International Journal of Science Engineering and Advance Technology (IJSEAT)
ISSN 2321-6905, Vol. 8, Issue 3, March -2020

A Novel SSGK To Protect The Communication Process And Shared Data From Unauthorized Access

[1]B.VenkateswaraRao, [2]P.RadhikaKrupalini
[1]Final year MSc(CS), Ideal College of Arts &Sciences, Kkd, A.P, India.
[2]Associate Professor, dept. of Computer Science, Ideal College of Arts & Sciences, Kkd, A.P., Indi

ABSTRACT:

A cloud-based big data sharing system uses a storage facility from a cloud specialist co-op to impart data to authentic clients. As opposed to customary arrangements, cloud supplier stores the mutual data in the huge server farms outside the trust area of the data proprietor, which may trigger the issue of data classification. This paper proposes a secret sharing group key management convention (SSGK) to secure the correspondence procedure and shared data from unapproved get to. Not quite the same as the earlier works, a shared key is utilized to encode the common data and a secret sharing plan is utilized to circulate the shared key in SSGK. The broad security and execution investigations demonstrate that our convention profoundly limits the security and protection dangers of sharing data in distributed storage and spares about 12% of extra storage space.

KEYWORDS: security and privacy, cloud storage, data sharing.

1] INTRODUCTION:

The developing advancements about big data, for example, Cloud Computing [1], Business Intelligence [2], Data Mining [3], Industrial Data Integration Engineering(IIIE) [4] and Internet-of-Things [5] have opened another period for future Enterprise Systems(ES) [6]. Distributed computing is another processing model, in which all asset on Internet structure a cloud asset pool and can be allotted to various applications and administrations powerfully. Contrasted and conventional disseminate system, a lot of speculation spared and it brings uncommon versatility, adaptability and proficiency for task execution. By using Cloud Computing administrations, the various undertaking interests in building and keeping up a supercomputing or lattice figuring condition for savvy applications can be effectively reduced.

In spite of these points of interest, security necessities drastically rise while putting away close to home recognizable on cloud condition [7], [8]. This raise administrative consistence issues since relocate the delicate data from unite space to convey area. To take the advantage empowered by big data advances, security and protection issues [9], [10] must be tended to initially.

Building security system for distributed storage isn't a simple errand. Since shared data on the cloud is outside the control space of real members, making the common data usable upon the interest of the authentic clients ought to be illuminated. Moreover, expanding number of gatherings, gadgets and applications associated with the cloud prompts the dangerous development of quantities of passageways, which makes it increasingly hard to take appropriate access control. Ultimately, shared data on the cloud are powerless against lost or inaccurately adjusted by the cloud supplier or system assailants. Shielding shared data from unapproved cancellation, alteration and manufacture is a difficult task.

2] LITERATURE SURVEY:

2.1] X. Wu, X. Zhu

Big Data concern enormous volume, perplexing, developing dataal collections with numerous, self-sufficient sources. With the quick improvement of systems administration, data stockpiling, and the data assortment limit, Big Data are presently quickly growing in all science and designing spaces, including physical, natural and biomedical sciences. This paper presents a HACE hypothesis that describes the highlights of the Big Data transformation, and proposes a Big Data preparing model, from the data mining point of view. This data driven model includes request driven conglomeration of data sources, mining and examination, client enthusiasm demonstrating, and security and protection considerations. We analyze the difficult issues in the data driven model and furthermore in the Big Data revolution.

2.2] Z. Fu, X. Sun

Numerous plans are proposed to make scrambled data accessible dependent on catchphrases. In any case, keyword-based search the semantic portrayal data of clients recovery, and can't totally meet with clients search goal. Accordingly, how to plan a substance based inquiry plan and make semantic hunt increasingly successful and setting mindful is a troublesome test. In this paper, we proposed an

inventive semantic inquiry plot dependent on the idea chain of command and the semantic connection between ideas in the scrambled datasets. All the more explicitly, our plan initially lists the records and manufactures trapdoor dependent on the idea progression. To additionally improve the pursuit productivity, we use a tree-based index structure to sort out all the report index vectors.

3] PROBLEM DEFINTION:

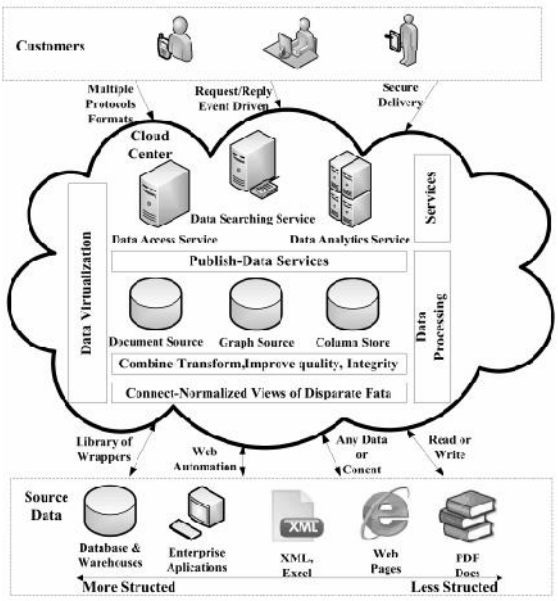
Rao [19] proposed a protected sharing plans of individual health records in cloud computing based on ciphertextpolicy attributed-based(CP-ABE) signcryption [20]. It center around limiting unapproved clients on access to the secret data. Liu et al. [21] proposed an entrance control strategy dependent on CP-ABE for individual records in distributed computing also. In [19] and [21],only one completely believed focal expert in the system is answerable for key management and key generation.

Huang et al. [22] presented a novel open key encryption with approved correspondence warrants on the entirety of its ciphertext or a predefined ciphertext. To fortify the making sure about necessity, Wu et al. [23] proposed an effective and secure personality based encryption plot with equity test in distributed computing. Xu et al. [24] proposed a CP-ABE utilizing bilinear matching to furnish clients with looking through capacity on ciphertext and fine-grained get to control. He et al. [25] proposed a plan named ACPC planned for giving secure, effective and fine grained data get to control in P2P storage cloud.

4] PROPOSED APPROACH:

In SSGK, an efcient arrangement is proposed to take care of the protected issues of data sharing on the distributed storage without depending on any trust outsider. Past utilizing symmetric encryption calculation [11] encrypt the shared data, asymmetric algorithm [12] and secret sharing plan [28], [29] is utilized to forestall the key used to decode the common data from getting by unapproved clients. Secret sharing plans were presented by both Blakley [30] and Shamir [31] autonomously in 1979 as answer for safe guarding cryptography keys. In a secret sharing plan, a secret is separated into n shares by a vendor and shared among n investors. Any t offers can recreate this secret.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

6.1] THE CLOUD PROVIDER:

Provides a public platform for data owners to store and share their encrypted data. The cloud provider doesn't conduct data access control for owners. The encrypted data can be download freely by any users.

6.2] DATA OWNER:

Defines the access policy and encrypts its data with a symmetric encryption algorithm using a group key. The group members who satisfied the access policy constitute a sharing group. Then secret sharing scheme is used by the owner to distribute the encryption key to the sharing group. Group members: every group member including the data owner is assigned with a unique and a pair of keys.

6.3] THE GROUP MEMBERS

Can freely get any interested encrypted data from the public cloud. However the user can decrypt the data if and only if it get the data decryption key from the data owner.

7] ALGORITHM:

Step 1: Start

Step 2: Every participant produces a pair of public key SKiand it sends public key to the provider.

Step 3: The data owner O produces group key K randomly and it encrypts the shared data D using then it uploads Cipher(D) to the cloud.

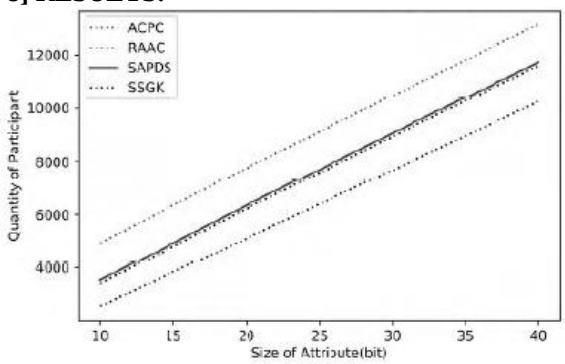
Cipher(D) = $AES_K(D)$

Step 4: The data owner generates a random polynomial F(x) of degree n-1.

Step 5: According to the secret sharing scheme, the data owner computes n sub-shares $s_1,s_2,\ldots\ldots,s_n$and the verified element V.

Step 6: After calculation, the data owner gets the public key from cloud provider and encrypts every sub-share siusing Cipher(si) = RSA_{PKi}(si)
step 7: Then, the encrypted sub-share and v are sent to i; i = 1,2,…..n throng point to point public channel.
Step 8:After key distribution protocol, every participant may get an encrypted sub-share si.
Step 9: Stop

8] RESULTS:



Communication overhead of ACPC, RAAC, SAPDS and SSGK.

9] CONCLUSION:
We propose a novel group key management convention for the data partaking in the distributed storage. In SSGK, we utilizes RSA and verified secret sharing to cause the data proprietor to accomplish fine-grained power over the redistributed data without depending on any outsider. What's more, we give point by point investigation of potential assaults and comparing guards, which exhibits that GKMP is secure under more vulnerable presumptions. Also we show that our convention displays less capacity and figuring intricacy. Security mechanism in our plan ensures the protection of networks data in cloud storage. Encryption secures the transmission on the open channel; checked security conspire make the matrices data just got to be approved parties. The better execution regarding capacity and computation make our plan progressively reasonable.

10] EXTENSION WORK:
The problem of forward and backward security in group key management may require some additions to our convention. An efficient dynamic mechanism of group members remains as future work

11] REFERENCES:
[1] P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin, ‘‘On minimizing energy cost in Internet-scale systems with dynamic data,’’ IEEE Access, vol. 5, pp. 20068–20082, 2017.

[2] D. Wu, G. Zhang, and J. Lu, ‘‘A fuzzy preference tree-based recommender system for personalized business-to-business E-services,’’ IEEE Trans. Fuzzy Syst., vol. 23, no. 1, pp. 29–43, Feb. 2015.

[3] X. Wu, X. Zhu, G.-Q.Wu, and W. Ding, ‘‘Data mining with big data,’’ IEEE Trans. Knowl. Data Eng., vol. 26, no. 1, pp. 97–107, Jan. 2014.

[4] X. Shi, L. X. Li, L. Yang, Z. Li, and J. Y. Choi, ‘‘Data flow in reverse logistics: An industrial data integration study,’’ Inf. Technol. Manage., vol. 13, no. 4, pp. 217–232, Dec. 2012.

[5] N. Bizanis and F. A. Kuipers, ‘‘SDN and virtualization solutions for the Internet of Things: A survey,’’ IEEE Access, vol. 4, pp. 5591–5606, May 2016.

[6] S. Li, L. Xu, X. Wang, and J. Wang, ‘‘Integration of hybrid wireless networks in cloud services oriented enterprise data systems,’’ Enterprise Inf. Syst., vol. 6, no. 2, pp. 165–187, Nov. 2012.

[7] K.-Y. Teng, S. A. Thekdi, and J. H. Lambert, ‘‘Risk and safety program performance evaluation and business process modeling,’’ IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 42, no. 6, pp. 1504–1513, Nov. 2012.

[8] Z. Fu, X. Sun, S. Ji, and G. Xie, ‘‘Towards efficient content-aware search over encrypted outsourced data in cloud,’’ in Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2016, pp. 1–9.

[9] J. Han, W. Susio, Y. Mu, and J. Hou, ‘‘Improving privacy and security in decentralized ciphertext-policy attribute-based encryption,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 665–678, Mar. 2015.

[10] D. Zou, Y. Xiang, and G. Min, ‘‘Privacy preserving in cloud computing environment,’’ Secur.

Commun.Netw., vol. 9, no. 15, pp. 2752–2753 Oct. 2016.

[11] Y. Tang, P. P. C. Lee, John C. S. Lui, and R. Perlman, ‘‘Secure overlay cloud storage with access control and assured deletion,’’ IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 903–916, Nov./Dec. 2012.

[12] J. Shao, R. Lu, and X. Lin, ‘‘Fine-grained data sharing in cloud computing for mobile devices,’’ in Proc. IEEE Conf. Comput.Commun. (INFOCOM), Apr./May 2015, pp. 2677–2685.

[13] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ‘‘Privacypreserving public auditing for secure cloud storage,’’ IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[14] S. Tanada, H. Suzuki, K. Naito, and A. Watanable, ‘‘Proposal for secure group communication using encryption technology,’’ in Proc. 9th Int. Conf. Mobile Comput. Ubiquitous Netw., Oct. 2016, pp. 1–6.

[15] J. Zhou et al., ‘‘Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation,’’ Comput. J., vol. 60, no. 8, pp. 1210–1222, Aug. 2017.

Mr.B.VenkateswaraRao is a student of Ideal College of Arts& Sciences, Kakinada. Presently he is pursuing his M.Sc in Computer Science from this college and he received his BSc (Computer Science) from Ideal college of Arts& Sciences, affiliated to AKNU University, Kakinada in the year 2017. His areas of interest includes Computer Networks and Object Oriented Programming languages, all current trends and techniques in Computer Science.

Mrs.P.RadhikaKrupalini is an Associate Professor of Computer Science Department at Ideal College of Arts & Sciences, Kakinada,AP, India. She obtained her MCA from Andhra University, M.Tech (CSE) from University College of Engineering, JNTUK. She qualified AP SET in Computer Science and Applications. She has 14+ years of teaching experience at Post Graduate Level. Her areas of interest are Operating Systems, Network Security & Cryptography, ArtificialIntelligence, Cloud computing, Data Mining and Software Engineering.