ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.02, Issue.11
November -2020
Pages: -214-218

A CONCRETE DCONBE SCHEME FOR KEY MANAGEMENT IN FOG COMPUTING

[1]RAVULA HIMAKETHANA, [2]KAMBHAM SALIVAHANA REDDY, M. tech (Assistant professor)

[1,2]Global College of Engineering and Technology, Dept. of CSE

ABSTRACT: Cloud computing is an attractive criterion for accessing virtually unlimited storage and computational resources. Cloud computing has many advantage, but providing the data confidentiality in the cloud is major concern. The major disadvantages in the cloud computing is high latency, limited mobility, slow response time because data is transferred through Multiple hops. And it is centralized Geo-distribution. In Our System, we propose the Fog computing which address the above problems faced by cloud computing. Fog computing is a criterion which extends the cloud computing and its services to the network edge. It can't replace cloud. It extends the cloud computing by providing the security in the cloud atmosphere. Fog has many advantages when compared to the cloud i.e., less data traffic, low cost and latency. It also eliminates the overhead to the centralized computing system, and security is high because data moves across the edge of the network so response is quick. Still there are many advantageous in fog computing, but some of the security issues also taken into consideration while transferring the data. In our system we focus on providing the security to the data while transferred via cloud. Here Outsourcer sends the encrypted data along generated key (cipher key/encrypted key) to the data user via Fog Server. Using that encryption key the user decryption is performed and then viewed the original data.

Keywords: FOG computing, key management

1. INTRODUCTION: Fog computing is mainly used for Internet of Things. From network centre, Fog computing obtain data and services to the network edge. Similar to Cloud, Fog also data, compute, storage, application services are given to the end-users. The services and applications of fog are distributed that means fog fetches the data storage, processing and application. Fog computing is a distributed computing model that from the centralization to the network edge device such as set top box, access point. Fog computing is hosted locally so the user uses the service. Instead of sending to cloud Fog computing provides IOT data processing, storage, it is locally processed in smart devices. The purpose of both Cloud and fog are for compute, storage and networking resources. In fog computing, instead sending the collected data by sensors to the cloud server it is sent to devices such as network edge or set top box, routers, access point for processing. By doing this, the traffic is reduced due to low bandwidth. Fog computing enhance the Quality of service and also latency is reduced. Small computing works are processed locally and end users get the responses back without the use of cloud. For smaller computing works, Fog computing is better option compared to the cloud computing. Fog computing reduces the data traffic to the cloud. Since fog system provides better response time without delaying. Good example for Fog Computing is jet engine. Suppose jet engine is connected to the internet, 10 TB of data is created by jet engine within half an hour running time. For this huge data more bandwidth is needed. Fogging is complemented to cloud. Some features in fog computing differentiate from the cloud, the purpose of Fog Computing is real time interactions but it can't replace cloud computing as it preferred for high end batch processing. As the name suggests cloud system is placed at a distant where as the fog system is placed locally near to the end user. Our new key management scheme can be viewed as a dynamic ConBE (DConBE) scheme, in which a group of fog nodes that want to establish a fog system may first negotiate a group size. Then they can further agree on an initial public encryption key and their respective decryption key. Learning the public encryption key, any end user may broadcast encrypted messages to any subset of the fog nodes in the fog system. Only the fog nodes in the selected subset can decrypt the ciphertexts received. We also allow nodes to join or leave the fog system. Similar to the static ConBE, when the fog system is first initialized, only one round is required to establish the (initial) public encryption key and decryption key of each fog node. However, when the system is set up, our scheme for fog computing allows a fog node to join or leave the system. When a fog node joins or leaves the system, only one round communication is required to update the public encryption key and each fog node's decryption key. Further, we also introduce a synchronization technique for key updating based on blockchain . We note that our key management scheme is fully collusion-resistant and stateless which are two important requirements that a key management scheme should satisfy. Collusion resistance denotes that if some fog nodes in a fog system are later revoked, only the remaining fog nodes in the system are able to access the encrypted contents broadcasted. A key management scheme is called fully collusion-resistant if the scheme remains secure even all the revoked nodes collude. The latter property means that the fog nodes in a fog system do not need to update their decryption keys when some fog nodes in the system are revoked. This property is important for the efficiency of the scheme. If a key management scheme is not stateless, the decryption keys of the fog nodes in the system must be distributed again when the receiver set is changed.

II LITERATURE SURVEY:

EXISTINGCLOUD COMPUTINGSYSTEM First, 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 centres for Customers facing Web Application

1. Data breaches – This led to the loss of personal data and credit card information of about 110 million people, it was one of the theft during processing and storage of data. 2. Data loss – Data loss occurs when the disk drive dies without any backup created by the cloud owner. It occurs when the encrypted key is unavailable with the owner. 3. Account or service traffic hijacking – Account can be hacked if the login credentials are lost. 4. Insecure API's – Application Programming Interface controls the third party and verifies the user. 5. Denial of service – This occurs when millions of users request of same service and the hackers take this. 6. Malicious insiders – This occurs when a person close to us knows our login credentials. 7. Abuse of cloud services – By using many cloud server‟s hacker can crack the encryption in very less time. 8. Insufficient due diligence- Without knowing the advantages and disadvantages of the cloud many businesses and firms jump into cloud thus leading to data loss 9. Shared technology – This occurs when the information is shared by the many sites.

NEED OF FOG COMPUTING Fog Computing enables a new breed of applications and services, and that there is a fruitful interplay between the Cloud and the Fog, particularly when it comes to data management and analytics. Fog Computing extends the Cloud Computing paradigm to the edge of the network. While Fog and Cloud use the same resources (networking, compute, and storage), and share many of the same mechanisms and attributes (virtualization, multi-tenancy) The Fog vision was conceived to address applications and services that do not fit well the paradigm of the Cloud. Applications that require very low and predictable latency the Cloud frees the user from many implementation details, including the precise knowledge of where the computation or storage takes place. This freedom from choice, welcome in many circumstances becomes a liability when latency is at premium (gaming, video conferencing). Geo-distributed applications (pipeline monitoring, sensor networks to monitor the environment). Fast mobile applications (smart connected vehicle, connected rail). Large-scale distributed control systems (smart grid, connected rail, smart traffic light systems).

Fog computing extends the cloud-based Internet by introducing an intermediate layer between mobile devices or the end user device and cloud, aiming at the smooth,low-latency service delivery from the cloud to smart device. This accordingly leads to a three hierarchy Mobile-Fog-Cloud architecture. The intermediate Fog layer is composed of geo-distributed Fog servers which are deployed at the edge of networks, e.g., parks, bus terminals, shopping centres, etc. Each Fog server is a highly-virtualized computing system, similar to a lightweight cloud server, and is equipped with the onboard large- volume data storage, compute and wireless communication facility.

III IMPLEMENTATION:

Fog computing extends the cloud-based Internet by introducing an intermediate layer between mobile devices or the end user device and cloud, aiming at the smooth,low-latency service delivery from the cloud to smart device. This accordingly leads to a three hierarchy Mobile-Fog-Cloud architecture. The intermediate Fog layer is composed of geo-distributed Fog servers which are deployed at the edge of networks, e.g., parks, bus terminals, shopping centres, etc. Each Fog server is a highly-virtualized computing system, similar to a lightweight cloud server, and is equipped with the onboard large- volume data storage, compute and wireless communication facility. The role of Fog servers is to bridge the mobile users and cloud. On one hand, Fog servers directly communicate with the mobile users through single-hop wireless connections using the off-the-shelf wireless interfaces, such as Wi-Fi, Bluetooth. With the on-board compute facility and precached contents, they can independently provide pre-defined service applications to mobile users without assistances from cloud or Internet. On the other hand, the Fog servers can be connected to the cloud so as to leverage the rich functions and application tools of the cloud. To summarize, the purpose of Fog computing is to place a handful of compute, storage and communication resources in the proximity of mobile users, and therefore to serve mobile users with the local short-distance highrate connections. This overcomes the drawback of cloud which is far to mobile users with elongated service delays. Therefore, the fog is interpreted as the cloud close to the ground. DConBE scheme, we assume the communications among the fog nodes go through authenticated channels during Initialize, Join and Leave. However, confidential channels are not required during the execution of these protocols. In a fog system, the fog nodes are usually from trusted organizations and should be authenticated. If misbehavior is found, the malicious node will be punished. An authenticated channel may be also used to avoid a misbehaving node to join the system multiple times without executing Leave each time. To avoid this attack, we may restrict that the same node cannot join the system without executing Leave. The most usual method to build authenticated channels is to use digital signatures. If digital signatures are applied, then we need a certificate authority (CA). In our scheme, the CA may serve as the TA in practice. We note that TA is different from trusted dealer. TA is used to generate the system wide parameters (and issue certificates for the users in the system). A fully trusted dealer is an entity other than the TA in the system. It is used to manage a group, e.g., issue group decryption keys for the users in the group. Obviously, he has the knowledge of the group members' group decryption keys and may always decrypt the messages sent to the group. Our main goal is to remove the need for a fully trusted dealer.

4. CONCLUSION:

We have defined the notion of DConBE and proposed a concrete DConBE scheme for key management in fog computing. In DConBE, any end user can send encrypted messages to any subset of fog nodes in a fog system without requiring a trusted dealer. The new DConBE scheme allows a fog node to join or leave the fog system efficiently. The security of the proposed scheme is proven under the decision `-BDHE assumption in the standard model. In our scheme, if an end user wants to send encrypted messages to its preferred fog nodes in a fog system, the user has to know the structure of the fog nodes. As future work, it would be interesting to design a key management scheme without using the structure of the fog nodes.

5. REFERENCES:

[1] P. Mell, and T. Grace, "The NIST Definition of Cloud Computing," NIST Special Publication, 2011, pp. 800–145. [2] J. Li, L. Zhang, K. Liu, H. Qian, and Z. Dong, "Privacy-Preserving Public Auditing Protocol for Low Performance End Devices in Cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, 2016. [3] L. Zhang, X. Meng, K.R. Choo, Y. Zhang, and F. Dai, "PrivacyPreserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud", IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2018.2797190. [4] R. Meulen, "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015," http://www.gartner.com/newsroom/id/3165317 (11/10/2015). [5] IDC Market in a Minute: Internet of Things, http://www.idc.com/downloads/idc market in a minute iot infographic.pdf. [6] L. Zhang, and J. Li, "Enabling Robust and Privacy-Preserving Resource Allocation in Fog Computing," IEEE Access, vol. 6, pp. 50384–50393, 2018. [7] M. Chiang, and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854–864, 2016. [8] A. Fiat, and M. Naor, "Broadcast Encryption," in Annual International Cryptology Conference (CRYPTO), 1993, pp. 480–491. [9] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "PrivacyPreserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, 2016. [10] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed Aggregate Privacy-Preserving Authentication in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017. [11] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure Intelligent Traffic Light Control Using Fog Computing," Future Generation Computer Systems, vol. 78, part 2, pp. 817-824, 2018. [12] M. Burmester, and Y. G. Desmedt, "A Secure and Efficient Conference Key Distribution System," in Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 1995, pp. 275–286. [13] S. Jiang, "Group key agreement with local connectivity", IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp.326–339, 2016. [14] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, and O. Farras, "Bridg- ´ ing Broadcast Encryption and Group Key Agreement," in Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2011, pp. 143–160. [15] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and J. A. ´ Manjon, "Contributory Broadcast Encryption with Efficient En- ´ cryption and Short Ciphertexts," IEEE Transactions on Computers, vol. 65, no. 2, pp. 466–479, 2016. [16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009, http://www.bitcoin.org/bitcoin.pdf [17] D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," in Annual International Cryptology Conference (CRYPTO), 2005, pp. 258–275. [18] D. Boneh, and B. Waters, "A Fully Collusion Resistant Broadcast, Trace, and Revoke System," in ACM Conference on Computer and Communications Security (CCS), 2006, pp. 211–220. [19] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion ´ Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," in International Conference on PairingBased Cryptography (Pairing), 2007, pp. 39–59. [20] Y. Dodis, and N. Fazio, "Public Key Broadcast Encryption for Stateless Receivers," in Security and Privacy in Digital Rights Management (DRM), 2002, pp. 61–80. [21] J. Kim, W. Susilo, M. Au, J. Seberry, "Adaptively Secure IdentityBased Broadcast Encryption with A Constant-Sized Ciphertext," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 679–693, 2015. [22] F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in 1st edition of the MCC workshop on Mobile cloud computing (MCC 2012),

2012, pp. 13-16. [23] S. Yi, Z. Qin, and Q. Li, “Security and Privacy Issues of Fog Computing: A Survey,” in International Conference on Wireless Algorithms, Systems, and Applications (WASA 2015), 2015, pp. 685–695.