International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

A PRACTICAL SCHEMA FOR PRIVACY PRESERVED DATA SHARING IN DISTRIBUTED NETWORKS

Suriyanarayanan.S,
Velammal Engineering College,
Chennai, Tamilnadu, India.

Sathiyanarayanan.S,
Velammal Engineering College,
Chennai, Tamilnadu, India.

Pradeep Kumar.J,
Velammal Engineering College,
Chennai, Tamilnadu, India.

Abstract: Data Privacy and System Performance to be safe and efficient over the data collection. distributed data sharing with Privacy-preserving requirements the problem is to transmit data safely and accurately. Handling data stream efficiently. Shadow Coding – achieves privacy preserving computation in a data-recoverable Application – pilot system in a city. In order to alleviate message redundancy and reduce message latency

Keywords: Data Recoverable, Safe and Secure

I. INTRODUCTION

It's to be safe and efficient considering both data privacy and system performance. Enable the data demander to access the distributed data without knowing the privacy of any individual provider. Propose practical method and shadow coding to be privacy preserved data sharing.Achieves privacy preserving computation in a data-recoverable, efficient, and scalable way.Collecting data from distributed data providers is a challenging task to big data related research communities and industries.These local sites provide communication services for mobile phones. Call volume and the location of each base station are considered commercially confidential by each communication operator.To protect the correlation such as the distribution of base stations of a specified operator. It is also highly required to be practical in deployment. The data demander requires the accurate data to support data analysis. Prior literature and research challenges for a better understanding of distributed data sharing in a privacy-preserved and recovery ensured way.

II. PROPOSED SYSTEM

Identity-based systems allow any party to generate a public key from known identity value as ASCII string. A trusted third party called the Private Key Generator (PKG), it generates the corresponding private keys. In thus master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with their identity value. The proposed system consists of the following goals and has the scope as follows:

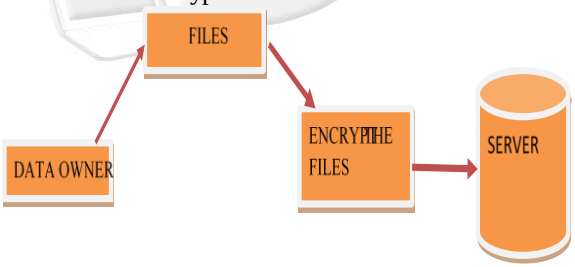
a) Goals:

- Collecting data from distributed data providers is a challenging task to big data related research communities and industries.
- To improve the existing system.
.
- The data demander requires the accurate data to support data analysis.

b) Scope:

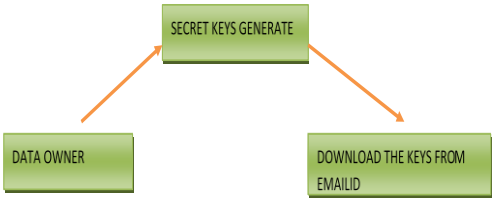
- Ensure that all the functionalities of a manual data demander are covered.
- Make sure the program is simple and easy to use.

Cloud Server: The cloud server hosts third-party data storage and retrieve services. Since data may contain sensitive information, the cloud servers cannot be fully entrusted in protecting data. For this reason, outsourced files must be encrypted. Any kind of information leakage that would affect data privacy are regarded as unacceptable the data user encrypts the query and sends it to the cloud server that returns the relevant files to the data user. Afterward, the data user can decrypt and make use of the file.

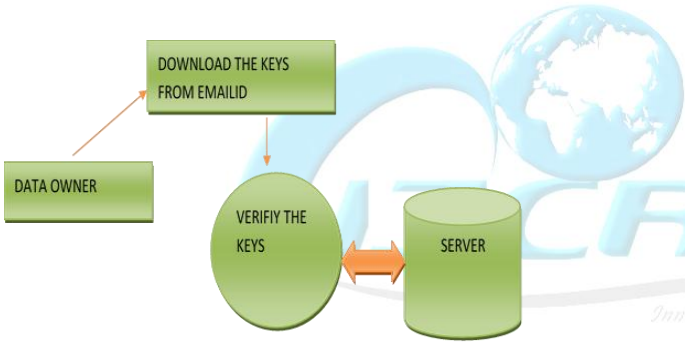


Asymmetric Key Generation: In the asymmetric cryptography, refers to a cryptographic algorithm which is requires to two separate keys one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext**.** The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both.

IJCRCST © 2017 | All Rights Reserved

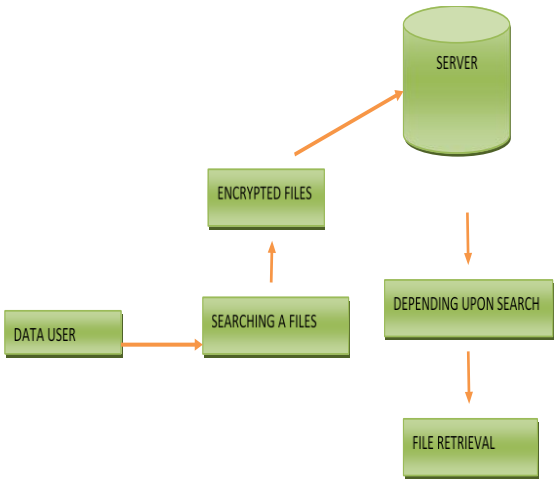


Data Authentication: When it comes to cloud data protection methods, no particularly new technique is required. Protecting data in the cloud can be similar to protecting data within a traditional data center. Authentication and identity, access control, encryption, secure deletion, integrity checking, and data masking are all data protection methods that have applicability in cloud computing. This will briefly review these methods and will note anything that is particularly unique to when these are deployed in a cloud Authentication of users takes several forms, but all are based on a combination of *authentication factors*: something an individual knows (such as a password), something they possess (such as a security token), or some measurable quality that is intrinsic to them (such as a fingerprint).

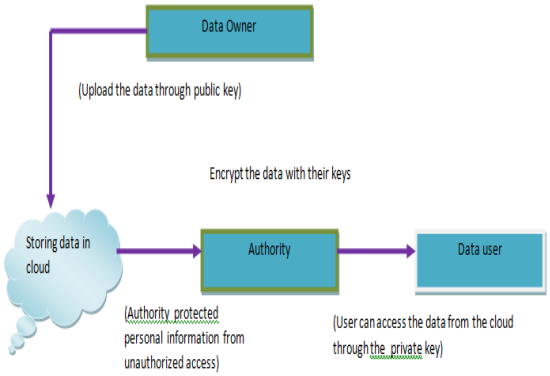


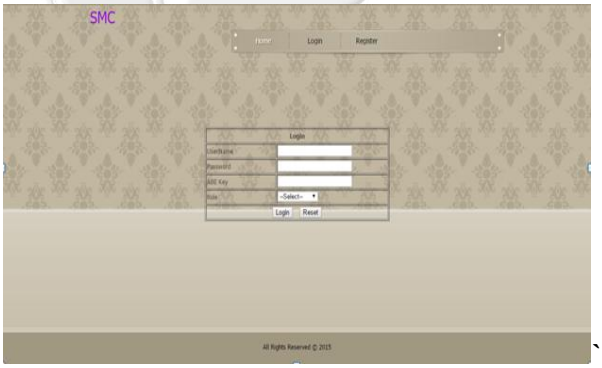
Single factor authentication is based on only one authentication factor. Stronger authentication requires additional factors; for instance, two factor authentications is based on two authentication factors (such as a pin and a fingerprint).Authentication is usually predicated on an underlying identity infrastructure. The most basic scheme is where account information for one or a small number Cloud Data Security: Sensitive Data Categorization 137 of users is kept in flat files that are used to verify identity and passwords, but this scheme does not scale to more than a very few systems.

File Retrieval: The search time includes fetching the posting list in the index, decrypting, and rank ordering each entries. Our focus is on top-k retrieval. As the encrypted scores are order preserved, server can process the top-k retrieval almost as fast as in the plaintext domain. Note that the serverdoes not have to traverse every posting list for each given trapdoor, but instead uses a tree-based data structure to fetch the corresponding list. Therefore,
theoverall search time cost is almost as efficient as on unencrypted data.



System architecture:





Description: The user has to login or register started with the Web. After clicking LOGIN button, the entered password and the entered username will be sent to the back-end database and the user will be granted access if he is registered within the system. On clicking the 'REGISTER NOW' button, the user will be directed to the registration form.

Description:
The Home Page offers: The login and register to generate the account details process.

Fig: Home page

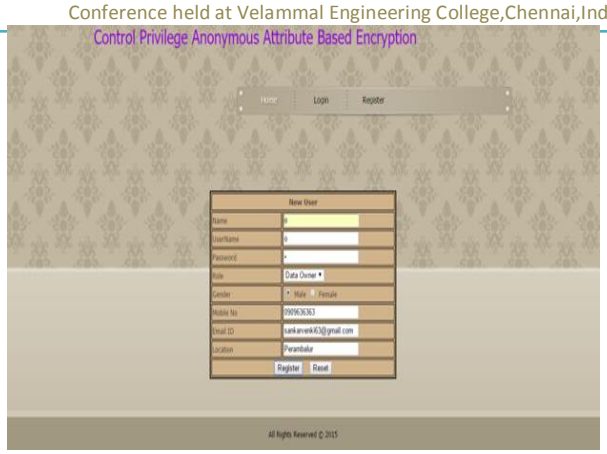
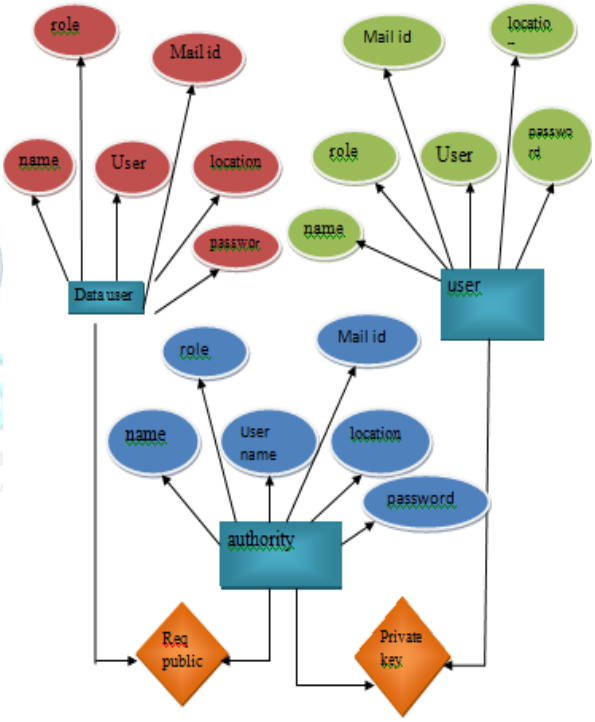


Fig: Data owner

ıgram

Figure :user details

Description: For the security purpose the user has to fulfill the above details. unique passwords will be given for security reason.



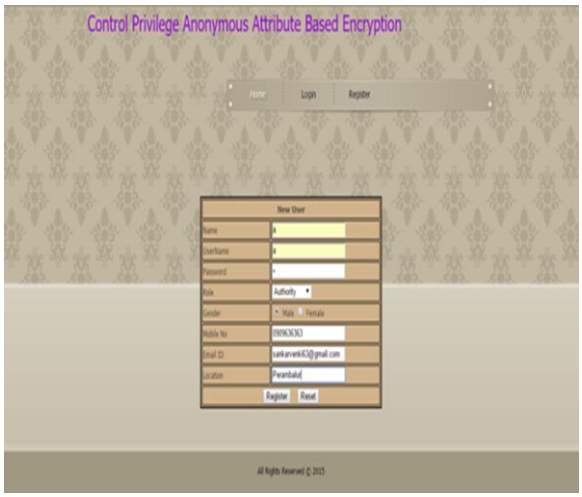


Fig: Register authority

III.CONCLUSION

A privacy-preserved data sharing problem is studied in the context of real-life distributed mobile phone networks. We formulate the problem as a distributed data sharing problem, and we propose a shadow coding method with shadow matrix computation, which is privacy-preserving, efficient, and data-recoverable. A generalization of this method is also used. To evaluate the proposed methods, we conduct the experiments with a large-scale real-lifedatasets. The proposed schema is also implemented as a pilot system in a cityto collect distributed mobile phone data.

REFERENCES

.

[1] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin and Y. Theodoridis, "State-of-the-art in privacy

preserving data mining," ACM SIGMOD Rec., vol. 33, no. 1, pp. 50–57, 2004.

[2] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Compute Surv., vol. 42, no. 4, pp. 14:1–14:53, 2010.

[3] M. C. Gonzalez, C. A. Hidalgo, and A. Barabasi, "Understanding individual human mobility patterns," Nature, vol. 453, pp. 779–782, 2008.

[4] R. Carlo, S. Williams, D. Frenchman, and R. M. Pulselli, "Mobile landscapes: using location data from cell phones for urban analysis," Environment and Planning B: Planning and Design, vol. 33, no. 5, pp. 727–748, 2006.

[5] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2010, pp. 735–746.

[6] J. Gao, J. X. Yu, R. Jin, J. Zhou, T. Wang, and D. Yang, "Outsourcing shortest distance computing with privacy protection," Int. J. Very Large Data Bases, vol. 22, no. 4, pp. 543–559, 2013.

[7] M. Yuan, L. Chen, and P. S. Yu, "Personalized privacy protection in social networks," in Proc. VLDB Endowment, 2010, vol. 4, pp. 141–150.

[8] S. Liu, L. Chen, and L. Ni, "Anomaly detection from incomplete data," ACMTrans. Knowl. Discovery Data, vol. 9, no. 2, pp. 1–22, 2014.

[9] S. Liu, L. Kang, L. Chen, and L. M. Ni, "Distributed incomplete pattern matching via a novel weighted bloom filter," in Proc. IEEE 32nd Int. Conf. Distrib. Comput. Syst., 2012, pp. 122–131.

[10] R. Agrawal and R. Srikant, "Privacy-preserving data mining," ACM SIGMOD Rec., vol. 29, no. 2, pp. 439–450, 2000.

IJCRCST © 2017 | All Rights Reserved