International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Secured Processing of Data Over Cloud using Disjoint Multi Attribute Authority Scheme for Key Generation

Praveen Banasode, Sunita S. Padmannavar

Cloud computing being the extensive technology used across globe for data sharing. The data may vary from small file to a highly confidential file consisting of various sensitive information stored in it. Since the cloud services are provided by the third party vendors, users are very much concerned about the security and privacy of the data and data access details. The users wants their traceability to be hidden by the cloud vendors. The biggest challenge is to share the data in a most secured way by encrypting and also preserving the anonymity of the users in cloud from the vendors. This paper addresses the issue by proposing a multi attribute authority in key generations of users, where the few sub sets of attributes will be used by multiple attribute authorities randomly and hence masking of the selection of attributes from various authorities and providing a mechanism for efficient data distribution in cloud by preserving the anonymity of the users.

Keywords: Cloud Computing, Anonymity, User privacy and Attribute authorities.

I. INTRODUCTION

The advancement in technologies have exponentially increased the generation of data at a rapid rate in various fields such as healthcare, automobile , drug care and sensor networks etc. The economical drop down in hardware devices have led to development of large scale storage devices and enhancing the processor capability to infinite extent. The generation of data across the web of world have significantly created challenges in lateral dimension for gathering data, processing in a secured way and preserving the anonymity of users [1]. A huge demand in online web applications have created a commercial boom in terms of data. Various marketing websites, social networking sites collect our personal information and get the data insight and generate a various commercial applications. Generation of data is so rapid that it's extreme difficult to handle data with a traditional ways. The term big data have exploded in the industry as a means to deal with huge data in various forms and in a most effective way. The big data have emerged in various forms such as structured data, unstructured and semi structured, each of which imposing a different challenges in handling data at different levels. The exploration of huge data in a proper way can generate the more useful insights and can help in taking effective decisions for the organizations [2]. The concept big data can be summarized with the significant five V's i.e. Velocity, Volume, variety, veracity and value. The figure 1 illustrates the concept of big data.

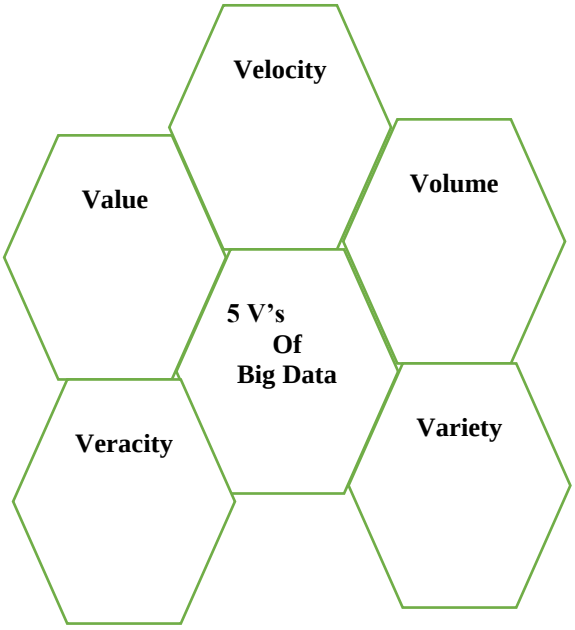

Fig 1: 5 V's of Big Data

The term velocity describes the rate of change of data in real time or process stream of data. Volume referring to the size of data in TB, PB and ZB. Variety referring to the various types of data emerging in online such as image, text and video etc. Veracity deals with the authentication and genuineness of data source and data itself. Value deals with the change in demand of data in accordance with the time. Despite of various advantages of big data, it suffers from various threats in breach of security at various levels. For example various shopping websites breach our personal interests by using our shopping preference history. YouTube recommends us video by tracing our searching history. User's personal data can be breached under various circumstances such as combining the collected user's personal data with the various external datasets and gathering insight about the user. Many a times user's personal data collected to add a tremendous value to the business such as various recommendation engines. Probability of data leakage occurs if data is stored and processed in unsecure data center locations.

To ensure big data privacy and security various security algorithms and framework are been proposed and implemented at various level of stages of big data processing such as data generation,

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Praveen Banasode*, Department of Computer Science and Engineering, Jain College of Engineering, Belagavi. India. E-mail praveen.bansode112@gmail.com
Sunita Padmannavar, Department of MCA, GIT Belagavi, India. E-mail: praveen.bansode112@gmail.com

data storage and data processing. Various traditional approaches such as falsifying data techniques i.e altering the original data bits before transmitting to third party is been used. Various encryption techniques such as Attribute-based encryption (ABE) and Identity based encryption (IBE) are used at data storage level and restriction access provision being used at processing level.

Our work majorly focuses on the securing of big data and preserving the privacy by enhancing the anonymity feature for the users and data by decentralizing the key generation by masking of the details of the attributes selected by authorities. The paper is organized in to VI Sections. Section II highlights the work carried out so far in the direction of preserving the anonymity of cloud users. Section III gives the details of the proposed system. Section IV gives the discussions on the results. Section V concludes the paper.

II. RELATED WORKS

This section provides a comprehensive state-of-art review carried in the directions of providing the security to cloud services and by preserving the information about the users in cloud environment. The cloud user's usually upload the data to the cloud servers provided by vendors. The data is stored in remote unknown locations. These servers are maintained and operated by third party cloud vendors. Hence the data owners and users are concerned about the data integrity, confidentiality and trust ability. Various users can be given access to different levels based on their access privileges. The various work carried out are discussed.

Hong Liu et.al [3] addressed the challenge of privacy preserving in cloud system using a shared attribute authority system by anonymzing the access request mechanism with privacy and security concerns. They extended the use of attribute based access control to ensure that only authenticated user's access the data specified only for them. The system has addressed issue to extent for collaborative computing in distributed environment.

Taeho et.al [4] proposed a semi anonymous scheme for achieving anonymity of users. They emphasize on the usage of decentralized authority for limiting the identity leakage and extends to generalize the file access control by privilege control on the cloud data by using fine tune granular access to the data stored on the cloud.

Jia-Lun Tsai et.al [5] addressed the privacy resilient data concerns in the Smart card generators (SCG) they proposed the scheme to reduce the usage of higher memory and bounded the secure key generators for distribution of keys in cloud environment and restricted the interaction of cloud service provider to the Scg.

Yaser Baseri et.al [6] investigated the Location based service for attribute based control for the dynamic mobile cloud environment. The approach used the multiple authority attribute based control access by using the dynamic location of the users and embedding it as a one attribute in computation of key and distributing the parameters over the set of users in cloud environment.

Prosanta Gope and Ashok Kumar Das [7] proposed the manual authentication scheme for mobile users and cloud service providers by providing their legitimacy to enrich the confidence of the mobile users for using the services provided by the cloud, where n value depends on the level of the user paid for.

Salasiah Abdullah and Khairul Azmi Abu Bakar [8] proposed a scheme for preserving anonymity of the users in Risk Adaptable access control with the flexible prospect in various exceptional cases and reacting to the suspicious user attacks.

III. PROPOSED MODEL

In our proposed architecture we have four main entities Data Owner (D), Data consumers (C), Attribute authorities (A) and cloud servers (CS). The attribute authorities A refers to the complex formulated entities who manages the attributes of the users in disjoint sets. The data owners, consumers are registered with the multiple attributes. These attributes are in turn divided into multiple disjoint sets. Each set being monitored and managed by different authorities. The users will be issued a keys private to each user by using these multiple disjoint sets and the users are masked of this iteration. Every user can able to access the data which is being encrypted but the valid users with the satisfying private key are able to perform the various operations associated with their access tree structure defined in AT. The figure 2 illustrates the framework of cloud service. The Data owners will be issued with the public key using which encryption will be performed and data consumers will be issued the private keys using which the decryption is performed and data is stored on the semi honest cloud servers. The attribute authorities are responsible for transferring the keys over the network to the dedicated users.

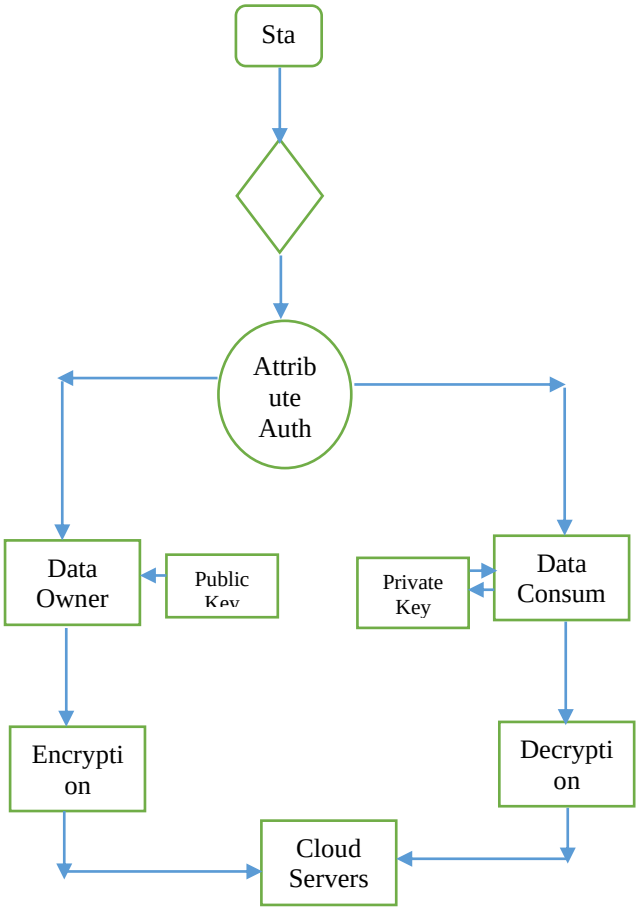

Fig 2: Framework of cloud services

Assuming that cloud servers are not fully honest i.e they try to breach the privacy of the users by showing curiosity of gathering personal information of users by using the attributes values, who have stored their data in cloud. Data consumers are random users who wants the access to data, and also may be illicit users who want to access data files illegally. The model takes the initial setup of generating the public key parameter PK and security parameter yk common to all attribute authority. Every user generates his private key Sk by exposing his attributes set Uk to all attribute authorities. The key Sk is generated by disjoint set of attributes and those are masked away from the users. Once the keys for each user is generated, the user can initiate the encryption operation on message M with the key set parameters Pk, Sk and Yk and can generate a cipher text CT along with the identification set IT defining the set of operations that can be performed on the data by a authenticated users with their access structure policies.

CT-> ENCRYPT (M,Pk,Sk,yk)----------(1)

One of the designated master authority chooses a bilinear group G0 with a prime group parameter P with a generator g and publishes to all the disjoint authority sets. Each attribute authorities in turn generates the Yk by randomly choosing the attributes and distributes to each authorities. So every authorities have independently computed the security parameters revealing no information about each other and users attributes. The master key Mk and public key Pk is computed as follows:

Mk= {yk,Ak}-------------------------(2)

Pk= { Mk,Yk}-------------------------(3)

Every users attribute set at is provided to every attribute authority and each attribute authority randomly selects the attributes az E at. The encryption operations are performed by user and generates the CT by encrypting data with Pk, SK and yk. Here every transaction is unique as the choice of yk is random by user in each operation. So the details of the users are masked as the value yk is randomly chosen and hence achieves the highest degree of anonymity. Once the encrypted data is downloaded by the authenticated user, decryption operation is performed by using his private key and the yk. The key yk is shared to list of authenticated users by attribute authorities.

M-> {CT,pk,yk}---------------(4)

Every encrypted message will be appended with the access tree structure Tp which defines the privileges of operations that can be performed on the data. The proposed model encourages the anonymity preserving of users by randomly choosing the attribute authorities, in turn attribute authorities choosing the attributes of user in random way.

IV. RESULTS AND DISCUSSIONS

In our model, we have implemented the system in Kali Linux i3 machine 8 GB Ram. The OpenStack was deployed with three vm's. The users were given a single dashboard for registration and login. The user's attributes were accessed by all disjoint attribute authorities and were allowed to choose the attribute sets randomly by all disjoint authorities for generation of yk. The data was uploaded to cloud server by data owners with their respective keys. The unknown and authentic data consumers were validated and provided with the keys to download the data. Every transaction involved randomly picked authorities for generation of keys for the users. So every transaction involved unique identity associated with all users and masking the user details to the cloud server and other users in the network. The figure 3 shows the efficiency of proposed system with various combination of disjoint attribute authorities.

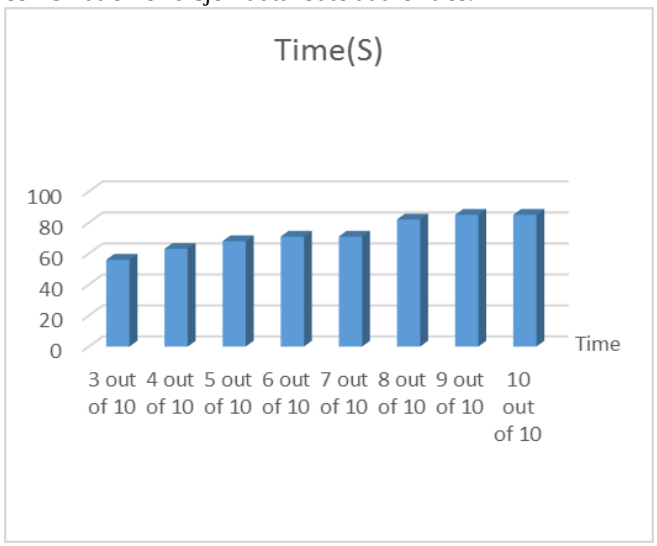

Fig 3: Efficiency of attribute authorities

The experiments demonstrated that difference in timing is very negligible with choosing more attribute authorities. As the number of attribute authorities increase the probability of extracting the information from every transaction decreases exponentially.

File Upload History | File Download History

User Name	File Name	Date	Time
[C@145dbcd	[C@1617fc5	[C@b70a8	[C@11151ba
[C@c8efc	[C@7f6b72	[C@1673ef7	[C@156cce6
[C@1a62f80	[C@1788380	[C@1015590	[C@987d26
[C@14066d1	[C@11e356b	[C@453182	[C@b575f3
[C@152b54b	[C@fc84f2	[C@7c470b	[C@11c3b04
[C@66b56b	[C@110860e	[C@1d13c26	[C@1c4048c
[C@14cb19e	[C@210805	[C@9596e5	[C@e5ab41

Fig 4: Transaction details in Cloud Server Log

Figure 4 shows that the no details regarding the user or the transaction details are revealed, hence preserving the anonymity of the users in a distributed cloud environment.

V. CONCLUSION

The primary concern for not adopting the cloud at a larger pace is due to the security concern that the user's privacy may be breached and also concern with the stored data at unknown location. This issue is tried to address by preserving the anonymity of the users by limiting their information being exposed to other entities in cloud environment. The use of masking of attributes usage in multiple attribute authorities have addressed the security concerns of data in cloud.

The work is limited to a certain disjoint attribute authorities and can be enhanced to large scale deployment by use of hybrid and public cloud services..

REFERENCES

1. P. Mell, T. Grance : "The nist definition of cloud computing," National institute of standards and technology, vol. 53, no. 6, p. 50, 2009. http://www.ossec.net/
2. Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang : "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" in IEEE Transactions on Parallel and Distributed Systems (Volume: 26 , Issue: 1 , Jan. 2015)
3. Taeho Jung, Xiang-Yang Li, Zhiguo Wan and Meng Wan: "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption" in IEEE Transactions on Information Forensics and Security (Volume: 10, Issue: 1 , Jan. 2015)
4. Jia-Lun Tsai, Nai-Wei Lo : "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services" in IEEE Systems Journal (Volume: 9 , Issue: 3 , Sept. 2015)
5. Yaser Baseri, Abdelhakim Hafid and Soumaya Cherkaoui : "K-anonymous location-based fine-grained access control for mobile cloud" in 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2016
6. Prosanta Gope and Ashok Kumar Das :" Robust Anonymous Mutual Authentication Scheme for n-Times Ubiquitous Mobile Cloud Computing Services " in IEEE Internet of Things Journal (Volume: 4 , Issue: 5 , Oct. 2017)
7. Salasiah Abdullah and Khairul Azmi Abu Bakar : "Security and Privacy Challenges in Cloud Computing" in IEEE International conference Cyber Resilience Conference (CRC) 2018.
8. Qi Jiang, Jianfeng Ma and Fushan Wei : "On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services" in IEEE Systems Journal (Volume: 12 , Issue: 2 , June 2018)
9. Debiao He, Neeraj Kumar, Muhammad Khurram Khan, Lina Wang and Jian Shen : "Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services" in IEEE Systems Journal (Volume: 12 , Issue: 2 , June 2018)

AUTHORS PROFILE

Praveen Banasode, working as Assistant Professor in Jain College of Engineering. He is research scholar in VTU. His research interest includes Big data, cloud computing and has published several papers in his domain.

Dr. Sunita S. Padmannavar, working as Assistant professor in GIT Belagavi and a research guide in VTU. She is currently guiding in Big data , cloud computing and has published several papers in national and international conferences and Journals