A Survey on Security and Privacy Using Block Level for Group Sharing in Health Care System

Saudamini S. Deshmukh[1], Prof. Geetha R. Chillarge[2]
[12]Department of Computer Engineering
[12]Marathawada Mitra Mandal's College of Engineering
[12]Pune, India

Abstract- Now a days cloud computing plays a vital role as the number of connected devices are increasing and also the computing and storage for the data is necessary. Security of the cloud is also a major concern as the data storage is in high scale on cloud. The security has become a big challenge which has to be addressed properly to maintain the privacy of the data. Several new technologies are introduced to keep track of the cloud services securely as well as efficiently. This paper discusses some cloud services regarding security and many algorithms are used to secure the cloud data.

Index Terms- Cloud storage, Cloud Security, Data sharing, Key management, Block level.

I. INTRODUCTION

Cloud is a basically a huge source to store the data and that data can be accessed remotely anywhere anytime. Now a day's rapid development of cloud computing in smart health care system has significantly improved the quality of health. However data security and user privacy are in concern for smart health care system. These days any kind of data can be used for malicious purposes. Many harmful entities constantly try and gain access to the personal data of internet users. This data includes sensitive information that doctors store of patients and is often stored using some kind of third party cloud providing service that is not very secure.But as the huge database is stored on the cloud security also needs to be considered for securing data efficiently. In this paper . The security challenges and problems are considered and many techniques are introduced to overcome them.

II. REVIEW OF LITERATURE

This system newly introduces the concept of smart health which is the context-aware complement of mobile health within smart cities and is very efficient [1]. The smart health is nothing but the technology which leads to good diagnosis of health using smart tools and best treatments. System provide an overview of the main fields of knowledge that are involved in the process of building this new concept. Additionally, the author discuss the main challenges and opportunities that s-health would imply and provide a common ground for further research. This system improves policy decisions and cost saving. But sometimes online predictions also causes failure.

Cloud computing plays an important role in IOT [2]. In this System, the service perspective is considered and quality model named CLOUDQUAL for cloud services is initiated. This model contains quality dimensions that focuses on general cloud services. CLOUDQUAL contains six quality dimensions and they are usability, availability, reliability, responsiveness, security, and elasticity, from which usability is subjective, while the others are objective. To demonstrate how effective the CLOUDQUAL is system conducts empirical case studies on three storage clouds. System uses the IDEA and MD5 algorithm. The results show that CLOUDQUAL can evaluate their quality. To demonstrate the soundness of it, the author has validated CLOUDQUAL with standard criteria and shows that it can differentiate service quality. This system provides a quality model for cloud services, called CLOUDQUAL, which specifies six quality dimensions and five qualities metric and Security. But the main drawback is that offer an infinite amount of storage space.

This system introduces a new type of IBE scheme [3]. This is called Fuzzy Identity-Based Encryption. In Fuzzy IBE author defines set of descriptive attributes. This scheme uses a private key for an identity, and decrypt a cipher text which is encrypted. Anytime a biometric identity is sampled it will have some noise. The results shows that fuzzy IBE scheme is used to enable encryption as it mainly has error tolerance properties. Here, the MD5 algorithm is used for security purpose and system defines that Fuzzy-IBE can be used for applications that term "attribute-based encryption". For fault tolerance Scheme the Error tolerance property is used.

This system focuses on the encryption of data based on the attributes [4]. More and more confidential information is shared and stored by third-party sites on the web every day. Therefore there is a need to encrypt data that has stored at those sites. In this system a new system of cryptography is developed for easy sharing of encrypted data that we can say Key-Policy Attribute-Based Encryption (KP-ABE).This system has cipher texts. These cypher texts are tagged with sets of attributes. Private keys are linked with access structures. These access structures have control of cipher texts. The user can decrypt these access structures. The fully homomorphism encryption algorithm is introduced and the system demonstrates the applicability of author's construction to share the audit-log information and broadcasts the encryption. Author's construction helps proper distribution and assigning of private keys which absorbs HIBE. Coarse-grained level encryption and generated the private key but private key is not secure.

This System constructs such a scheme for predicates corresponding to the evaluation of inner products over ZN (for some large integer N) [5]. This, enables constructions in which the predicates correspond to the evaluation of disjunctions, polynomials, CNF/DNF formulae, or threshold predicates (among others). Besides serving as a significant step forward in the theory of predicate encryption, the results lead to a number of applications that are interesting in their own right. Polynomial Equations and inner products. disjunctions, polynomials, CNF/DNF formulae are work on the single work.

Security challenges in the cloud is the newest term which defines a long dreamed vision of computing as a utility[6]. In this system the cloud provides a convenient on demand network for accessing the pool of computing resources which are centralized and configured. These resources can be sent with great efficiency. This system provides Public cloud is used when the data are stored in greater efficiency**.** The main disadvantage of system is no trustworthy public cloud environment is there.

This system introduces a provable data possession model which allows a client who has stored his data at an untrusted server to verify that the server contains the original data without fetching it from its location [7]. This model creates probabilistic proofs of possession by simply sampling random sets of blocks from the server, which reduces huge input output costs. The client has the data required for verification of proof. The main disadvantage of the system is that original data can be retrieved easily.

In this system with the help of cloud storage, users can store their data remotely and can enjoy the high demand quality applications and services from the computing resources which are available in a shared manner[8]. Local data storage and maintenance need not be considered. Integrity checking is used. This system's drawback is only own file access control is there.

A POR scheme authorizes an archive or backup service to produce an incisive proof that a user can retrieve a target file F, that is, the archive keeps and accurately sends the file data[9]. This data is sufficient for the user to recover F completely. Earlier techniques of cryptography helped users to confirm the privacy and integrity of the files they retrieved. User wants to confirm that archives do not delete or change files before they are retrieved. This system displays that a file can be retrieved within a specific time period.

This system mainly focuses on how to deal with the client's key exposure while storing the data on the cloud[10]. Here, system's goal is on the key exposure avoidance using the new standard called auditing protocol. In this protocol the updation of keys is done after every sharing of data. System used the concept of binary tree and stack in it for the secured storage of the data. The integrity of the data stored in the cloud cannot be integrated easily.

In this system to overcome the issue of key exposed and security lost, the key-exposure resilience scheme is introduced[11]. In existing scheme, the data from the cloud can be illegally accessed later than the key-exposure time period using the same secret key had been provided for auditing the cloud data. An innovative paradigm called strong key-exposure resilient auditing for secure cloud storage which allows to set a particular time period for the key exposure. This preserves the security of the cloud not only earlier but also later than the key exposure time period.

This system uses the RDIC processwhich makes use of OTP for providing enhanced level of data integrity and security[12]. Along with the use of OTP a particular time session is provided to every user which makes the users to use the OTP in an efficient manner with the maintained security. For sharing the files securely the OTP will be generated and issued to the selected clients via e-mail ID which will be sent usingSMTP protocol. This protocol is low in cost and the delivery of the messages will be done in very faster manner. In addition to this the security is provided at both the front end, as well as back end. The back end security is provided by storing of the data in an encrypted format. For this two algorithms are being used, Blowfish algorithm and AES algorithm. By combining these two Algorithms the back end security is achieved very efficiently.

Now a days, many users used to store their data in cloud[13]. To ensure the security of the cloud and stored data users used many encryption techniques. The security of data has always been an aspect of quality, cloud computing cause a new security threats. In cloud storage systems, the server which stores the user's data is not always trusted. In this system high security is provided which can provide security against for Collusion attack, DDOS attack. As the previous data auditing schemes have security risks in processing of data. To achieve the efficiency of cloud storage, the proposed system provides flexible data segmentation with additional authorization process among the three participating parties of client, server and a third-party auditor.

In this system an IDEA algorithm is used[14]. IDEA is an universal algorithm which is used for block cipher encryption Which allows the effective protection of transmitted and stored data against unauthorized access by third parties. The basic criteria for developing the IDEA algorithm is military strength for all the security requirements and easy hardware and software implementation. This algorithm is used worldwide in various banking as well as industry applications. They redesign the algorithm for use in a great number of commercial applications. Here, in this system the IDEA algorithm is used for securing cloud data.

In this system the enhanced RSA method is used for the ensuring the storage correctness of the remote data stored in the server[15]. This provides the evaluation of service quality of the stored data in cloud computing. The ENHANCED RSA method also overcomes the problem of variable size file blocks. This method is much secured as there are two levels of authentications used. Hence there are more chances of detecting the file blocks that are missing or deleted from the remote server. It also supports insertion, modification and deletion as the classic Merkle Hash Tree for block tag authentication is improved. After performing the data correctness checking the future work is to reduce the latency in accessing the file stored in the remote server. Moreover, the communication overhead takes place in using the ENHANCED RSA method needs to be considered in future. The support of data insertion, deletion and modification are to be checked using the real time applications.

Sr No.	Title	Author	Technology	Advantages	Disadvantages
1.	"Smart health: a context-aware health paradigm within smart cities," *IEEE Communications Magazine,* vol. 52, no. 8, pp. 74-81, 2014.	Solanas, C.Patsakis, M. Conti, I.S. Vlachos, v. Ramos, F.falcone, O.Postolache, P. A. Prez-Martnez, R. Di Pietro, D. N. Perra et al.,	Predication Methods (random Forest).	Improving Policy Decisions and Cost Saving.	Online Predication sometime failure.
2.	"Cloud Quall: A Quality Model for Cloud Services". *IEEE transactions on industrial informatics,*vol.10, no.2, pp.1527-1536,2014.	X. Zheng, P. Martin, K.Brohman, and L. Da Xu,	DEA and MD5 Algorithms.	specifies six quality dimensions and five qualities metric for Security.	Vulnerable to attacks.
3.	"Fuzzy Identity-Based Encryption". *in Advances in Cryptology*, pp.557-557,2005	X. Zheng, P. Martin, K.Brohman, and L. Da Xu	ABE Algorithms and MD5	Attributed based encryption (ABE) and Fuzzy Identity-Based Encryption	Error tolerance property is used for fault tolerance Scheme.
4.	"Attributed – based encryption (ABE) and Fuzzy Identity-Based Encryption". in Proceedings *of ACM Conference on Computer and Communications Security,* (CCS'06), pp. 89-98, 2006.	V. Goyal, O. Pandey, A. Sahai, and B. Waters,	Fully Homomorphism encryption algorithms	Key-Policy Attribute-Based Encryption (KP-ABE) and Hierarchical Identity-Based Encryption (HIBE).	coarse-grained level encryption
5.	"Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proceedings of *International Conference on the Theory and Applications of Crypto-graphic Techniques (EUROCRYPT08),* pp.146-162 2008.	J. Katz, A. Sahai, and B. Waters,	CNF and DNF Formula	Polynomial Equations and inner products.	disjunctions, polynomials, CNF/DNF formulae are work on the single work.
6.	"Security challenges for the public cloud," *IEEE internet compute.,* volume. 16, no.1, pp. 6973, January. 2012.	K. Ren, C. Wang, and Q. Wang,		Public cloud is used when the data are stored in greater efficiency.	No trustworthy public cloud environment.
7.	"Provable data possession at untrusted	G. Ateniese et al.,	Random block	Provable data	Original data is

	stores, in Proc," 14th ACM *Conf. Compute. Communication. Security*. pp. 598-609, 2007.		generation	possession is used.	retrieved easily.
8.	"An efficient and fine-grained big data access control scheme with privacy-preserving policy," *IEEE Internet of Things Journal*, volume. 4, no. 2, pp. 563-571, 2017.	K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen,	Ciphertext-policy attribute-based encryption	Integrity checking is used.	Only own file access control is there.
9.	"Pors: Proofs of retrievability for large files,". *14th ACM Conf. Comput. Commun. Secur.*, pp. 584-597, 2007.	A. Juels and B. S. Kaliski, Jr.,	Data Deduplication	Ensure the privacy and integrity of files they retrieve. User want to verify that archives do not delete or modify files prior to retrieval.	Shows that a file is retrievable within a certain time bound.
10.	"Enabling cloud storage auditing with key-exposure resistance," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.	J. Yu, K. Ren, C. Wang, and V. Varadharajan,	Public and private key encryption	Key is used for securing the data on high scale.	Data storage is the main issue.
11.	"Strong key-exposure resilient auditing for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.	J. Yu and H. Wang	strong key-exposure resilient auditing scheme	Strong security is provided.	Chances of key explosion is there.
12.	"Identity based remote data integrity checking with perfect data privacy preserving for cloud storage based on OTP,"International Journal of Pure and Applied Mathematics Volume 119 No. 15 2018, 995-1000	S.V. Kavya, M. Hemamalini, K. C. Nishitha	Blowfish and AES algorithm	OTP provides strong security.	Data management is properly needed.
13.	"Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud," IEEE Transactions on Information Forensics and Security , Vol.11, June 2016	Huaqun Wang, Debiao He and Shaohua Tang	ID-PUIC protocol	Provides security against Collusion and DDos attacks.	Data leakage problem.
14.	"International data encryption algorithm for data security in cloud,"International Journal of Technology and Engineering System (IJTES) Vol 8. No.1 – Jan-March 2016 Pp. 06-11	S. Artheeswari Dr.R. M. Chandrasekaran	IDEA Algorithm is used for encryption.	Symmetric key concept is used for security.	Key needs to be updated always for security.

15.	“Epsshic-enabling privacy andsecurity of smart health care system in cloud,”International Conference on Recent Trends in Information Technology (ICRTIT) ISBN2013.	S.R.Satheesh, D.Sangeetha, V.Vaidehi	RSA Algorithm is used for encryption.	Easy to archive patients records.	Very expensive and not affordable for small organizations.

III. REFERENCES

[1]. Solanas, C.Patsakis, M.Conti, I.S. Vlachos, v.Ramos, F.falcone,O.Postolache, P. A. Prez-Martnez, R. Di Pietro, D. N. Perra et al., “smart health: a context –aware health paradigm within smart cities,” *IEEE Communications Magazine,* vol.52, no.8,pp.74-81,2014.

[2]. X. Zheng, P. Martin, K.Brohman, and L. Da Xu, “Cloudqual: a quality model for cloud services,” *IEEE transactions on industrial informatics,*vol.10, no.2, pp.1527-1536,2014.

[3]. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *in Advances in Cryptology*, pp.557-557,2005

[4]. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings *of ACM Conference on Computer and Communications Security,* (CCS’06), pp. 89-98, 2006.

[5]. J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunctions, polynomial equations, and inner products,” in Proceedings of *International Conference on the Theory and Applications of Crypto-graphic Techniques (EUROCRYPT08),* pp.146-162 2008.

[6]. K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” *IEEE internet compute.,* volume. 16, no.1, pp. 6973, January. 2012.

[7]. G. Ateniese et al., “Provable data possession at untrusted stores, in Proc,” 14th ACM *Conf. Compute. Communication. Security.* pp. 598-609, 2007.

[8]. K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, “An efficient and fine-grained big data access control scheme with privacy-preserving policy,” *IEEE Internet of Things Journal,* volume. 4, no. 2, pp. 563-571, 2017.

[9]. A. Juels and B. S. Kaliski, Jr., “Pors: Proofs of retrievability for large files,” . *14th ACM Conf. Comput. Commun. Secur.,* pp. 584-597, 2007.

[10]. J. Yu, K. Ren, C. Wang, and V. Varadharajan, “Enabling cloud storage auditing with key-exposure resistance,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.

[11]. J. Yu and H. Wang, “Strong key-exposure resilient auditing for secure cloud storage,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.

[12]. S.V. Kavya, M. Hemamalini and K. C. Nishitha, “Identity based remote data integrity checking with perfect data privacy preserving for cloud storage based on OTP,”International Journal of Pure and Applied Mathematics Volume 119 No. 15 2018, 995-1000.

[13]. Huaqun Wang, Debiao He and ShaohuaTang,“Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud,” IEEE Transactions on Information Forensics and Security , Vol.11, June 2016.

[14]. S.Artheeswari, Dr.R. M. Chandrasekaran “International data encryption algorithm for data security in cloud,”International Journal of Technology and Engineering System (IJTES) Vol 8. No.1 – Jan-March 2016 Pp. 06-11.

[15]. S.R.Satheesh, D.Sangeetha, V.Vaidehi, “Epsshic-enabling privacy andsecurity of smart health care system in cloud,”International Conference on Recent Trends in Information Technology (ICRTIT) ISBN2013.

[16]. Y. Zhang, J. Li, D. Zheng, X. Chen, and H. Li, “Accountable large universe attribute-based encryption supporting any monotone access structures,” in Proceedings of *Australasian Conference on Information Security and Privacy (ACISP’16),* pp. 509-524, 2016.

[17]. L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” *IEEE Transactions on industrial informatics,* volume. 10, no. 4, pp. 2233-2243, 14.

[18]. H. Shacham and B. Waters, “Compact proofs of retrievability,” J. Cryptol., volume. 26, no. 3, pp. 442-483, Jul. 2013.

[19]. Z. Liu, Z. Cao, and D. S. Wong, “Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay,” in Proceedings of *ACM Conference on Computer & Communications Security* (CCS’13), pp. 475-486, 2013.

[20]. D. Boneh, E.-J. Goh, and K. Nissim, “Evaluating 2-dnf formulas on cipher texts,” in *Proceedings of Theory of Cryptography Conference* (TCC’05), pp. 325-34, 2005.

[21]. A. Lewko and B. Waters, “New proof methods for attribute-based encryption: Achieving full security through selective techniques,” *in Proceedings of Annual International Cryptology Conference* (CRYPTO’12), pp. 180-198, 2012.

[22]. A. De Caro, V. Iovino, and G. Persiano, “Fully secure anonymous hibe and secret-key anonymous ibe with short cipher texts,” *in Proceedings of International Conference on Pairing-Based Cryptography (Pairing’10),* pp. 347-366, 2010.

[23]. A. Lewko and B. Waters, “New techniques for dual system encryption and fully secure hibe with short cipher texts,” in Proceedings of *Theory of Cryptography Conference (TCC’10),* pp. 455-479, 2010.

[24]. A. D. Caro and V. Iovino, “jpbc: Java pairing based cryptography,” in Proceedings *of IEEE Symposium on Computers and Communications (ISCC’11),* pp. 850-855, 2011.