Privacy Preservation in Cloud Against Lack of Transparency and Disclosure

Chidananda Murthy P 1, Bajrang Prajapati K2
1Assistant Professor, Dept. of CSE, SET, Jain University
2M.Tech, Dept. of CSE, SET, Jain University

Abstract :- Cloud is a very hot topic currently being discussed in the new era of technology. Organizations step back from adapting cloud technology mainly because of the security and privacy concerns. Processing or sharing privacy-sensitive data sets on cloud probably engenders severe privacy concerns because of multi-tenancy. Lack of transparency attack where the flow of client's data is not known and disclosure attack where identity of the client is disclosed, are two major concerns of privacy preservation. This paper proposes a methodology of privacy preservation in cloud against the lack of transparency and disclosure through GSM module.

Keywords: cloud, privacy preservation, lack of transparency, disclosure, GSM module, flow, attacks.

INTRODUCTION

Cloud computing, trends at present, offers a large number of business opportunities, and likewise pose considerable challenges on the current information technology (IT) industry and research communities [1, 2]. Data sets in most applications such as social networks and sensor networks have become increasingly large and complex so that it is a considerable challenge for traditional data processing tools to handle the data processing pipeline (including collection, storage, processing, mining, sharing, etc.). As with virtual machines, a customer's data is stored over a shared infrastructure that may be distributed throughout multiple cloud data centers. Adequate security measures must be in place to ensure unauthorized clients to access data either intentionally or accidently. Cloud systems provides massive computation power and storage capacity that enable clients to deploy applications without infrastructure investment. Because of its salient features, cloud is promising for clients to handle the big data processing pipeline with its elastic and economical infrastructural resources [3].

Clients expect their data and applications stored in cloud to remain private and secure. As the challenges of security and privacy are evolving along with cloud, security is responsibility of both the customer and the service provider. There are various privacy attacks such as lack of transparency, disclosure, discrimination and surveillance. And I have focused on two attacks lack of transparency and disclosure.

LACK OF TRANSPARENCY

Lack of transparency is an attack where the client is not known about his own data (i.e. where exactly his data is moved, who has used it where and when) this degrades the privacy parameter in cloud. Basically the flow of client's data is not known which can be dangerous sometimes. Sometimes it happens

that the one's data is used by other in-order to know his nature or some data. This is considered to be a major threat to the privacy in cloud which needs to be overcome. Appropriate transparency could, at least in theory, make it possible for individuals to choose to deal with companies that minimize disclosure risks. Transparency could also diminish the effectiveness of personalized persuasion, again at least in theory [5].

DISCLOSURE

Disclosure is an attack which is faced during gathering of information in cloud. This attack leads to disclose one's identity to others which also leads to the problem of discrimination which is based on the races and religion. One disclosure threat might be the nosy employee who looks up people he knows in a corporate database and can access the data. Another might be an identity thief who successfully hacks into a database. Problems of security are the major problems for disclosure.

RELATED WORKS

Many existing studies are focused at a single privacy level which is not flexible. Hazem Elmeleegy.et.al. presented a work where the use of only one privacy level, but he said that it will either fail to meet the precision requirement of the government agency, or leak more information [5]. There are various applications which provide privacy of the client's data to themselves. The client can set privacy of his data to local, private or public. Xuyun Zhang proposed system where scalable and cost-effective framework for privacy preservation can anonymize large-scale data sets and mange anonymous data sets in a highly flexible, scalable, efficient, and cost-effective fashion [3]. Besmer et al [6] presented work which allows clients that are tagged in photos to send a request to the owner to hide the linked photo from certain people.

- Traditional tools were not designed to analyze and manage huge amount of data with respect to transparency and disclosure.
- Though traditional network security systems collect logs and events from a huge variety of systems they cover only a part of potentially relevant activity.

PROPOSED WORK

The proposed work implements the privacy levels on the server side where the client's data is stored and preserved at different levels of privacy. At H-level privacy the client can just see the files but cannot open or download file without the permission of file owner. M-level privacy the user can view the files and download files with the file owner permission and at the L-level privacy the client can directly download the file without permission of the file owner but notification is sent to the file owner through GSM module. Proposed work focuses mainly on the privacy preservation of data against the lack of transparency and disclosure attack through mobile**.** The new framework is used to distribute data and to store at different levels of privacy.

ARCHITECTURE

The proposed method has different clients at different levels of privacy, which helps in keeping track of the client, who accessed the client's data, for how many no of times and for what purpose. The proposed system works has mentioned below steps.

- Client sends the request that can be either data, which is to be stored into the database or can request for retrieving the data from the database.

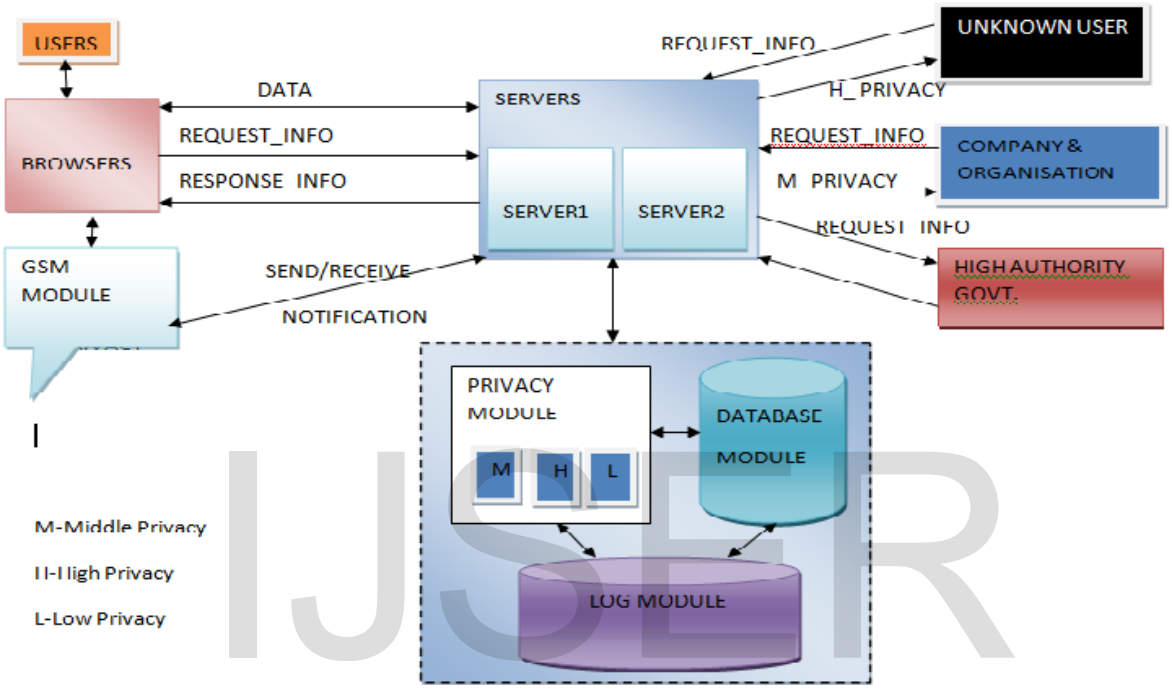

Fig1.Proposed Architecture

- The server than authorizes the client and if the client_id exist in the database, the data is shared with the client, in accordance to the level of privacy which he belongs to.
  - If an unauthorized client tries to access the data from the database, the client's data is at given H-level privacy .
  - If some registered company or organization request for the client's data then the client data is given M-Level privacy.
  - If some higher authority from government wants to access client data he should be registered in the L-Level privacy.
- The log module in the system keeps track of the client data, stores each transaction performed on the client information.
- When the client request for his data he can view the all transactions or operations performed on his data.

When client's information is accessed by other people, server should send the notification to the client's entered mobile no. Figure below depicts the working of the system with various clients at different level of privacy.

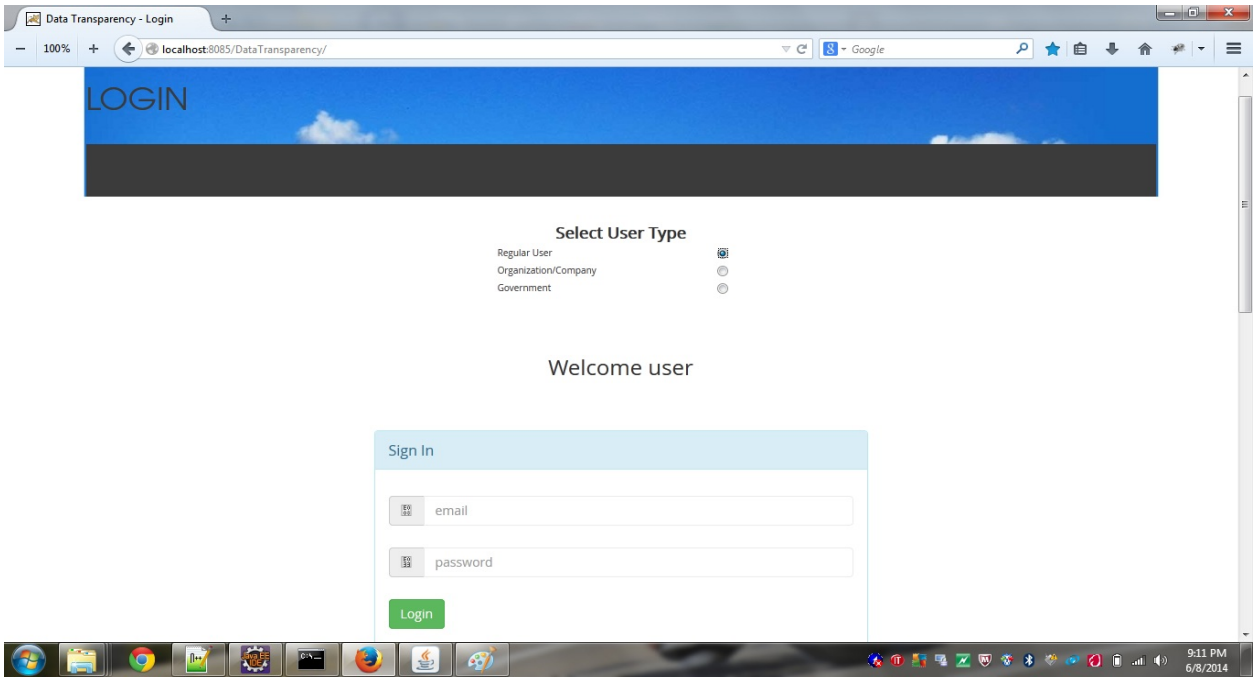

Fig 2: Shows the various user types login

Fig 3: Shows the message being send by the server to the user

RESULTS

The results obtained by the proposed architecture are on the basis of user's data flow and disclosure. The user himself will be responsible for disclosing his data to the clients through SMS notification. It has been observed that the proposed architecture reduces the disclosure parameter since user being given the permission to allow clients to use his uploaded data (through messages on mobile) and the proposed framework will allow the user to know which user has access how many no. of times his data being accessed in cloud by the client at which privacy level which reduces the lack of transparency (data flow).

CONCLUSION

The proposed architecture effectively and efficiently provides preservation of the data in cloud, by storing and providing the data at different levels and by keeping client updates about his data flow, which avoids the lack of transparency and disclosure. The client's properties are stored to track the clients accessing the cloud services. The log is maintained and a notification mail and message is sent to the client regarding the activities which increases the trust and reputation of the cloud services.

FUTURE WORK

The proposed method is restricted to 3 levels of privacy, in future work it can be increased, according to the client requirement. Proposed work may be used for more complex data which is increasing day by day. In future we may see the privacy permission to be distributed among the client and server. The proposed system fails if the client doesn't have network in mobile nor internet.

Acknowledgment

I would like to thank my author Chidananda Murthy P, Assistant Professor , Dept of CSE, School of Engineering & Technology, JAIN UNIVERSITY, Gazala Amin and all my friends who supported me in doing this paper.

REFERENCES

[1].Borkar V, Carey MJ, Li C. Inside "Big Data Management": Ogres, Onions, or Parfaits. *Proceedings of the 15th International Conference on Extending Database Technology (EDBT'12), 2012.*

[2].Chaudhuri S. What Next?: A Half-Dozen Data Management Research Goals for Big Data and the Cloud. *Proceedings of the 31st Symposium on Principles of Database Systems (PODS'12), 2012; 1–4.*

[3]. Xuyun Zhang1, Chang Liu, Surya Nepal, Chi Yang, Wanchun Dou and Jinjun Chen "SaC-FRAPP: a scalable and cost-effective framework for privacy preservation over big data on cloud" *Concurrency Computation: Pract. Exper. 2013 Published online in Wiley Online Library (wileyonlinelibrary.com).*

[4].https://cloudsecurityalliance.org/research/big-data

[5]. Hazem Elmeleegy, Mourad Ouzzani, Ahmed Elmagarmid, Ahmad Abusalah. A Study of Privacy and Fairness in Sensitive Data Analysis**.** SIGMOD '10: *Proceedings of the* 2010 *international conference on Management of data.*

[6]. A. Besmer and H. Richter Lipford. Moving beyond untagging. *In Proceedings of the 28th international conference on Human factors in computing systems - CHI* '10, *page* 1563, Apr. 2010.

[7].Mr.D.Kishore Kumar,Dr.G.Venkatewara Rao, Dr.G.Srinivasa Rao, Cloud Computing: *An Analysis of Its Challenges & Security*, IJCSN, 2012.

[8].S.Hemalatha, S.Alaudeen Basha, Enabling for Cost-Effective Privacy Preserving of Intermediate Data Sets in Cloud. *International Journal of Scientific and Research Publications, Volume 3, Issue* 10, October 2013

[9]. Felix T. Wu, Defining Privacy and Utility in Data Sets, *84 U. COLO. L. REV* , 2013.