JES
Journal of Engineering Sciences

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

Minimizing Security and Privacy Risks of Shared Big Data in Cloud Environment

Mr Udayagiri Prasad[1], T Sai Praneeth[2], G V S D S Rama Sastry[3], G Srinivasulu[4], J Sai Kiran[5], K Venkateswara Rao[6]

1 Assistant professor, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
2,3,4,5,6 Students, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)

Abstract: Data contribution in the cloud is a procedure so as to allow users to expediently right of entry information in excess of the cloud. The information holder outsources their data in the cloud due to cost lessening and the huge amenities provided by cloud services. Information holder is not able to manage over their information, since cloud examination contributor is a third party contributor. The main disaster with data partaking in the cloud is the seclusion and safety measures issues. Different techniques are obtainable to sustain user seclusion and protected data sharing. This paper focal point on different schemes to contract by means of protected data partaking such as information contribution with forward security, protected information partaking for energetic groups, quality based information partaking, encrypted data sharing and mutual influence Based Privacy-Preserving verification set of rules for right to use manage of outsourced information.

INDEX TERMS Big data, security and privacy, cloud storage, data sharing

I. INTRODUCTION

The emerging technologies about big data such as Cloud Computing [1], Business Intelligence [2], Data Mining [3], Industrial Information Integration Engineering (IIIE) [4] and Internet-of-Things [5] have opened a new era for future Enterprise Systems (ES) [6]. Cloud computing is a new computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically. Compared with traditional distribute system, a considerable amount of investment saved and it brings exceptional elasticity, scalability and efficiency for task execution. By utilizing Cloud Computing services, the numerous enterprise investments in building and maintaining a supercomputing or grid computing environment for smart applications can be effectively reduced. Despite these advantages, security requirements dramatically rise when storing personal identifiable on cloud environment [7], [8]. This raise regulatory compliance issues since migrate the sensitive data from federate domain to distribute domain. To take the benefit enabled by big data technologies, security and privacy issues [9], [10] must be addressed firstly.

Building security mechanism for cloud storage is not an easy task. Because shared data on the cloud is outside the control domain of legitimate participants, making the shared data usable upon the demand of the legitimate users should be solved. Additionally, increasing number of parties, devices and applications involved in the cloud leads to the explosive growth of numbers of access points, which makes it more difficult to take proper access control. Lastly, shared data on the cloud are vulnerable to lost or incorrectly modified by the cloud provider or network attackers.

Protecting shared data from unauthorized deletion, modification and fabrication is a difficult task.

Conventionally, there are two separate methods to promote the security of sharing system. One is access control [11], in which only authorized user recorded in the access control table has the access privilege of the shared data. The other method is group key management [12] _ [16] in which a group key is used to protect the shared data. Although access control makes the data only be accessed by legitimate participants, it cannot protect the attack from cloud providers. In the existing group key sharing systems, the group key is generally managed by an independent third party. Such methods assume that the third party is always honest. However, the assumption is not always real especially in the environment of cloud storage.

To address the security problem of sharing data on the cloud storage, a secret sharing group key management protocol is proposed in the paper and the following means are taken by our protocol to help detect or prevent frauds. Firstly, in order to make the shared data usable upon demand by the legitimate users, symmetric encryption algorithms [17] are used to encrypt the shared data. Once one data owner wants to share data with others, the decryption key is distributed to the legitimate sharers by the data owner. Secondly, the key used to decrypt the shared data controls the access permission for shared data. Asymmetric encryption algorithms [18] are used to encrypt the interactive message and makes only legitimate participants have the ability to decrypt the key. Thirdly, in case of shared data being known by unauthorized users, this protocol uses secret sharing scheme to assign key to the legitimate participants. By adding security mechanism to conventional service oriented clouds, we obtain a security aware cloud and guarantee the privacy of data sharing on cloud storage. Building security mechanism on cloud storage may accelerate the deployment of a cloud in mission critical business scenario.

II. RELATED WORK

Many solutions had been proposed to clear up the privateness risks of cloud-based totally storage.

Rao [19] proposed a secure sharing scheme of private fitness facts in cloud computing based totally on ciphertext policy attributed-primarily based (CP-ABE) signcryption [20]. It recognition on restricting unauthorized customers on get entry to the confidential records. Liu et al. [21] proposed a get admission to manipulate policy based totally on CP-ABE for non-public information in cloud computing as nicely. In [19] and [21], only one completely depended on primary authority within the system is accountable for key management and key era.

Huang et al. [22] added a unique public key encryption with legal equality warrants on all of its ciphertext or a specified ciphertext. to bolster the securing requirement, Wu et al. [23] proposed an efficient and cozy identification-based encryption scheme with equality take a look at in cloud computing. Xu et al. [24] proposed a CP-ABE using bilinear pairing to offer customers with looking capability on ciphertext and ne-grained get admission to manipulate. He et al. [15] proposed a scheme named ACPC aimed toward presenting comfy, efficient and engrained records get admission to manage in P2P garage cloud. Currently, Xue et al. [16] proposed a new framework, named RAAC, to eliminate the single-factor overall

performance bottleneck of the exiting CP-ABE based totally get admission to manage schemes for public cloud garage. While these schemes use identification privateness by the usage of characteristic-based techniques which fail to guard person attribute privacy.

The most recent paintings addressing the privateness issues in a cloud-primarily based storage is completed by means of Pervez et al. [17], who proposed a privateness aware facts sharing scheme SAPDS. It combines the characteristic primarily based encryption at the side of proxy re-encryption and secret key updating functionality without depending on any depended on 0.33 birthday party. But the storage and communique overhead of SAPDS is decided by characteristic encryption scheme.

In SSGK, an efficient solution is proposed to clear up the comfortable issues of statistics sharing at the cloud storage without relying on any believe 0.33 celebration. past the usage of symmetric encryption set of rules [11] to encrypt the shared statistics, uneven algorithm [12] and secret sharing scheme [18], [9] is used to save you the key used to decrypt the shared information from getting by using unauthorized users. Secret sharing schemes had been brought by way of each Blakley [10] and Shamir [11] independently in 1979 as answer for secure guarding cryptography keys. In a secret sharing scheme, a key's divided into n stocks via a supplier and shared amongst n shareholders. Any shares can reconstruct this mystery. Chor et al. [12] prolonged the perception of the authentic mystery sharing and provided a perception of verifiable secret sharing (VSS). The asset of verifiability means that shareholders are able to verify whether their shares are regular.

III. SECURED CLOUD STORAGE IN BIG DATA ERA

The structure of cloud primarily based large information is illustrated in figure.1. It includes three elements: source information, cloud center and offerings. Among supply statistics and cloud center layer, unstructured or semi-dependent source facts are structured. They include processing methods together with statistics series [13], records mining [14] and statistics aggregation [15]. The processed source statistics is saved on cloud in relational or NoSQL databases [16]. Ultimately, service layer solutions information requests submitted by customers via integrating facts saved in cloud.

Beyond permitting customers to place all facts into cloud, cloud garage presents all types of information services for customers. due to the fact scale horizontally runs on cheap commodity hard in a disbursed conjuration and there may be no need for clients to buy and preserve their very own IT centers, cloud based totally big records stores brings in inherent availability, scalability and price effectiveness.

AN EXAMPLE OF HEALTHCARE INFORMATION SYSTEM

Cloud garage gives now not simply low price, however high scalability and availability. It is able to be a herbal option to some of troubles in storing and studying the growing patients' clinical statistics [17]. For healthcare vendors, simplest based on the aggregation of all sufferers' scientific statistics, ought to proper diagnosis be made. Reference [18] proposed a cloud primarily based platform for healthcare. Cloud storage affords a not unusual

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

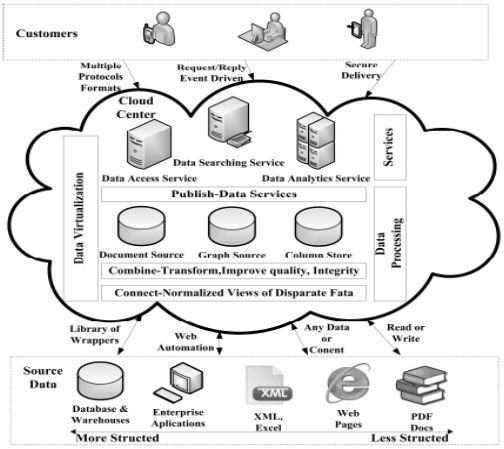

FIGURE 1. Cloud storage architecture for big data

area for storing scientific statistics which conquer the delay of shifting medical information among distinct healthcare vendors and make diagnostic procedure more efficient. The e-healthcare cloud offers many benefits in collaboration and facts sharing amongst healthcare providers. However, in remember of the exceptionally privacy of medical data it comes with significant dangers of scientific data. First of all, medical statistics are shared on the public channel where many attackers at the channel to eavesdrop the scientific statistics. Additionally, due to the growing quantity of events, devices and applications concerned in cloud, unauthorized parties or cloud providers may have the ability to get entry to shared medical records. Remaining however not the least, some legal events may fit collectively to get some unauthorized clinical statistics illegally. E-healthcare services require a safety mechanism to guard the privacy of medical facts.

IV. THE PROPOSED SSGK PROTOCOL

On this phase we describe more approximately the proposed protocol model and algorithm of SSGK.

A. PROTOCOL MODEL

1) Data Sharing Model

Don't forget a cloud garage records sharing system with more than one entities and the information sharing model is shown as figure.2. The protocol version includes 3 varieties of entities: cloud issuer, information proprietor and organization contributors. The cloud company: affords a public platform for records proprietors to keep and share their encrypted data. The cloud company does not behavior records access control for proprietors. The encrypted data can be downloading freely with the aid of any users.

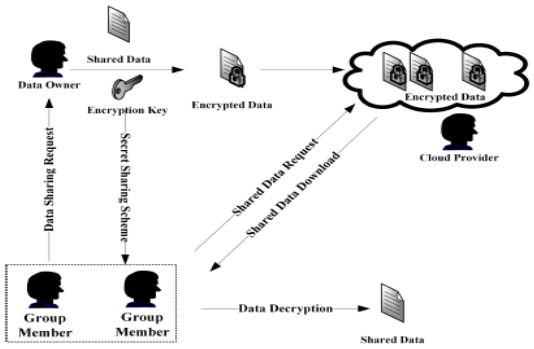

FIGURE 2. Data protocol model of the proposed SSGK.

Data owner: defines the get right of entry to coverage and encrypts its records with a symmetric encryption algorithm the use of a group key. The organization participants who satisfied the get admission to coverage represent a sharing organization. Then mystery sharing scheme is utilized by the owner to distribute the encryption key to the sharing institution.

Organization members: each institution member inclusive of the records proprietor is assigned with specific and 2 keys. The organization individuals can freely get any interested encrypted statistics from the general public cloud. However the person can decrypt the facts if and simplest if it get the records decryption key from the information proprietor.

2) PROTECTION MODEL

In SSGK, we have the following assumptions:

The information proprietor is completely relied on and will in no way be corrupted through any adversaries. Cloud issuer is semi-trusted, it correctly executes the challenge assigned to them for profits, but they would try and find out as a good deal mystery facts as feasible based totally on the data owner's uploaded facts. We now describe the security version of SSGK by way of list possible assaults. The group key is shipped by strolling the name of the game sharing scheme. Elements of the institution individuals can collect their sub secret stocks to reconstruct the organization key.

B. DEFINITIONS AND NOTATIONS

Definition 1 ((t,n)VSS): A verified mystery sharing scheme contains four steps:

Sharing technology algorithm: An algorithm that, on enter a protection parameter okay and a random polynomial f (x) of diploma t - 1, output n sub-stocks and a verified value v; Distribution: The provider distributes each sub-percentage and v to every scheme participant secretly,

TABLE 1. Notations.

Notation	Description for the Notation
O	data owner
D	shared data
K	group key used to encrypt shared data
P_i	Group member P with indentified ID_i
$cipher(x)$	Cipher-text of x
$E_k(P)$	encrypt P with key k using encryption algorithm E
$E^{-1}{}_k(C)$	decrypt C with key k using decryption algorithm E^{-1}
SK_i	Secret key of P_i
PK_i	Public key of P_i

Verify: A verification set of rules that, on enter a sub-percentage and v, output whether the sub-share is tempered at some stage in distribution; mystery Reconstructed: For any t sub-stocks, the safety parameter ok may be reconstructed.

Definition 2 (fairness and Availability): Verified mystery sharing scheme guaranteeing equity and availability with two conditions: Any player set in the percentage group, wherein the size of the set is much less than the overall amount, the members in the set can't get any records approximately ok; handiest with cooperation of all the legitimate participants, ok may be reconstructed.

Definition 3 (Condentiality): Verified secret sharing scheme ensures condentiality if any users out of doors the sharing group cannot get any facts of okay inspire of the know-how of sufficient interactive messages.

C. PROTOCOL DETAILS

The scene describes as a protocol player O wishes to share facts D with the legitimate members Pi; i = 1; 2; : : : ; n. first off, O generates a mystery key ok and uses okay to encrypt D, then O stores the encrypted statistics cipher(D) to the cloud. Secondly, O stocks ok with the legitimate members and all individuals paintings collectively to certify and reconstruct okay. Subsequently, each player gets okay and downloads cipher (D) from the cloud. The exact technique of SSGK is proven as Figure.3.

The statistics proprietor O creates the secret key and encrypts the statistics the usage of symmetric encryption set of rules AES. Then secret sharing scheme is used by *O* to distribute the secret key. As the public channel is available for communications among each pair of contributors, an asymmetric encryption algorithm RSA is used to protect the important thing sub-stocks from known

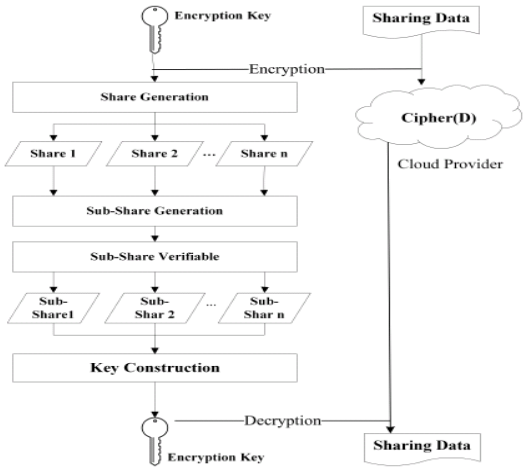

FIGURE 3. Data sharing model of the proposed SSGK protocol.

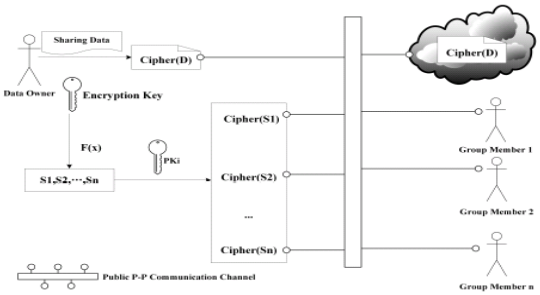

FIGURE 4. Data sharing model of the proposed SSGK protocol

DATA SHARING MODEL OF THE PROPOSED SSGK PROTOCOL

By means of unauthorized customers. The distribution protocol is summarized as accompanied steps and proven as determine.4.

KEY RECONSTRUCTION AND VERIFICATION

All the individuals may get Cipher (D) and v from the point to-factor public channel. The subsequent aim of the individuals is to reconstruct k with collaboration and to confirm whether or not there are any corrupted contributors. The stairs of the reconstruction protocol are described as follows:

Step 2: every player Pi; i = 1; 2; : : : ; n except for O calculates Ki, a duplicate of k, and V using Lagrange Interpolating formulation. Then, it computes V mod Ki, if VmodKi 6D v, it will broadcast that there are compromised participants; in any other case, it's going to send its identity encrypted with sj to the cloud company for facts get right of entry to permission. As Pi calculates the institution key ok, it can download the Cipher(D) from cloud and decrypts it by okay the usage of equation.

$$D = AES^{-1}{}_{K}\,(Cipher(D))$$

Thru above steps, ok used to encrypt the shared records is disbursed to the contributors secretly thru public channel and shared records is decrypted by means of legal members. Our sharing protocol protects the shared statistics from being known by using the cloud company and unauthorized customers.

V. SECURITY ANALYSIS AND PERFORMANCE

A. safety evaluation

Risks exist in both the sharing information distribution section and the everyday broadcast phase. On this section we cope with a few security properties of SSGK with the aid of showing some theorems. SSGK should guarantee equity and availability.

Proof of Theorem: for you to prove that our protocol guarantees fairness and availability, in keeping with definition three, we need to show that the net to be had m members cannot get any statistics about k while m < n. in which n stands for the potential of this sharing institution. There are participants online, they cloud calculate *m* sub shares s1; s2; : : : ; sm the usage of equation 2. The group key ok D F(zero) D a0 may be calculated as follows the usage of determinant operation:

$$\begin{pmatrix} 1^0 & 1^1 & 1^2 & \dots & 1^n \\ 2^0 & 2^1 & 2^2 & \dots & 2^n \\ & & \dots & & \\ m^0 & m^1 & m^2 & \dots & m^n \end{pmatrix}, \quad |A| = \begin{cases} = 0, & \text{if } m < n \\ \neq 0, & \text{if } m = n \end{cases} \tag{9}$$

step2:

$$A \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_n \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \dots \\ s_m \end{pmatrix} \tag{10}$$

The value of okay which now not be calculated as A^{-1} does now not exist while m < n, in order that the available m members cannot get any facts of k.

B. performance

In this phase, we offer the performance assessment of the proposed protocol. The subsequent experiments recognition on the garage and computation overhead of SAPDS and the proposed protocol SSGK. These experiments are going for walks on a server with Intel center 2, 2.93GHz twin middle processor and 2GB RAM.

1) Contrast ON safety

This segment places forwards targeted comparison on various protection and functionality capabilities of the proposed scheme with a few currently developed CP-ABE primarily based schemes. For evaluation, we don't forget associated schemes ACPC [15], RAAC [16], and SAPDS [17]. Table3 tabulates the evaluation results on numerous protection attributes. It's far stated that our scheme helps many useful residences, which include data equity, condentiality and integrity protection, collusion resistance and privateness safety.

2) Storage Overhead

The storage overhead of ACPC, RAAC, SAPDS and SSGK is tested in order to evaluate their scalability. The variety of personal and public keys of those schemes is counted. We count on that the variety of the group individuals is n and the key length is L bits. Private keys constitute the storage consumption on one group members in protocol. InACPC, mystery key and user attributes are used to compute the encryption key. In RAAC, more than one CAs are used for key era, 4 kinds of unique keys are saved by users: the symmetric set of rules key to decrypt shared records, user's mystery characteristic based key, person attributes and CA verified keys(Six CAs are simulated in our test).

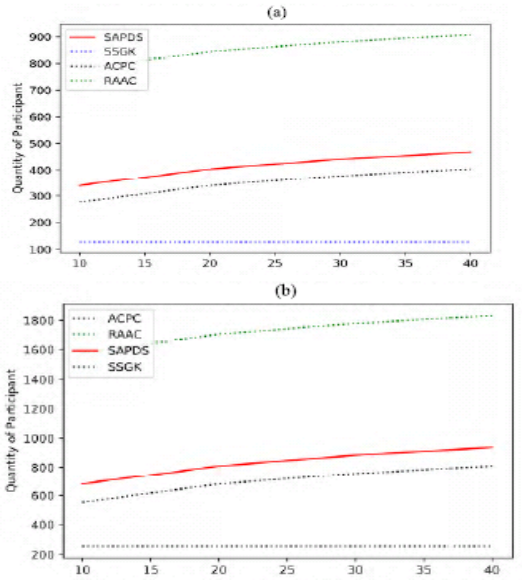

Figure 5 Storage overhead of ACPC,RAAC, SAPDS and SSGK.

Figure.5 (a)(b) suggests the exchange of storage overhead of those schemes with the ability of participant varies from 10 to 50 and the dimensions of attribute length varies from 64bits to 256bits. information imply that once the size of characteristic grows, the difference price rises rapid, while the range of participant has letter influence on storage value in SSGK. Public keys constitute the garage overhead on cloud provider.

In ACPC, the cloud offer shops n public keys for customers and attributes of a get admission to tree. In RAAC, the cloud gives stores attributes of a get entry to tree, public keys of the organization contributors and 6 CAs. In SAPDS, cloud provider shops the encrypted key used to decrypt the shared

information, public keys of the organization participants and attributes of a get entry to tree.

3) Communication Overhead

The first step in SSKG is generating a key ok, a random polynomial F(x) of degree n and computing n sub-stocks. The first venture of ACPC, RAAC and SAPDS is defining a get right of entry to coverage which the name of the game k is hid. The subsequent step in those four schemes is retrieving the secret key ok. In SSGK, contributors execute mystery sharing scheme to distribute k and CP-ABE is accomplished by way of the contributors of ACPC, RAAC and SAPDs. Key era and distribution are wished by using the schemes to get okay. The verbal exchange overhead on those schemes incorporates components: key era instances and key distribution times. And the time is decided via the capacity of the sharing group.

Figure.6 (a) illustrates the time taken via ACPC, RAAC, SAPDS and SSGK to generate key. The era time is shown to be trusted the number of organization individuals. It takes at maximum 14s to generate group key via RAAC, however it simply take at most 143ms by way of SSGK. About ninety eight percent of technology time is saved.

Figure.6 (b) illustrates that the distribution instances with six exclusive participants over 128bits of and 512bits of individuals' public key. Proven in the figure, associated with the quantity of participants, ACPC, RCCA and SAPDS have a tendency to eat more instances as compared with SSGK.

Figure.6(c) indicates the total computation price with six unique contributors. Approximately ninety five% of general times are stored with the aid of SSGK than RAAC. SSGK does no longer depend upon any 1/3 party to manipulate the key management. Schemes primarily based on CP-ABE delegate key management to cloud server might also raised same safety

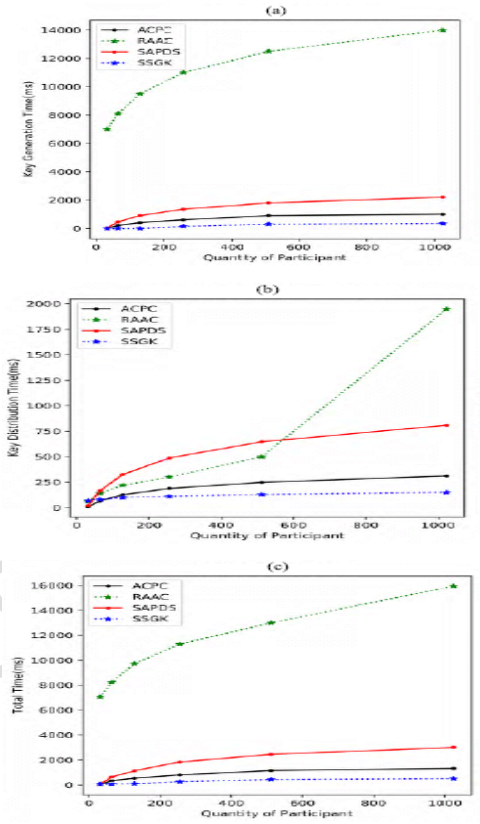

FIGURE 6. Communication overhead of ACPC, RAAC, SAPDS and SSGK.

Issues as noted earlier than. And the simulation consequences show that our protocol incurs less storage computation overhead. The evaluation result highlights the truth that SSGK enables the owner to preserve fine-grained manage over the outsourced data with minimum charges.

VI. CONCLUSION

In this paper, we propose a novel group key management protocol for the data sharing in the cloud storage. In SSGK, we use RSA and verified secret sharing to make the data owner achieve fine-grained control over the outsourced data without relying on any third party. In addition, we give detailed

analysis of possible attacks and corresponding defenses, which demonstrates that GKMP is secure under weaker assumptions. Moreover we demonstrate that our protocol exhibits less storage and computing complexity. Security mechanism in our scheme guarantees the privacy of grids data in cloud storage. Encryption secures the transmission on the public channel; verified security scheme make the grids data only accessed by authorized parties. The better performance in terms of storage and computation make our scheme more practical. The problem of forward and backward security in group key management may require some additions to our protocol. An efficient dynamic mechanism of group members remains as future work.

VII. REFERENCES

[1] M. Qiu, K. Gai, B. Thuraisingham, L. Taob, H. Zhao, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in the financial industry", ELSEVIER Future Generation Computer Systems, Vol. 80, pp. 421-429, 2018.

[2] Mitchell G. Goldenberg, Teodor P. Grant charov, "Enhancing Clinical Performance and Improving Patient Safety Using Digital Health", In Springer Digital Health. Health Informatics, pp 235-248, 2018.

[3] Y. Wang, B. Rawal, Q. Duan, "Securing Big Data In the Cloud with Integrated AuditIng", IEEE International Conference on Smart Cloud (SmartCloud) Pgs. 126 - 131, 2017.

[4] M. Dieye, M. F. Zhani, H. Elbiaze, "On achieving high data availability In heterogeneous cloud storage systems", IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Pgs. 326 - 334, 2017.

[5] Z. Liu, Z. L. Jiang, X. Wang, S. M. Yiu, C. Zhang, X. Zhao, "Dynamic Attribute-Based Access Control In Cloud Storage Systems", IEEE Trustcom/BigDataSE/ISPA, Pgs. 129 - 137, 2016.

[6] W. Li, K. Xue, Y. Xue, J. Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System In Public Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2016.

[7] M. Anisetti, C. Ardagna E. Damiani, F. Gaudenzi, "A semi-automatic and trustworthy scheme for continuous cloud service certification" IEEE Transactions On Services Computing, 2016.

[8] V. Chang, M. Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, 2015.

[9] B. Dong, R. Liu, Hui Wang, "Trust-but-Verify: Verifying Result Correctness of Outsourced Frequent Itemset Mining In Data-mining-as-a-service Paradigm", IEEE Transactions on Services Computing, 2015.

[10] N. A. Kofahi, A. R. Al-Rabad, "Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey", Advances in Networks, 6(1): 1- 13, 2018.

[11] I. Ahmad, H. Bakht, and U. Mohan, "Cloud Computing – Threats and Challenges", Journal of Computer Management Studies, vol. 1, no. 1, 2017.

[12] P. Johri, A. Kumar, S. Das, S. Arora, "Security framework using Hadoop for big

data", International Conference on Computing, Communication and Automation (ICCCA) Pgs. 268 - 272, 2017.

[13] W. Tang, K. Zhang, J. Ren, Y. Zhang, X. Shen, "Lightweight and Privacy-Preserving Fog-Assisted Information Sharing Scheme for Health Big Data", IEEE Global Communications Conference (GLOBECOM 2017) Pgs. 1 - 6, 2017.

[14] S. LIns, P. Grochol, S. Schneider, and A. Sunyaev, "Dynamic Certification of Cloud Services: Trust, but Verify", IEEE Computer and Reliability Societies, 1540-7993/16, 2016.

[15] F. Corradini, F. Angelis, F. Ippoliti and F. Marcantoni, "A Survey of Trust Management Models for Cloud Computing", In 5th International Conference on Cloud Computing and Services Science, Pgs. 158-162, 2015.

[16] P. Mell, T.Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.

[17] T. Noor, Q. Sheng, L. Yao, S. Dustdar and A. Ngu. "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE transactions on parallel and distributed systems, Vol. 27, no. 2, Pgs. 367-380, 2015.

[18] C. Yanli, S. Lingling,and Y. Geng, "Attribute-Based Access Control for Multi-Authority Systems with Constant Size Ciphertext in Cloud Computing Computing", IEEE, China Communications, Vol. 13, Pg. 146 - 162, DOI-10.1109/CC.2016.7405733, 2016.

[19] Y. S. Rao, M. Wang, X. Liu, and J. Sun, "Efficient distributed access control for big data in clouds", Proc. - IEEE INFOCOM, vol. 20, no. BigSecurity, pp. 202– 207, 2015.

[20] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A. Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method", IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 4, 2016.

[21] K. Liang, W. Susilo, and Joseph K. Liu, "PrivacyPreserving Ciphertext Multi-Sharing Control for Big Data Storage", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, 2015.

[22] S. Wang, J. Zhou, Joseph K. Liu, Jianping Yu, J. Chen, WeixinXie, "An Efficient File Hierarchy AttributeBased Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, Volume:11, Issue: 6, 2016.

[23] J. E. Vascellaro, "Google Discloses Privacy Glitch. English. Wall Street Journal", LInk: http://blogs.wsj.com/digits/2009/03/08/1214/, 2009.

[24] J. K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang, "TwoFactor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, 2015.

Authors Profile

Mr Udayagiri Prasad working as an Assistant Professor in the Department of Computer Science & Engineering in QIS Institute of Technology, Ongole, Andhra Pradesh, India.

Vol 11, Issue 5, MAY /2020
ISSN NO:0377-9254

T Sai Praneeth pursuing B Tech in Computer Science Engineering from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

G V S D S Rama Sastry pursuing B Tech in Computer Science Engineering from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

G Srinivasulu pursuing B Tech in Computer Science Engineering from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

J Sai Kiran pursuing B Tech in computer science engineering from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

K Venkateswara Rao pursuing B Tech in Computer Science Engineering from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively