IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Privacy Preservation in Big Data

M. Prashanthi[1*], A.P. Siva Kumar[2]

[1*]Department of CSE, JNTUA College of Engineering, Ananthapuramu, India
[2]Department of CSE, JNTUA College of Engineering, Ananthapuramu, India

[*]*Corresponding Author: prashanthi494@gmail.com*

Available online at: www.ijcseonline.org

Received: 14/Jul/2017, Revised: 27/Jul/2017, Accepted: 19/Aug/2017, Published: 30/Aug/2017

***Abstract*—**As of late, enormous info has switched into a hot analysis theme. The expanding resolution of immense information builds the shot of breaking the safety of people. Since enormous info needs high calculation ability and intensive stockpiling, use distributed frameworks. As different gatherings are enclosed in these frameworks, the danger of security violation is expanded. Many securities safeguarding systems are created at information era, information stockpile and information handling levels of huge info life cycle. Protection conservation parts with large info and the difficulties for existing instruments are the prevailing goals. Specifically, we represent the new framework for securing immense info named ring signature. Moreover safeguarding modules in every section of the large fact life chain. In this, the file will be encrypted and stored in the cloud storage. If the attackers get the decryption key, the privacy of the file will be violated. And the integrity of the file not guaranteed. The file should be securely shared inside the group of the user without outsiders' inference. Besides, we speak the difficulties and future analysis directions determined with security in big data.

***Keywords*—**Info stockpile, data auditing, privacy, data handling, ring signature

I. INTRODUCTION

All the tremendous info created from many sources of various arrangements with speedy alluding as giant information. In the unit of time, huge info is in organized, semi-organized, or unstructured, which include new difficulties polishing off info storage and managing assignments [1]. Gigantic info, caught and examined in a convenient way can advance the logical research and economy by changing conventional plans of action and logically esteems.

Client's security might break under the accompanying conditions [2-3]:

- Peculiar documents, when merging with outside data sets might prompt the surmising of new certainties of the shoppers. Shrouded facts should cover huge realities.
- Sensitive data is gathered to raise the worth of a business. For instance, person's shopping propensities might uncover the specialized information.
- The delicate information handled in a space does not seem to secure fitly and data spillage might happen amid ability and organizing stages.

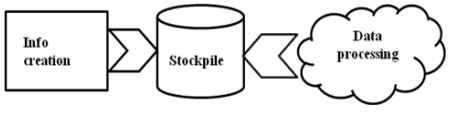

Figure 1. Big testimony activity cycle.

Ensuring protection for monumental info is a quick developing examination sector. Albeit associate and some papers have given an overview/survey style of papers. In addition, while these papers given the elementary plan of security insurance against large info, they neglected to cover many essential components of this region. Pertaining to an instance, neither offers definite discourses association with huge info nor agreement on allotted computing. Hence, ring signature, which aims to provide secure sharing of files, is needed.

The remaining contents of the paper are arranged as follows. Section II gives information about related works. Propose work and architecture are explained in Section III. Section IV contains the information about implementation and essential steps. Sections V and VI includes experimental results and conclusions respectively.

II. RELATED WORK

As we have mentioned the dimensions conjointly form into the fact go on spreading new tools and techniques used to handle such knowledge ought to upgrade alike. Here is some existing privacy conserving techniques.

Waters [5] worked on a paper that proposes attribute-based encoding theme. It is one among the encryption techniques that guarantee associate degree finish to finish in cloud storage system. Access policies are outlined by the data keeper and together with compilations encrypt beneath those

© 2017, IJCSE All Rights Reserved

policies. Information will solely get through the customer whose aspects related them. When dealing with massive knowledge one might have compelled to amendment knowledge access policies. Current encoding doesn't support policy change. Policy rectification is a hard task during this sort-of encoding. Logic beneficial is generally expanded upon crowd reserve; the advice partner wouldn't keep the native transcript system. If they need to amend the protocol, he has to move the info back to the local system. This leads to high communication overhead and high process price [6].

X. Boyen and B. Waters [8] scheduled identity-based encoding, an associate degree different social code that planned to change key administration arrangement certificate-based social basic framework by victimization mortal circumstances like email or IP address. Sender and receiver plan the theme; no way guide the cipher text receiver.

C. Gentry created a study on homomorphic encoding [10]. Expose public cloud to secrecy violation owing to multi-ownership and virtualization. The distinct cloud users might share a similar physical area. In such a scheme, the possibilities of information outpouring are additional high. One style to shield the conversation is to produce privacy. Allow performing arts computations over encrypted knowledge. Total homomorphic encoding is the encoding manner certificates the function to compute on encrypted knowledge. Given the unreadable message, one can get associate degree encoding of a performance by computing on the message. Homomorphic encryption provides privacy, however, the downside processed the quality and generally, it's terrible onerous to add with existing technologies.

III. PROPOSED MODEL

Establishment of new security insurance, the Ring Signature conspires to take place. The shut acquiring document verification framework, where the evidence partner is willing to secure share his documents within the gathering while untouchable's induction. Also, give the trustworthiness of the record. Pertaining to every single document, produce the ring stamp. With the aid of ring sign, the gathering people will all set to effective decipher the document and transfer from the cloud.

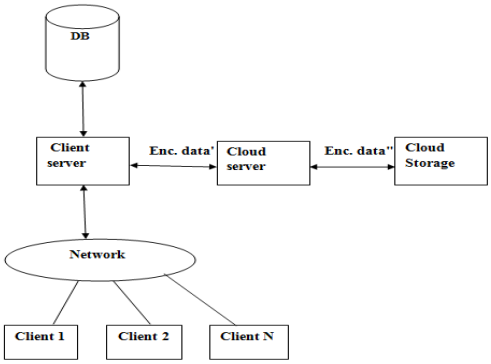

Figure 2. Proposed model.

The above design explained how we own an impulse to rings signature conductive to produce certainty. Admin will show a cluster by aggregation their id. Next he will give security keys to all users within the cluster. The client sends the file, keep in client-server. In customer server, keep up one database. Encipher that records with the band stamp and sent to a cloud server. The file will be second time enciphered reaching toward cloud storage by deception AES key. If anybody wants to transfer the record, he has to transfer the ring signature. Otherwise, he cannot download the file.

IV. RESULTS AND DISCUSSION

IMPLEMENTATION

A. *Group and User formation* - Admin can view the group added and can add the new groups. The user collects the login details.

B. *Transmitting records* - The manager views the list within class and uploads new facts.

C. *Ring Signature origination* - The user will get the public keys of all partners in user's cluster and generates a hash code for the uploaded file. By this, perform XOR work using public keys. Later takings of XOR action are the secure MD (Secure Message Digest). At that instant, formulate effective received into the folder thereby securing register. After concealing the secured register amidst non-public key of uploading operator, recognize the encoded record as Ring Signature of the uploaded file. Designing to ring signature, the user sends the file to the handpicked members of the cluster through e-mail.

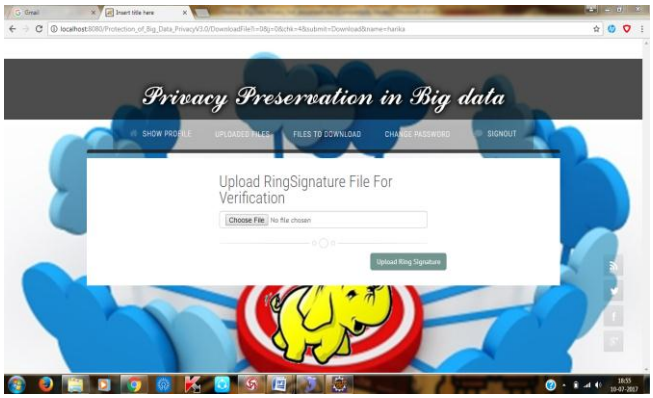

Figure 3. Uploading Ring Signature.

D. *File Coding process* - Fetch the key and encrypt the uploaded file using encryption standard technique.

E. *File Cryptography process* - Decode the received file with the standard cryptography technique.

F. *Ring Signature Verification* - The destination operator obtains the keys of loading the file using SecureMD, assumed as SecureMD1. Now, decrypt the ring signature directory including the key of the user and

© 2017, IJCSE All Rights Reserved

find the SecureMD, taken as SecureMD2. Evaluate SecureMD1 and SecureMD2.

V. EXPERIMENTAL RESULTS

Admin will generate a group by taking user's id. All the users in the cluster are provided with security keys. Then the file is taken to the client server. After that file is encoded using ring signature and is stored in the cloud server. Again the file is encrypted before going to the cloud storage with the key. Now the document is totally encrypted. The group members can securely share the documents by uploading ring signature as shown in Fig. 3.

Evaluate the ring signature file with the document that contains encrypted keys. If matches confirmation action fruitful and download the file to the shopper system otherwise authentication method failure and can offer the error message that ring signature is mismatching as shown in Fig. 4.

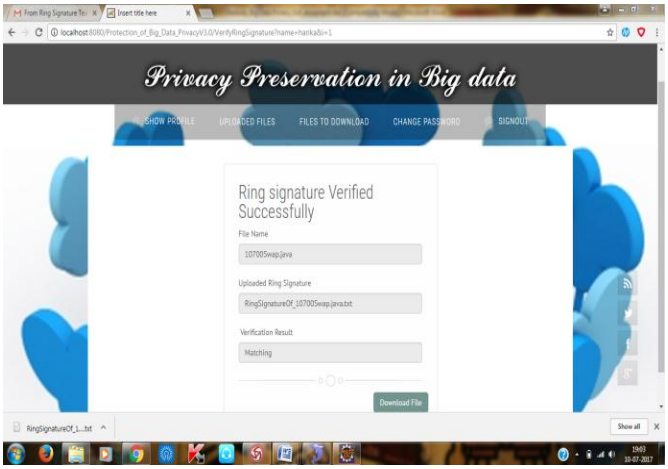

Figure 4. Ring Signature verification.

The integrity of the file is guaranteed. Privacy of the file is protected efficiently. Now, the user can receive the data by uploading the necessary file of sing signature. Fig. 5 shows the overall performance with different techniques.

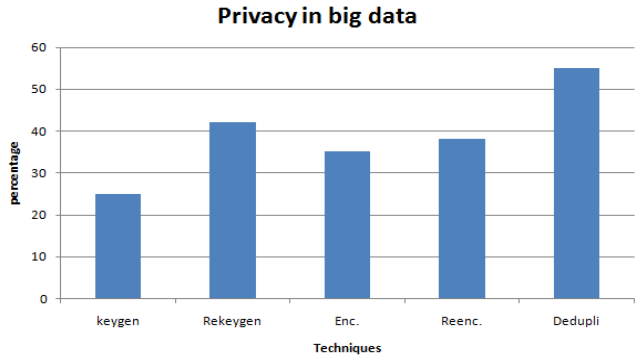

Figure 5. Experimental results.

VI. CONCLUSION AND FUTURE SCOPE

The amount of knowledge is growing and it's undesirable to imagine next applications without assembling and executing prominent driven methods. To resolve such issues, we designed privacy conserving mechanism that processes different knowledge. The main advantage in deploying ring signature scheme is to keep the data complexity as low as conceivable. Lot masterpieces have accomplished to preserve the privacy of users from knowledge formulation to processing part.

Sometimes the input data by a company doesn't have enough info (i) to find helpful facts in the domain, (ii) acquiring that knowledge might be expensive or tough to legal constraints and (iii) concern of secrecy violation. To solve these issues, a multiparty homomorphic method can be deployed.

REFERENCES

[1] A. Katal, M. Wazid, and R. H. Goudar, ``*Big data: Issues, challenges, tools and good practices*," in Proc. IEEE Int. Conf. Contemp. Comput., Aug. 2013, pp. 404-409.

[2] J. Manyika et al., "*Big data: The Next Frontier for Innovation, Competition, and Productivity",* Zurich Switzerland: McKinsey Global Inst., Jun. 2011, pp. 1-137.

[3] Z. Xiao and Y. Xiao, ``*Security and privacy in cloud computing*," IEEE Commun. Surveys Tuts. vol. 15, no. 2, pp. 843-859, May 2013.

[4] V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``*Attribute-based encryption for fine-grained access control of encrypted data*," in Proc. ACM Conf. Comput. Commun. Secure. Oct. 2006, pp. 89-98.

[5] S. Singla and J. Singh, "*Cloud data security using authentication and encryption technique*," Global J. Comput. Sci. Technol., vol. 13, no. 3, pp. 2232-2235, Jul. 2013.

[6] J. Bethencourt, A. Sahai, and B. Waters, "*Ciphertext-policy attribute-based encryption*," in Proc. IEEE Int. Conf. Secure. Privacy, May 2007, pp. 321-334.

[7] K. Yang, X. Jia, and K. Ren, "*Secure and verifiable policy update outsourcing for big data access control in the cloud*," IEEE Trans. Parallel Distrib. Syst., vol. 26, no.12, pp. 3461-3470, Dec. 2015.

[8] X. Boyen and B.Waters, "*Anonymous hierarchical identity-based encryption (without random oracles)*," in Proc. Adv. Cryptol. (ASIACRYPT), vol. 4117. Aug. 2006, pp. 290-307.

[9] M. Green and G. Ateniese, "*Identity-based proxy re-encryption*," in Proc. Int. Conf. Appl. Cryptogr. Netw. Secure. 2007, vol. 4521. pp. 288-306.

[10] C. Gentry, "*A fully homomorphic encryption scheme*," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[11] C. Liu et al., "*Authorized public auditing of dynamic big data storage on a cloud with efficient verifiable fine-grained updates*," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2234-2244, Sep. 2014.

[12] B. Sowmya, K. Madhavi, "*Secure Cloud Storage via Attribute-based Encryption*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.7, pp.96-100, 2017.

© 2017, IJCSE All Rights Reserved

Authors Profile

M. Prashanthi received B. Tech degree in Computer Science and Engineering from Sree Vidyanikethan Engineering College, A. Rangampet, Andhra Pradesh, India. She is currently pursuing M.Tech in Software Engineering at JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, India.

Dr. A.P. Siva Kumar is an Assistant Professor of Computer Science and Engineering at JNTUA, Ananthapuramu. He obtained his Bachelor degree in Computer Science & Information Technology from JNTU Hyderabad, Master of Technology in Computer Science from JNTU Hyderabad and Ph.D. in cross-lingual information Retrieval from JNTU Ananthapuramu. He has published several Research papers in National International Conferences and Journals. His research interests include Information Retrieval and Natural Language Processing.

© 2017, IJCSE All Rights Reserved