International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Securing Insurance with Privacy-Preserving Data Aggregation

Priyanka R[1] and Dr. J Bhuvana[2]

[1]Student, Department of Master of Computer Applications School of Computer Science IT, Jain Deemed to Be University, Jayanagar 9th Block, Bengaluru, Karnataka– 560041, India.

[2]MCA Coordinator, Department of Master of Computer Applications School of Computer Science & IT, Jain Deemed to Be University, Jayanagar 9 th Block, Bengaluru, Karnataka– 560041, India.

Abstract **-** Edge computing are used increasingly as it is more powerful and widespread deployment of edge devices, which enables users to manage and analyze data, while also extending computational power and data retrieval to network edges. Cloud computing is more effective in providing secure and reliability to users. However, privacy and security of outsourced data in cloud communications are difficult to address. The proposed system is secure and Privacy-preserving Data Aggregation scheme, which achieves diversified both privacy and security of outsourced data. The proposed work used proxy re-encryption concept to provide more security to the outsourced data. The proposed system is designed as Insurance services application. The outsourced data is encrypted with Advance Encryption Standard (AES) algorithm, and re-encrypted to make more secure. The data outsourced to cloud server thus user can retrieve and provided decryption key to decrypt, re-decrypt and view the data. There are three entities designed in the proposed work are aggregator, user and agent. Users or producer provide the details are encrypted and stored in cloud server. The agent or consumer are one, who retrieves data and view for further processing. Aggregator is the one, who aggregates data and store in cloud server, manage user and access to data. Aggregator also generated key and provide data security and privacy to users.

INTRODUCTION

Insurance is an agreement in which an individual or institution receives financial protection or compensation from an insurance provider in the event of a loss, represented by a policy. Insurance is a widely practiced method of security all over the world. Fog/edge computing extends from cloud computing and has greater demand in most of the real world applications in recent years. Fog/edge computing enables customers to realize computation, communication and storage locally, and extends functions of cloud computing to network edges. In the big data era, users have higher expectations for service quality and network performance. Traditional cloud computing has a significant shortage of storage capacity and computing power while handling a large number of user queries and reports. Therefore, it is beneficial to transfer some of the cloud's functionalities to the fog node. Fog/edge computing has the advantages of fast response, low delay, fog volatility, large position perception, and enhanced safety and reliability in comparison with cloud computing.

RELATED WORK

As the explosive growth of smart devices and the advent of many new applications, traffic volume has been growing exponentially. The traditional centralized network architecture cannot accommodate such user demands due to heavy burden on the backhaul links and long latency. Therefore, new architectures, which bring network

functions and contents to the network edge, are proposed, i.e., mobile edge computing and caching. Mobile edge networks provide cloud computing and caching capabilities at the edge of cellular networks. [1] In this survey, we make an exhaustive review on the state-of-the-art research efforts on mobile edge networks. We first give an overview of mobile edge networks, including definition, architecture, and advantages. Next, a comprehensive survey of issues on computing, caching, and communication techniques at the network edge is presented. The applications and use cases of mobile edge networks are discussed. Subsequently, the key enablers of mobile edge networks, such as cloud technology, SDN/NFV, and smart devices are discussed. Finally, open research challenges and future directions are presented as well.

Fog computing extends the Cloud Computing paradigm to the edge of the network, thus enabling a new breed of applications and services. Defining characteristics of the Fog are: a) Low latency and location awareness; b) Wide-spread geographical distribution; c) Mobility; d) Very large number of nodes, e) Predominant role of wireless access, f) Strong presence of streaming and real time applications, g) Heterogeneity. [2] In this paper we argue that the above characteristics make the Fog the appropriate platform for a number of critical Internet of Things (IoT) services and applications, namely, Connected Vehicle, Smart Grid, Smart Cities, and, in general, Wireless Sensors and Actuators Networks (WSANs).

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. [3] In this article, we elaborate the motivation and advantages of Fog computing, and analyses its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. 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. We investigate the stealthy features of this attack by examining its CPU and memory consumption on Fog device.

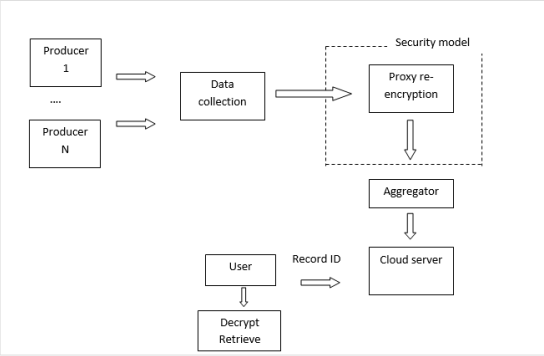
PROBLEM STATEMENT

Fog nodes may tamper with or steal data while acquiring or transferring data. Therefore, while data is processed and transferred between fog devices, authentication, data protection and other security issues need to be followed. In the current architecture of fog computing, as fog nodes and fog servers are easier to be attacked, the queried data from fog network may not be trusted. So, focusing on building a reasonable interaction between cloud service and fog network to solve the verification problem of queried data from fog network. When some applications need to require real-time process with high security such as insurance services provided to customers.

PROPOSED SYSTEM

A secure data query framework for cloud and fog computing. In this framework, a cloud server is used to check the queried data from the fog network when the fog network provides the queried data to the users. The cloud server aggregate the data from fog server and encrypted ciphertext are uploaded to the cloud server. Provided data verifying mechanisms user retrieval with access permission are controlled by the authority. Improved proxy re-encryption technique to secure the whole data and encrypted and re-encrypted form to outsource to the cloud server.

METHODOLGY



Data publisher/producer

Data publisher or producer is the one who generates data or outsource data to the cloud server. The data is insurance data for the customer and premium payment details are store in the server. The data can be stored by the producer based on the frequency of premium paying. For example, monthly, quarterly or annual. The details are stored along with the premium amount and date paid and receipt number are important to retrieve the data later for use.

Data Consumer/User

Data consumer or user are the one who is user of the stored insurance details, this may be an insurance agent or insurance officer for checking the regularity of payment and verification done by the producers. These data consumers are considered to be trusted authority and they are authorized by the trusted authority. Data consumer can retrieve the stored data by selecting the receipt number of the premium payment and verify the data.

Data Privacy module

Data privacy is an important issue while handling the insurance premium details. As this will affect the user's privacy the details are to be protected from un-necessary information. The privacy of users data are preserved by the trusted authority by providing the key to only trusted user after verification. The consumer cannot login and access the application, once they are untrusted or illegitimate transactions.

Data Security

Data security is provided by the application for the outsourced data by the system. The algorithm used for encryption is Advances Standard Encryption (AES), the cipher text and key generated are re-encrypted with proxy re-encryption. The cipertext is stored in the local database as well as in the cloud server after aggregation. The trusted authority in fog environment uploads data to the cloud server.

Fog to cloud data storage

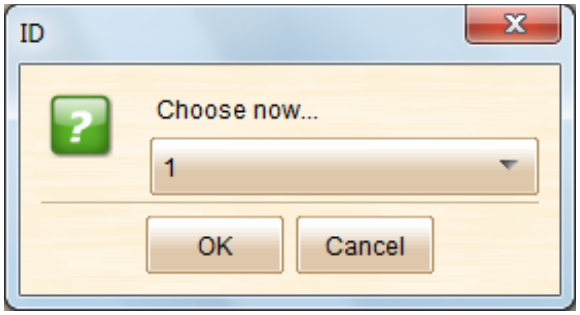
Fog node is the who is responsible to uploading the aggregated data to the cloud server. The data file contains the encrypted data, which is aggregated data of all the producer's insurance information. This cipher text data is generated and stored in the text file is uploaded to the cloud server through file transfer protocol.

RESULTS AND DISCUSSION

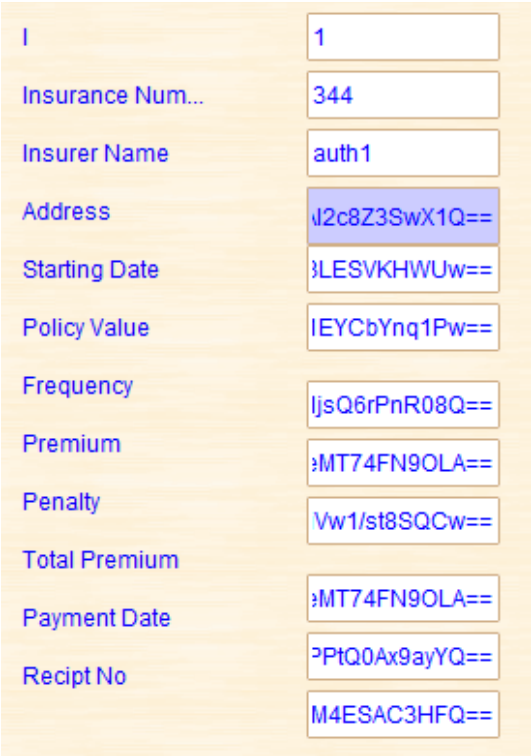
In the implemented experiments, we focus on the developing an Insurance service application, in which user can enter the premium details with full personal details. The implementation is carried out in JAVA 1.7 with Java swing as front end and MySQL server as backend. As the data handled is the insurance data along with personal details of users, here achieving the data privacy and data security are the main challenges.

Privacy of the data can be preserved by activating only trusted consumers by the trusted authority.

The results are show below.



The data shared is encrypted for preserving the data security the following screen show the re-encrypted content before uploading to the cloud server



CONCLUSION

Data privacy and security in fog-cloud architecture is a challenging technique. The proposed work considered insurance service application, which is privacy and security for data aggregation and outsource to cloud. This is achieved by two phases. Trusted authority provides data privacy through providing access or limiting access to data producer and consumer. Data security is provided by implementing AES algorithm for data encryption and storage in cloud server. The fog node which aggregated data in periodic manner and upload to cloud server. Finally, the experimental setup shown that the system is privacy preserving and secure data storage is achieved.

The future extension different encryption algorithm such as ECC can be implemented. Along with encryption, creating the block chain with SHA has function is the future work which will give more security to the application and other users or third party cannot update the data as it updated via block chain.

REFERENCES

[1] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang and W. Wang, "A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications in IEEE Access," vol. 5, pp. 6757-6779, 2017

[2] Bonomi, Flavio & Milito, Rodolfo, "Fog Computing and its Role in the Internet of Things", Proceedings of the MCC workshop on Mobile Cloud Computing, vol. 2012

[3] K. Lee, D. Kim, D. Ha, U. Rajput and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment", 6th International Conference on the Network of the Future (NOF), Montreal, QC, Canada, 2015, pp. 1-3

[4] Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues" , 2014 Federated Conference on Computer Science and Information Systems, Warsaw, Poland, 2014, pp. 1-8

[5] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang and X. Yao, "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things" in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1143-1155, Oct. 2017

[6] Y. Huo, C. Yong, and Y. Lu, "Re-ADP: Real-time data aggregation with adaptive-Event differential privacy for fog computing," Wireless Commun. Mobile Comput., vol. 2018, pp. 1–13, Jul. 2018.

[7] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," IEEE Internet Things J., vol. 6, no. 3, pp. 4946–4967, Jun. 2019.

[8] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure FaBric blockchain-based data transmission technique for industrial Internet-of-Things," IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3582–3592, Jun. 2019.

[9] G. Xu et al., "DT-CP: A double-TTPs based contract-signing protocol with lower computational cost," IEEE Access, vol. 7, pp. 174740–174749, 2019.

[10] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities," IEEE Netw., vol. 32, no. 6, pp. 144–151, Nov. 2018.