring conceivable security threats on smart healthcare devices. IEEE Access **6**, 20722–20733 (2018)
15. Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.D.: The role of trust management in distributed systems security. In: Vitek, J., Jensen, C.D. (eds.) Secure Internet Programming. LNCS, vol. 1603, pp. 185–210. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48749-2_8
16. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Acad. Manag. Rev. **20**(3), 709–734 (1995)
17. Noor, T.H., Sheng, Q.Z.: Trust as a service: a framework for trust management in cloud environments. In: Bouguettaya, A., Hauswirth, M., Liu, L. (eds.) WISE 2011. LNCS, vol. 6997, pp. 314–321. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24434-6_27
18. Colquitt, J.A., Scott, B.A., LePine, J.A.: Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. J. Appl. Psychol. **92**(4), 909 (2007)
19. Kang, D., Jung, J., Mun, J., Lee, D., Choi, Y., Won, D.: Efficient and robust user authentication scheme that achieve user anonymity with a Markov chain. Secur. Commun. Netw. **9**(11), 1462–1476 (2016)
20. Aazam, M., St-Hilaire, M., Lung, C.-H., Lambadaris, I., Huh, E.-N.: IoT resource estimation challenges and modeling in fog. In: Rahmani, A.M., Liljeberg, P., Preden, J.-S., Jantsch, A. (eds.) Fog Computing in the Internet of Things, pp. 17–31. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-57639-8_2