Security and Confidentiality of the Data Using Block Level in Health Care System

Saudamini Deshmukh, Geetha R.Chillarge

Abstract*: Nowadays rapid development of cloud computing in smart healthcare system has significantly improved the quality of health. However, data security and user privacy are a major concern for smart healthcare systems. These days any kind of data can be used for malicious purposes. Many harmful entities constantly try to 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. To take care of this issue, in this paper, Symmetric Balanced Incomplete Block Design (SBIBD) is utilized for key Security so that unauthorized client can't get access to the data easily. It also allows the patients immediate and easy access to the data using unique user ID. This system makes use of double encryption using Blowfish algorithm to ensure maximum security of data and the concept of block level is used where data is stored using multiple blocks.

Index Terms: Cloud storage, Data security, ealthcare Key management, Block level.

I. INTRODUCTION

In cloud computing, data sharing empowers various members to share the information gathered from different sources which broadly enhances the proficiency of work. To guarantee the security of information available on the cloud is very difficult as it is open to all. Secret keys and encryption techniques have played an essential role in secure and effective data hiding. To take care of this issue, in this system Symmetric Balanced Incomplete Block Design (SBIBD) is utilized for key security. Unapproved client can't get access to the data which has been gathered from various sources. SBIBD scheme uses a basic structure for producing the basic key 'K' for different participants. The structure (v, k+1, 1), which is a square structure is utilized to store information. This system stores information from dynamic gathering. Data is partitioned in multiple blocks so that whole file cannot be accessed at one place. Hence, better system performance is achieved as compared to existing systems. It also helps for best calculations using RSA and Blowfish for encryption.

1.1 MOTIVATION

Every day, we come across news related to hacking of data. High level security is one of the best solutions for solving these issues in today's age of growing technology. As we all know that health plays a vital role in each and every human being's life and therefore the security of health records is also very important. The existing systems for health record security are vulnerable. To overcome this, SBIBD (Symmetric Balanced Incomplete Block Design) is proposed.

1.2 OBJECTIVE

The System presents a model of secure Smart healthcare system using a simple approach of block level.
The system provides security by simply using single secret key.
The System provides data security using double encryption technique.

II. REVIEW OF LITERATURE

This system introduces a new type of IBE scheme [1]. 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 [2]. 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 introduces a provable data possession model which allows a client who has stored his data at an

Revised Manuscript Received on July 9, 2019
Saudamini Deshmukh, Department Of Computer Engineering, Marathwada Mitral Mandal's College Of Engineering Pune ,India.
Prof. Geetha Chillarge, Department Of Computer Engineering, Marathwada Mitral Mandal's College Of Engineering Pune, India.

untrusted server to verify that the server contains the original data without fetching it from its location [3]. 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. 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[4]. 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 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 newly introduces the concept of smart health which is the context-aware complement of mobile health within smart cities and is very efficient [7]. 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 [8]. 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.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[9]. 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.

III. EXITING SYSTEM

In exiting system, patients get records physically after visiting the hospital. Mainly doctor performs patient checkup and stores the data according to user id. The data is stored on the local machine. But in this scheme there is a problem of data security. No security is there for the data and due to that the data is vulnerable to hacking. As health records are private records of patients there is a need to maintain the privacy and security. In this proposed system, the data is stored on cloud so that it can be easily accessed by patient from anywhere, at any time. To maintain the security and privacy the SBIBD scheme has been introduced.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed System (SBIBD) mainly includes peoples of same interests for example doctors who want to store their data on the cloud. The most serious problem when users store data in the Cloud server is confidentiality of the outsourced data. To overcome this problem a common key, called secret key, is shared to encrypt the data. This technique provides an identity-based data integrity auditing scheme for secure cloud storage. This supports data sharing with sensitive information hiding and provides double encryption with block level where data is stored in multiple blocks randomly. Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the common secret key. In addition, anonymity is also a concern for users. Our scheme uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud. In this system there are four roles Doctor, Admin (Sanitizer), Patient (User) and Researcher.Patient (User): Users search for their health reports in two ways - either by using their own Id or by the doctor's name. After searching the reports, user gets all the files uploaded by the doctor the user then selects the file which is needed and sends the request to the admin for that file, the admin accepts the request and sends the user's private key by email and then the user gets the report by using the private key. If the private key is matched only then can the user download the report. Doctor: Doctor uploads the patient's health reports on cloud server with all the details of patient and patient id. The reports will then be sent to the admin for

encryption.Administrator: After uploading the health reports by doctor, admin converts the data into encrypted format using AES algorithm. After converting into encrypted format again data is converted into second level encryption called as the content level encryption using blowfish algorithm and then encrypted data gets stored in block level randomly. Then admin will generate unique private key for each patient.Researcher: Researcher can access only required data of the patient for their work of research by doctor.

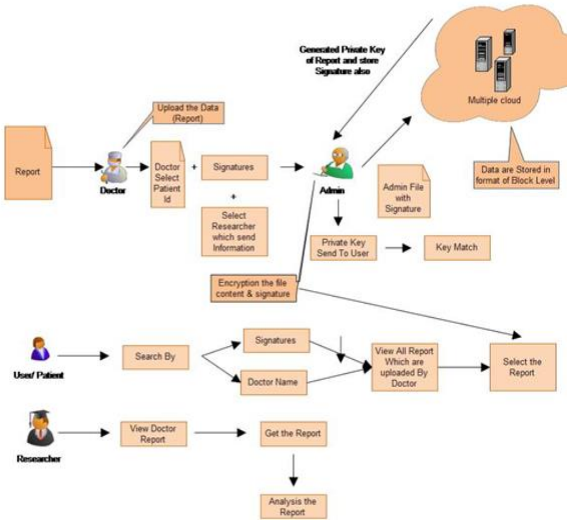

Fig 1. Architecture of proposed system

Algorithms

1. **Generation of Block B**

2. **Reconstruction of B**

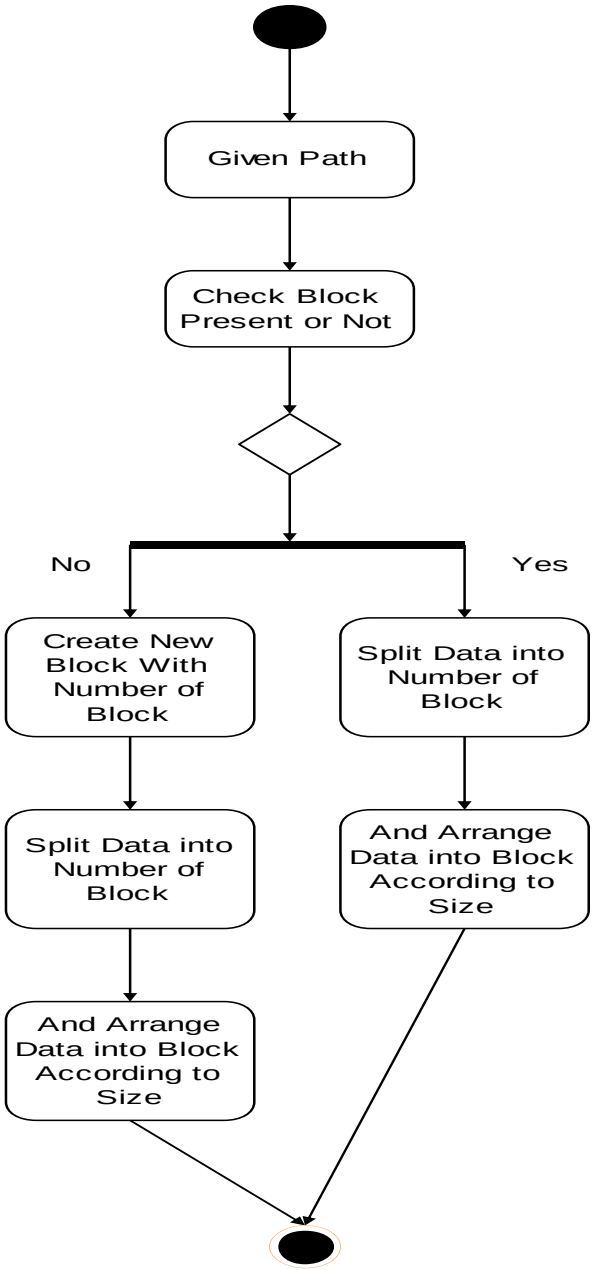

Fig 2. Flowchart of working of algorithms

The working of algorithm starts and checks whether blocks are available or not. Initially no blocks are available. If data has arrived then initially it is checked whether blocks are available or not .If blocks are available then data get split randomly and stored in the block and then the available space in the block is checked. Now if the available blocks are full and no space is available then the reconstruction of block is performed. i.e. new blocks are created again for storing the data. In this way the process is carried on continuously as the new data is arrived.

B. Advantages

1) In this system the sensitive information is hidden with help of Double Encryption.

2) In this System the file stored in the cloud can be shared and used by others given the condition that the sensitive information is protected using a secret key.
3) The concept of block level is used to randomly store data and maintain security.
4) Both security and privacy of the patient's records is maintained.

V. RESULTS

This system requires a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. System uses Java programming language with many types of encryption algorithms such as RSA and Blowfish Algorithm. The concept of block level is used for securing the data on the cloud. In our experiment, system initially installs the required software. The Data is stored in the Block Level. In Block Level concept the Data is stored in random block which are generated by (SBIBD) Approach.

Entity	User	Admin	Cloud
Data Blind-ing	O(d_1)	—	—
Key gener-ation	O(n)	—	—
Block gener-ation	—	—	(v,k+1, 1)
Prof gener-ation	—	O(c)	—

Figure 2: Different between Different Entity with different Role

Parameter	Exiting System	Proposed System
PASH	Yes	No
Block Level	No	Yes
Data Security	No	Yes
Access Control	Yes	Yes
IDB (Identity based encryption)	No	Yes

Table 1: Comparison between Exiting System and Proposed System.

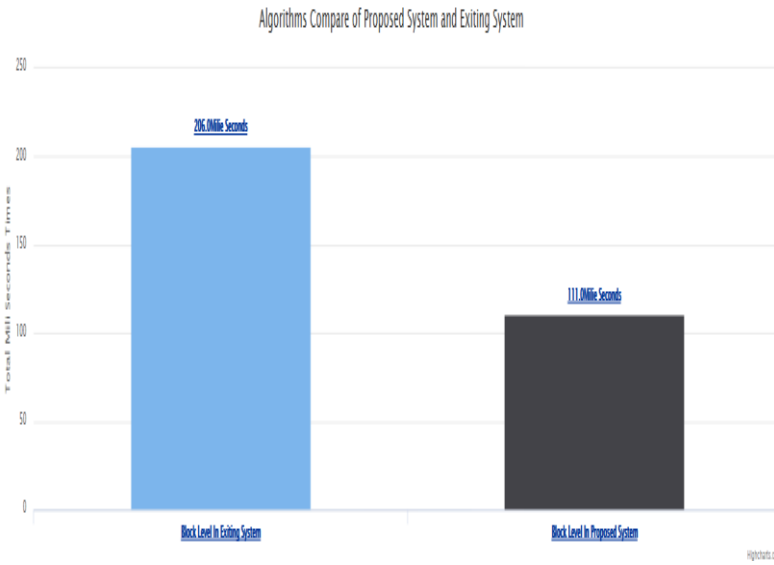

Fig 3: Algorithm comparison of proposed and exiting system.

This graph represents the execution time required by the existing system and the proposed system. The x axis contains the process name and the y axis contains the time in milliseconds. The results display that in existing system the time is 206.0 milliseconds to complete the execution using block level and the proposed system takes 111.0 milliseconds to complete the execution using block level. The execution time is calculated by taking the time from when you click for the process to run to when the process is completed.

VI. CONCLUSION

This system efficiently addressed data security and user privacy issues in s-health by introducing SBIBD, **(**Symmetric Balanced Incomplete Block Design). In SBIBD, sensitive attribute values involved in access policies are hidden. Double encryption is provided for the security purposed. As the data is stored in block level the data cannot be retrieved easily by unauthorized person. This system indicates that SBIBD is more secure, efficient, and expressive than existing schemes which are used until now for secure data storage on the cloud.

REFERENCES

1. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology, pp.557-557,2005.
2. V. 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.
3. G. Ateniese et al., "Provable data possession at untrusted stores, in Proc," 14th ACM Conf. Compute. Communication. Security. pp. 598-609, 2007.
4. A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," . 14th ACM Conf. Comput. Commun. Secur., pp. 584-597, 2007.
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 3challenges for the public cloud," IEEE internet compute., volume. 16, no.1, pp. 6973, January. 2012.
7. 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.
8. 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.
9. K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, "An e cient 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.

AUTHORS PROFILE

Miss Saudamini S. Deshmukh, pursuing ME in computer engineering at Marathawada Mitra Mandal's College of Engineering,Pune Prominently works on cloud security and Network security.

Prof. Geetha R. Chillarge, works as assistant professor in Department of computer engineering at Marathawada Mitra Mandal's College of Engineering, Pune. She has done her masters in Computer Engineering and currently pursuing her Ph.D.