

SECURITY ISSUES IN FOG COMPUTING

N. Lohitha¹, K. Revathi², Devi.T³, N.Deepa⁴

^{1,2}UG Scholar, Saveetha School of Engineering, SIMATS, Chennai

^{3,4}Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai

¹lohita432@gmail.com, ²revulovely123@gmail.com, ³devit.sse@saveetha.com,

⁴ndeepa.sse@saveetha.com

Abstract

The physical resources are shared among the users in today's IT world by the technology called virtualization. Hypervisors act as a translation layer between hardware and software. Cloud computing and fog computing employs the technology of virtualizing the resources. Extension of cloud computing that extends the functionality of the cloud nodes to the edge of the networks. Fog computing is mainly used nowadays because of its characteristics and advantages in usage. Several security issues arise due to certain characteristics such as virtualization and resource sharing. The paper provides a deep survey on the issues in fog computing related to network security, authentication, trust and so on.

Keywords: Virtualization; hypervisor; fog node; trust

1. Introduction

Smart devices are connected together that contribute to the major revolution in computing industry and thus lead to the development of IoT (Internet of Things). By the utilization of smart devices there is rise in the economic growth as well as expansion of the IT industry has also occurred. Due to the usage of smart devices several issues pertaining to computational power, bandwidth limits, usage of battery and experience of the user arise. Since the computational power of smart devices is limited there is a need of resources extension which can be handled by cloud computing. This is because cloud computing helps in scalability of resources by the usage of virtualization technology.

Virtualization is the process of virtualizing the resources with the help of hypervisors that act as an intermediate between the hardware and the software. Certain issues pertaining to reduced latency and support for mobility lead to the development yet another domain named fog computing. Fog computing mainly focus on the computing at the edge that helps in delivering new services as well as applications to the devices connected to them [1]. Devices employed in fog computing involves base stations, access points and so on. Service delivery model developed contains the three layers namely edge of network consisting of devices, fog as well as cloud computing. Such layers also support big data analytics [2] and content delivery through internet [3].

Fog computing aims at connecting the devices that are decentralized. As fog computing is actually extension of cloud, so issues related to security [4] as well as privacy that happens in

cloud may also occur in fog computing. Fog computing also utilizes virtualization as the major technology behind its success thus resource pooling is provided with the help of hypervisors. Service delivery models in fog includes Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) as well as Infrastructure-as-a-Service (IaaS) [18-20]. Public fog, private fog, community fog also contribute to the deployment models in fog computing. Table 1 describes the advantages as well as disadvantages of fog computing. Section 2 deals with the various security issues existing in fog computing and Section 3 concludes the paper.

Table 1: Advantages and disadvantages of fog computing

Advantages	Disadvantages
Data sent to cloud is reduced	Problem with physical location
Bandwidth conservation	IP spoofing issue
Response time of system improved	Issues related to privacy
Data remains near to edge for security	Cost of fog computing hardware
Support for mobility	Authentication

2. Security Issues In Fog Computing

Fog computing also makes use of virtualization of resources such as storage as well as network. Hypervisor acts as a translation layer between both hardware and software layer that helps in virtualizing the resources. When a physical device is shared among several virtual machines, there arises the problems related to security. Such issues also arise in fog computing as resources are virtualized. The security challenges in fog computing are discussed.

2.1. Issues Related To Trust

CSP (Cloud Service Providers) own the data centres in case of deployment of clouds. In fog computing, the cloud providers also differ because of various deployment options.

1. ISP - Internet Service Providers can erect fog using the available infrastructure as they have a control on home gateways.
2. CSP - Cloud Service Providers can develop the services offered by cloud to the network edges.
3. End Users - They privately own the cloud and in order to decrease the ownership cost they can turn the privately owned cloud into fog. As a result of this, the remaining resources are leased on their privately owned cloud.

Trust model that is completely based on reputation [5] is used in e-commerce as well as in social networks. As resource selection is one of the key feature of fog computing, a trust model [6] was proposed to select the resources in P2P networks. Algorithm for polling in a distributed manner was made used to identify the resource reliability before the process of downloading begins. While designing the trust model that is purely based on reputation, noteworthy issues are, (i) handling issues related to identity, (ii) handling issues related to misbehaviour, (iii) handling issues related to redemption. Several trust models based on hardware are also available such as Trusted Platform Module (TPM).

Attacker fog node: A fog node can also act as a legitimate node and fake the user as a original fog node. Instances of fog are managed by the administrator and when the attacker fog node is in the network, resources are being attacked and used without the knowledge of authenticated users. Comprising the gateway takes place before the man-in-the-middle attack occurred in fog computing. After getting connected the attacker node is able to hack the requests coming in and out of the network as well as he/she is able to modify the data. Security issues arise due to the availability of attacker fog node in the network.

Trust models based on measurement [7-8] are proposed that prevents the registered users from being connected to the access point which is fake. The round-trip time is thus leveraged among the users that assists the DNS server in detecting the client's attacker fog node.

2.2. Issues Related To Authentication

The users register with the necessary details with server to get access to the wide range of resources. The frontage fog nodes help in authentication of the users with fog computing services. Authentication is one among the major issue [9] that needs to be noted due to the involvement of various levels. Authentication methods based on Public-key Infrastructure (PKI) suffer from scalability issues. Physical contact [10] was proposed as one of the solution for authentication related issues. Biometric authentication is also used in certain areas that has lead to the usage of authentication based on biometric, based on face, based on touch as well as keystroke.

2.3. Issues Related To Network Security

Fog computing is mainly based on connectivity of wireless systems which makes the network security to be a notable issue in fog computing. Attacks based on jamming and sniffers serve as examples. Administrator of the network is always trusted to know about the configurations as it was done manually and they also help in isolation of traffic concerned with network management [11].

The usage software defined networking can help in managing the issues related to network security. The resources are available at the time of need thus making the feature of scalability of resources to be made used. As a result of utilising the leased resources the expenditure on resources gets reduced. SDN helps in monitoring the network traffic and also act as IDS (Intrusion Detection Systems). SDN also helps in isolating traffic as well as prioritizing the traffic along with the access control and sharing or network resources.

2.4. Issues Related To Protected Storage Of Data

User data is being outsourced in fog computing and at the same time the control is client data taken over by the nodes involved in fog computing. The issues pertaining to data storage in cloud computing are also applicable in fog computing also. Due to the chances of modification of data, integrity of data needs to be maintained. Data that is uploaded can also be tampered by unauthorised attackers.

Service for data storage can be audited to avoid the tampering of data. Homomorphic encryption as well as searchable encryption work together to protect data, to prevent from modification as well as to verify the data stored on untrusted servers. For auditing purpose, third-party auditor is also made use to provide privacy which can be done as public auditing. The important techniques used are homomorphic authenticator as well as masking randomly. Erasure code or LT code [12] were made use to provide data retrieval faster as well as reduced cost for communication. Service for auditing in case of data storage overview is discussed to get a deep insight into the auditing techniques available in fog computing.

2.5. Issues Related To Computation Of Data

Computational process can also be outsourced to cloud servers like the data being outsourced to untrusted servers by the clients. The proof of the results is verified by the results produced by other servers thus indicating the results to be true or false. This lead to the evolution of verifiable computing [13]. A fog node is offloaded with task of doing the computation. The user in fog computing can verify the correctness of the results produced after computation.

Client can verify the computation results based on the proofs that is non-interactive produced by the servers. Privacy for both input and the output is provided by such protocols as no information is revealed. Pinocchio [14] was the system proposed to confirm the results produced based on the assumptions of cryptography. An evaluation key which serves as a public key is made use for computation which is again utilised by the servers for evaluation of the results as well as to generate the computation proof.

2.5.1. Search for Data

Data privacy can be protected by encrypting data before storing in cloud servers. The type of encryption is referred to as client-side encryption as the client encrypts the data before outsourcing to cloud. In order to retrieve such encrypted documents, search need to be carried on them using specific keyword. Such process is referred to as keyword search and various schemes have been developed to search over encrypted data in a secure manner [15]. There is no need for decryption in such schemes. Encrypted data [16-18] can be searched thus providing secrecy as well as hidden query support is also obtained.

3. Conclusion

The security as well as privacy problems in fog computing are discussed as fog computing has revolutionised the IT industry due its characteristics and advantages. Several current issues related to trust, authentication, network security, data storage as well as data

computation are discussed to know the adverse issues caused by such issues. By finding the solutions for such issues, the number of users utilising fog nodes may be increased thus contributing to the success of fog computing.

References

1. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: workshop on Mobile cloud computing. ACM (2012)
2. Zao, J.K., et al.: Pervasive brain monitoring and data sharing based on multi-tier distributed computing and linked data technology. *Frontiers in human neuroscience* 8 (2014)
3. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. *Future Generation computer systems* 28 (2012)
4. Takabi, H., Joshi, J.B., Ahn, G.J.: Security and privacy challenges in cloud computing environments. *IEEE Security and Privacy* 8 (2010)
5. Jiang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. *Decision support systems* 43 (2007)
6. Damiani, E., et al.: A reputation-based approach for choosing reliable resources in peer-to-peer networks. In: CCS. ACM (2002)
7. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A measurement based rogue ap detection scheme. In: INFOCOM. IEEE (2009)
8. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A timing-based scheme for rogue ap detection. *TPDS* 22 (2011)
9. Stojmenovic, I., Wen, S.: The fog computing paradigm: Scenarios and security issues. In: FedCSIS. IEEE (2014)
10. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to strangers: Authentication in ad-hoc wireless networks. In: NDSS (2002)
11. Tsugawa, M., et al.: Cloud computing security: What changes with software-defined networking? In: *Secure Cloud Computing*. Springer (2014)
12. Cao, N., Yu, S., Yang, Z., Lou, W., Hou, Y.T.: Lt codes-based secure and reliable cloud storage service. In: INFOCOM. IEEE (2012)
13. Gennaro, R., Gentry, C., Parno, B.: Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: CRYPTO. Springer (2010)
14. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: Nearly practical verifiable computation. In: *Security and Privacy*. IEEE (2013)

15. Song, D.X., Wagner, D., Perrig, A.: Practical techniques for searches on encrypted data. In: Security and Privacy. IEEE (2000)
16. Wang, C., Cao, N., Ren, K., Lou, W.: Enabling secure and efficient ranked keyword search over outsourced cloud data. TPDS 23 (2012)
17. Cash, D., et al.: Dynamic searchable encryption in very-large databases: Data structures and implementation. In: NDSS. vol. 14 (2014)
18. Devi.T, Dr.K.Padmapriya, "A Novel Model for Securing Data and Bloom filter based Privacy Preserving Multiple Keyword Search over Encrypted Data In Cloud" in Journal of Advanced Research in Dynamical and Control Systems. special issue:17, 1-9, 2017.
19. Devi.T, S.Alagumani, C.Bharathi "RESEARCH CHALLENGES IN CLOUD VIRTUALIZATION" in Journal of Advanced Research in Dynamical and Control Systems, special issue:17, 235-242,2017
20. C. Bharathi, S.Alagumani, Devi. T, "MULTI PROFILE SECURE CLOUD COMPUTING WITH IMPROVED SECURITY MEASURES" in Journal of Advanced Research in Dynamical and Control Systems, special issue:17, 409-414, 2017

