A Survey on Secure and Verifiable Access Control Scheme for Cloud Computing

Mr Namith Valappil[1] Mr Abhay Deshpande[2] Mr Shubham Sarolkar[3] Mr Rohit Thorat[4]
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Dr. D. Y Patil Institute of Technology, Pimpri Maharashtra, India

Abstract— Due to the quality and volume, outsourcing data to a cloud is deemed to be one in all the foremost effective approaches for large knowledge storage and access. With increase in number of users the amount of data being stored on the cloud has substantially increased. The access legitimacy of a user firmly depends on the ciphertext policy accepted by the owner. Ancient approaches either fully ignore the difficulty of access policy update or delegate the update to a 3rd party authority. There are always possibilities of duplicate data on cloud. This paper has discussed various development their advantages and limitations of different encryptions.

Key words: Encryption, Decryption, Integrity, Ownership

I. Introduction

Big knowledge may be a high volume, and/or high speed, high selection data quality, which needs new kinds of process to modify increased higher cognitive process, insight discovery, and method improvement. Attributable to its complexness and enormous volume, managing massive knowledge mistreatment existing direction tools is tough. economical|a good} answer is to source {the knowledge|the info|the information} to a cloud server that has the capabilities of storing massive data ANd process users' access requests in an efficient manner. As an example in ehealth applications, the ordering data ought to be firmly hold on in an e-health cloud as one sequenced human ordering is around a hundred and forty gigabytes in size. However, once {a knowledge|a knowledge|an information} owner outsources its data to a cloud, sensitive data could also be disclosed as a result of the cloud server isn't trusted; so generally the ciphertext of the info is hold on within the may. however a way to update the ciphertext hold on during a cloud once a replacement access policy is selected by the info owner and the way to verify the legitimacy of a user WHO intends to access the info ar still of nice considerations. Most existing approaches for securing the outsourced massive knowledge in clouds ar supported either attributed-based cryptography or secret sharing. ABE based mostly approaches offer the flexibleness for an information owner to predefine the set of users WHO ar eligible for accessing the info however they suffer from the high complexness of with efficiency change the access policy and ciphertext. Secret sharing mechanisms enable a secret to be shared and reconstructed by bound variety of cooperative users however they generally use uneven public key cryptograph like RSA for users' legitimacy verification, that incur high process overhead. Moreover, it's conjointly a difficult issue to dynamically and with efficiency update the access policies in keeping with the new necessities of the info house owners secretly sharing approaches.

II. Literature survey

Esa Mohammed A, Hariharan N, Mohan R, Arul jothi K [5] Increasing importance of data storage has made the data size to be huge, slowing the process of knowledge collection from the large volumes of high-dimensional and complex data. Extracting and Mining data from huge knowledge assortment is to be an excellent challenge these days.

Shweta Agrawal Xavier Boyeny [2] Cryptosystems supported the hardness of lattice issues have recently non inheritable a lot of importance owing to their average-case to worst-case equivalence.

Chunqiang Hu, Fan Zhang1, Xiuzhen Cheng [4] the primitive functions to implement a secret-sharing primarily based Ciphertext- Policy Attribute-Based coding (CPABE) theme, that encrypts the information supported AN access structure fixed by the information supply. We have a tendency to additionally style 2 protocols to firmly retrieve the sensitive patient knowledge from a BAN and instruct the sensors in an exceedingly BAN. Our analysis indicates that the planned theme is possible, will offer message credibleness, and may counter doable major attacks like collusion attacks and battery-draining attacks.

Ebenezer R.H.P. Isaac et al [16] put forward a cryptosystem that was useful to verify the security of not only the data present with the user but also verify the security of the network. To provide security in both cases it uses a simple block cipher scheme. This can reduce both the space and the time complexities.

Einat Gil, James D. Slotta [3] proposed a study in this study students interact in learning regarding massive knowledge in a very data Community and Inquiry course of study.

Priyanka Ora et al [15] proposed a scheme which provides data security and data integrity on cloud. The proposed scheme has a combination of RSA Partial homomorphic and MD5 algorithm. The data is encrypted before loading it on the cloud server. Encryption and decryption is done on the data with the help of RSA partial homomorphic algorithm. Encryption as well as decryption is done with the help of public and private key which is provided by the RSA algorithm. Now data hashing is performed on the uploaded data by using MD5 algorithm to produce hash values. The hash values can be used for data verification. Data sharing is carried out among authorized users but it is not certain how effective the scheme can be.

III. Common issues

Due to the increase in use of computers and the availability of internet, cloud is mostly is used for storing data as it is easier to access and modify the data. But this has also given rise to many issues like data duplication, security, access control. Some issues are as follows:

1) The person who accesses the data from the organization should be verified.
2) The data should be stored without duplication.
3) Only people with proper authority should be allowed to accesses the data.
4) The network should always be checked for any security risks.

IV. Advantages

The projected theme will verify the shared secret info to forestall users from cheating and might counter varied attacks like the collusion attack.

1) Providing knowledge TIME based mostly
2) For a secure organization
3) Highly verifiable sector
4) Passport verification
5) Email account user verification
6) Bank security
7) Government files security

V. Conclusion

This paper gives an outline of all the recent changes and developments in the field of cloud storage access control schemes. This paper provides the researchers a knowledge about the previous works and what were their limitations. This paper will allow the researcher community to understand the need of the current market and also may help them to explore new techniques in future.

References

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.

[2] Shweta Agrawal Xavier Boyeny Vinod Vaikuntanathanz Panagiotis Voulgarisx. "Fuzzy Identity Based Encryption from Lattices." (2016)

[3] Einat Gil, James D. Slotta. "Knowledge Community and Inquiry about Big Data among High School Students with Interactive Orchestrated Learning Space." (2016)

[4] Chunqiang Hu, Fan Zhang1, Xiuzhen Cheng. "Securing Communications Between External Users and Wireless Body Area Networks." (2016)

[5] Esa Mohammed A, Hariharan N, Mohan R, Arul jothi K. "Enhancing the Performance of Association Rule Mining Using Inverted Index Compression." (2016)

[6] Marx, "Biology: The big challenges of big data," Nature, vol. 498, no.7453, pp. 255–260, 2013.

[7] G. P. Consortium et al., "A map of human genome variation from population-scale sequencing," Nature, vol. 467, no. 7319, pp. 1061–1073, 2010.

[8] Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.

[9] Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

[10] Perttula, B. Warner, and Z. Wilcox-O'Hearn, "Attacks on convergent encryption." (2016). [Online]. Available: http://bit.ly/ yQxyvl

[11] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, vol. 305, pp. 357–383, 2015, doi:10.1016/j.ins.2015.01.025.

[12] Lifei Wei, Haojin Zhu, Zhen fu Cao, Xiao lei Don, Weiwei Ji, Yunlu Chen and Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Information Sciences: an International Journal, Volume 258, Pages. 371–386, 2014, doi:10.1016/j.ins.2013.04.028.

[13] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Messagelocked encryption and secure deduplication," in Proceedings Cryptology—EUROCRYPT, 2013, pp. 296–312, doi: 10.1007/978-3-642-38348-9_18.

[14] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li and Albert Y. Zomaya, "SeDaSC: Secure data sharing in clouds," IEEE Systems Journal, 2015, Volume. 11 Page, nos. 99, pp. 1–10, 2015, doi: 10.1109/JSYST.2014.2379646.

[15] Priyanka Ora, Dr. P.R Pal "Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography" published in IEEE International Conference on Computer, Communication and Control (IC4-2015), ISBN 978-14799-8165-6

[16] Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi "Reverse Circle Cipher for Personal and Network Security" published in Information Communication and Embedded Systems (ICICES),2013 International Conference , DOI 10.1109/ICICES.2013.6508354.