Secure and Optimized Data Sharing Model Group in Healthcare Cloud Environment

Uma Hombal, Dayananda R.B.

Abstract-The cloud computing provides convenient on-demand access of the data. Sharing of data in the cloud computing will enable several users to easily handle the data that is being shared. The medical-field finds more advantages by the cloud-computing technology as the data can be accessed anywhere and anytime by the patients as well as this data can be shared with other medical-practitioners. This alarms for the security issues as the huge amount of sensitive data is being shared. The data must not be available to malicious-attackers. In this paper, we propose the block-design based key agreement protocol in order to share the data securely and the design provides fault-detection and fault-tolerance. The group-data model PSM is given with the block-based design, which decides how the sharing of the data is done by grouping and giving positions to users in particular blocks and the column. The $(np, i+1, 1)$ ***design is proposed in our paper, which gives the technique for positioning of the users. The encryption and decryption of data is done and their times cost according to file size is found. The comparison of the time-cost for our model and existing models is compared with respect to different number of simulations.***

Keywords: Cloud-computing, data-sharing, block-based design, group-key

I. INTRODUCTION

Health-care requires continuous innovations in all the fields in a systematic way in order to provide high quality services. Technology of Information is rapidly and vastly used in healthcare with the motivation of to enhancing and improvising the medical services for cost reduction. Modern health-care innovations rely on information system in all aspects. The application of information-technology in health-care has got its importance in all the countries [1]. Most of the services that are provided are being outsourced to the cloud servers. The cloud storage plays a very important role in the applications like the medical files transferring etc. The majority of data being outsourced will be the health-care data, which will include the personal health record, Electronic health record and related documents. The patients are sent to various tests which results in high exchange of data between different departments of medical units. But this must be done in a secure manner. Many researches have been done to protect the data that is being shared between different departments of these medical units and to identify the risks in sharing of this data [2] [3] [4].

The technology used which helps in this data-exchange is cloud computing. Cloud computing is said to be a model that enable on demand service. The resources can be dynamically increased which implies lot of medical data can be stored and this data can be used and can be accessed anywhere and anytime by the patients or the doctors as well as share the information among them.

Revised Manuscript Received on November 08, 2019.

Uma Hombal, Assistant Prof, Dept. of computer science and technology KLE Dr. MSSCET, Belagavi.

Dr. Dayananda R.B., Professor, KSIT, Bangalore

This alarms for the security and privacy issues as large amount of sensitive data will be shared. The patients' data must not be accessible to malicious attackers. The compromise in this data will be a threat to both the patient and the organization with whom the patient exchanges the data. Methods are taken to provide this security against the attacks [5]

Considering this application of information technology in health-care, the personal health record being outsourced to the servers has gotten numerous data-breaches related to cloud servers which includes the malicious attacks. Patients are unable to have any physical control over their own health-record. These sensitive data are not under the control of the control of these data-owners. So there requires an encryption mechanism to protect these records before out-sourcing is done. Here the owner must decide which user will get access to which data in this record. The decryption mechanism must be such that only those with the decryption ley must be able to decrypt and obtain the data [6] [7]. This implies that the authoritative-users get the access to the data that is being shared outsourced to the cloud.

In this paper we concentrate the sharing of data to multiple users. Here the multiple users will form a group and thereby exchange the data. Here the block-based design key-agreement way is used to design the block-based design structure which can support multiple-participants. This design helps all the data holders to share their data with the higher security as well as a much more efficient manner. This presents the group data-sharing model that supports sharing of this health-care data in a group manner. This DS(data sharing) model in group provides the definition of block based design which is symmetric which determines the way communication among the groups take place. It brings the concept of group-key that the multiple participants generate to share data in a secure manner. The group members make key-agreement to derive the common group-key. This key is being generated by the users themselves. Due to this, any sorts of attacks to the key is avoided and thereby the attack on the data is avoidable. The fault-detection and fault-tolerance is provided by this design. This ensures the group-key is being generated without failure. The fault-detection is done. In this, it can identify the volunteer who can replace the malicious-attacker. This enables to avoid different key-attacks which once again makes data sharing safe. In this, the CCSTPV i.e. the cloud-security service third-party-verifier is used. This is useful in providing the key-updates. It helps the user, to encrypt the file by using the key provided by the CCSTPV and thereby outsource the data to cloud, this encryption makes the data secure for against any middle-attacks.

This paper has organized in subsequent sections that are as follows, section- 2 discuss the Literature survey, in section 3 we described proposed model, section-4 we provide the result-analysis, section-5 gives the conclusion of our paper.

II. LITERATURE SURVEY

In the paper [8] secure healthcare data sharing and collaboration scheme, to provide the data privacy for health data is achieved. The privacy preserving technique is done for securing the personal-information. It uses the layered-model of the access-structure which will solve the problem of multi-hierarchical sharing of files. The de-duplication is implemented which will allow only single instance of the file to be saved and this thereby can save memory-wastage and the time saving. The attribute-based-encryption is the technique used in data based encryption. Separate key is provided for each of the file to be stored in cloud. This key is used during the decryption.

In paper [9], the medical data transmission and its analysis for the health-care system is done. Here the medical data is collected from the WBANs which will be transmitted through the wireless-sensor-networks. The homomorphic-encryption based on matrix scheme is used in order to ensure the privacy. The expert system is used to avoid doctor involvement always and thereby ti reduce the burden but this has lesser reliability. In paper [10], secure and private data management framework which can solve the security and the privacy issues of the medical-data that is outsourced to the database. It uses semantically-secure encryption schemes to keep the data encrypted that are being outsourced to the cloud. It provides with the query interface that will support multiple SQL-queries and provides with the complex data-mining tasks. It uses the concept of the differential-privacy that makes sure that the adversary learns nothing much about the individual. The communication and computational costs are low.

In paper [11] the privacy and security requirements for the personal health records (PHR) system is provided by an ac(access control) framework gets support through the IBE(identity-based encryption) for securing the PHR system. The framework is designed which enables the secure transfer/sharing of the PHRs. It uses IBE infrastructure which is employed on the basis of IBE library and it supports ECC(elliptic curve cryptography). In paper[12], the security challenges of sharing the medical-records is done by the authentication-scheme. In this the diagnosis reports by the doctors and other physical examination reports gets uploaded to the cloud through the authentication mechanisms. The patient can also authorize other parties that can access their medical-records. Moreover SET (symmetric-encryption technology) has been employed and the BFF(biometric-fingerprint feature) as well as the digital signatures has been used for the security.

In order to make data more secure while sharing it, multi-party is used in cloud computing where the data is encrypted using certain key policy [13]. Certain attributes are also used for this encryption. CP-ABE method is used where the, cipher text is created with an access structure. This specifies the encryption type and, and based on users' identity the private key is generated. The decryption of health data is done after the attribute and key policy is approved by the key distribution center and data verification center. The paper [14], secure data sharing is in the health-care system is done by the identity based encryption with the signature. This will provide the data accessing of the shared data only by the authorized-user which is based on the unique identity. The alterations during the data transmission is taken care. Here the data will be encrypted and can be accessed by the authenticated users. It uses the Identity-based-encryption and the BLS-signature in the proposed model. It uses the AES algorithm to encrypt the health-data. The signature generation is done with certificate using BLS signature through Encrypt and the sign-algorithms. The computation time of encryption, the signing, the decryption and verification is done.The paper [15] focusses on providing a cloud computing solution which helps in sharing the healthcare data based in Google app engine (GAE). Here GAE is implemented as cloud computing technique to share data. The data from healthcare center to hospital or vice-versa can be shared using personal number account. This is done by using the online interface at GAE. Here a device must be used as middleware in order to bridge among the hospitals and the health-care centers. SaaS can be the middleware of the information sharing among different hospitals and health-centers. The Google, Amazon, Microsoft will provide the users to develop the SaaS applications in their platforms. Certain latency is observed in this technique.

In paper [16], the secure data-sharing along with the key-management is developed. The public-key cryptography is used for securely soring as well as sharing the data in cloud. SI(searchable index)is proposed to provide the search over the given encrypted-data. Moreover confidentiality is also maintained by the data-owners. This even provides the synonym search over the encrypted-data will in turn improved the efficiency of the system. The paper [17] the SeDaSC methodology which helps in sharing of data without any re-encryption technique. Here the encryption is done using single encryption key. There are two different key shares where only one key is given to user and other key is stored by the trusted service.

III. PROPOSED MODEL

1.1 Designing a(np,i+1,1) model

To provide the DS (Data Sharing) scheme in group for the multiple-users, we suggest the $(np, i+1, 1)$ design. This is called the balanced incomplete design which is block-based. It is defined in general as follows:

$Np = \{0,1,2, \ldots np-1\}$, $Blk = \{Blko, Blk1, \ldots\ldots Blk_{blk-1}\}$,

Np determines the number of elements, b denoting the number of blocks, i is the number of elements in each block. $prm1$ and $prm2$ are the two parameter. In this paper, the design is the $(np, i+1, 1)$ −design. This is a decentralized model. Here i chosen will be prime number and the $prm1$=1. In this design, not all parameters are independent. The b and $prm1$ are dependent and are determined by np, i and $prm2$ as

$$blk * i = np * prm1 \qquad (1)$$

$$prm2\ (\mathrm{np}-1) = \mathrm{prm1}(\mathrm{i}-1) \qquad (2)$$

Exchanging of information in the key-Consensus protocol is primarily based on the $(np, i+1,1)$-design. In here every user can identify the response that the receiver or sender sends based on this DS-model in group.

1.2 The System-model

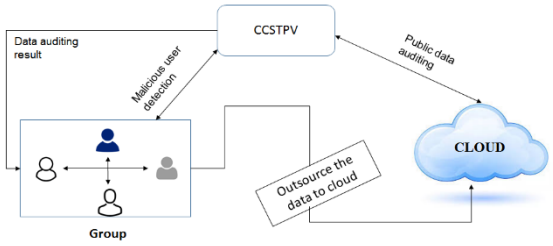

Fig1: The system-model for group-data-sharing

The system model has

1. The group: This include the individuals or any medical practitioners. In order to concatenate such that they can work together , they form the group and they upload the necessary data to the cloud.
2. Cloud: The data or the files that must be shared will be stored in the cloud. It is a semi-trusted party. The file can be uploaded and downloaded from the cloud.
3. The CCSPTV: This is responsible for the data-storage auditing, and in identification of any malicious users in the group of users. It is also responsible for generation of certain system parameters which is required for the group data sharing later.

1.3 Designing DSM (Data Sharing Model)

To provide the data sharing in group for multiple-users, by using the block-based design in a symmetric manner, we provide an algorithm to build the $(np, i+1, 1)$ design. Here the n participants must perform the key-agreement.

1.3.1 The (np,i+1, 1) design

In this design, the parameters have some specific meaning when used for the data-sharing between the users who wish to share the medical-data. The np denotes the number of users as well as the number of blocks. Here each block will have $i+1$ participants. Each and every participant will appear $i+1$ times in all the n blocks. The participants taken in pair will appear simultaneously in one of the n blocks. For the construction of this design the i is chosen. This i is a prime number. The number of users depends on this equation as

$$np = i^2 + i + 1 \qquad (3)$$

Here the np which is the number of users, is given as $N = \{0,1,2,\ldots . np-1\}$. The blocks Blk is given as $\{H_0, H_1, H_2 \ldots . Hnp_{-1}\}$. The np blocks are constituted by np users. Here each block is defined as

Which implies that the block has i+1 users and the notation $Blk_{m,n}$ implies that each of the user will be in the e n^{th}column of the m^{th}block. The range of m is from $m = 0,1,2,\ldots . i^2 + i$ and the value of n ranges as $n = 0,1,2,\ldots . i$.

The algorithm for this design is given as follows:

Algorithm1	The (np, i+1,1) design
Step1:	Start
Step 2:	Declare the value of i
Step-3:	Read the value of m
Step4:	Repeat the steps until m≪ i
	Step4.1 : Initialize the value of n
	Step 4.2 : Repeat the steps until n≪ i
	Step-4.2.1 : If n equals 0 $Blk_{m,n} \leftarrow 0$ Else $Blk_{m,n} \leftarrow m * i + n$
Step 5:	Initialize m ← $i+1$
Step 6 :	Repeat the steps until m≪ i^2+i
	Step 6.1 : Initialize the value of n
	Step 6.2 : Repeat the steps until n≪ i
	Step-6.2.1 : if n equals 0 $Blk_{m,n}$ ←floor((n-1)/i) else $Blk_{m,n}$ ←ni+1+MODi(m-n+(n+1)*floor((m-1)/i))
Step7:	Stop

In the above algorithm, the step-6.2.1 has MOD_i used for identifying the user will be belonging to which column. Here the MOD represents the modular-operation that will take the class-residue as an given integer in the range of $0,1,2 \ldots i-1$.

The zone is taken into consideration. A zone is basically collection of blocks. It is defined as

$$Zone_x = \{Blk_{\ i} : Blk_{i,0} = x\} \qquad (4)$$

Here the zone $Zone_0$ is defined as $Zone_{\ 0} = \{Blk0, Blk1, \ldots \ldots \ldots Blki\}$. The zone of the nth column is given as follows

$$Sect_n = \{Blk_{i*n+1}, Blk_{i*n+2}, Blk_{i*n+3}, \ldots \ldots . Blk_{i(n+1)}\} \qquad (5)$$

This is formed by the i blocks where the value of n ranges from n=1,2,3,….,i. So the value for Sect1 is $\{H_{i+1}, H_{i+2} \ldots H_{2i}\}$.Certain statements are considered for the further improvisations in the design of the DS model in group and they are:

Statement1: The $Zone_0$ with the (i+1)*(i+1) users, the 0^{th} user comes with the multiple of i+1 times in the given Initial column of the $Zone_0$ and the left out i^2+I elements appear exactly single time in $Zone_0$.

Statement 2: In the zone $zone_x$, with i blocks, the set of the i elements of the xth column is same as the IS(index set) of given i blocks in $Zone_x$.

1.4 DS Model -Design

The above described algorithm is constructed which is the $(np, i+1,1)$ design that is according to the block-based design. But in order to generate the general key for n users, the design must be altered in such a way that each of the block $H_{m,}$ must have the $user_{m.}$ Here the H_m is the m^{th} block of the given structure of the

$(np, i+1, 1)$. The structure of the block constructed by the algorithm1 doesn't have the required property. Based on the statement 1 and 2, the n blocks of Blk is restructured to obtain the new structure S. The algorithm2 is constructed and using this the design can be modified. This structure S is created after the algorithm1 creates the Blk structure. Here an additional flag bit is used for each of the H_m to identify of the Blk_m is modified or not. This flag bit is denote as Blk_m [f]. This value is 0 if the Blk_m is not modified according the second algorithm. Or else its value is set to 1.

Algorithm-2	The Reconstruction of Blk design
Step1:	Start
Step2:	$Z_0 \leftarrow H_0$
Step3:	Initialize the value of variable a←1
Step4 :	Repeat until a≤ i
	Step-4.1: $Za \leftarrow H_{a*i}+1$; $H_{a*i+1}[f] \leftarrow 1$
	Step-4.2: $S_{S_{a,a}} = Blk_{floor((S_{a,a}-1)/i)}$; $H_{a*i+1}[f] \leftarrow 1$
Step5:	Initialize m ← $i+1$
Step6:	Repeat the steps until m≪ i^2+i
	Step-6.1: if $H_m[f] \neq 1$; $S_{Blk_{m,floor((m-1)/k)}} \leftarrow Blk_m$
Step7:	Stop

The above algorithm is explained as:
The Z_0 is initialized to H_0. Therefore, it doesn't require any transformations. In the step-4.1, as per the definition of $Zone_x$, the Initial element of the each block will have identical element as x. Further the first block of $\{Zone_1, Zone_2, \ldots Zone_i\}$ of Blk will be transformed to the Z_1 to Z_a blocks of Z in order to satisfy the property that $user_a$ must belong to S_a.
In the step-4.2, it is based on the statement-1 that was defined. The equation in this step will also satisfy the property of $user_a$ must be belonging to the S_a.
In the step-6.1, it is based on statement-2 mentioned earlier. In this step 3, the $i-1$ blocks of each of the zone $Zone_x$ in Blk will be transformed into i*(i-1) blocks of S. The indexes of the $i*(i-1)$ blocks of S will be determined by the xth column of the remaining i-1 blocks of the Zone $Zone_x$ in Blk(x ≠ 0). Hence the $Blk_{m,x}$ is used as the index of the S(the new structure). Here the x is taken as $floor((m-1)/k$. Here them ranges between $i+1 < m < i^2+i$.

1.5 Restructured DS-Model

structure of S is given in different equations. The transformation from Blk structure to the structure of S. Here the a is the index of the given block of S and the n denotes the nth column of the block S. The $Z_{a,n}$ now denotes the user is present in the n^{th} column of the a^{th} block in S. These descriptions are given under different scenarios.
Scenario-1:
$Z_0 = Blk_0 = \{0,1,2, \ldots . i\}$
Scenario-2:
When $0 \ll n \ll i$ and $1 \ll a \ll i$

$$Z_{a,n} = H_{a*i}+1 \quad (6)$$

$$Z_{a,n} = a, (n = 0) \quad (7)$$

$$Z_{a,n} = n*i+1+MODi(a-1)(n-1); (n > 0) \quad (8)$$

Scenario-3
When the value of $0 \ll n \ll i$, a= $Z_{m,m}(1 \ll m \ll i)$

$$Z_{a,n} = Blk_{floor(a-1)/i),m}=0, (n=0) \quad (9)$$

$$Z_{a,n} = Blk_{floor((a-1)/i),m} = (floor(a-1)/i)*i+n, (n>0) \quad (10)$$

Scenario-4
When the value of n is $0 \ll n \ll i$, a= $Z_{m,x}$ ($a \neq Z_{m,m}$)

$$Z_{a,n} = Blk_{i(x+1)+r,n}=x, (n=0) \quad (11)$$

$$Z_{a,n} = Blk_{i(x+1)+r,n}=n*i+1+MODi(nx-x-n+r), (n>0) \quad (12)$$

The scenario-1 and the scenario-2 coincide to the step-4.1 of the algorithm-2. Scenario-3 coincide to the step 4.2 of the algorithm 2, last but not the least the scenario 4 coincide to the step-6.1 in the algorithm-2.

1.6 Key-Consensus method

The key agreement method involves three step key in it and they are

1. first stage: The CCSPTV will be generating certain system parameters that are required and will share the secret key for all the users. Moreover The mapping of the private keys and the public keys is done through the hashing
2. Second step: The common group-key will be generated by 2 rounds for the multiple-users. Thereby the exchange of the messages will be done according to the structure of S described earlier.
3. Third step: The authentication-phase or the fault-detection phase: All the users may not be honest. There can be malicious users who can affect the data being shared. The verification of keys of each of the participant is done and the authenticity of the participant is done to avoid any malicious attacks taken place.

IV. RESULT ANALYSIS

The files that will be shared between different users must be encrypted. The file that is shared with the specific user will later be decrypted. We consider the encryption and decryption alone for the text files that must be shared between different users. The file can be in .txt, .docx ,.pdf file format. The time taken for the encryption and the decryption of different file sizes is considered. The environment where all these computations were done are: the programming language used for this was the c programming by using the pairing-based library. GNU Multiple Precision Arithmetic Library in VMware workstation 12 machine on CentOS 6.7. The device is 8GB RAM and the CPU is Intel-core i5 @ 2.40GHz. The compiler used is gcc version-4.4.7. Here the PBC is used for the pairing operations. The encryption and decryption simulation techniques and the time taken for each file size is explained as follows.
The encryption of the file is done as follows:
The file that must be shared will have the confidential text data. This text data includes the medical information namely the medical prescriptions, the scanned data information of the patients, the regular-health reports if the patients etc. In our encryption technique,

particular hash message is considered. The file is read and the encryption technique is applies as, entire file is considered into blocks as per our hash message. The characters that must be encrypted will be converted to bytes. The encrypted message is obtained by multiplying the characters of the message and the hash message and this is done in block wise as per the taken hash message. The computational time for this encryption is done. For 20Mb file, the time taken for the encryption is 1.162seconds. For the 40Mb file, the time taken was 1.408seconds. For 80 Mb it takes 2.188 seconds and for 100 Mb it takes 3.01 seconds. It is clear that the encryption time increases with the increase in the file sizes but not in huge amount. And this is the way the encryption works.

The decryption of the data is done as follows:

The encrypted text file will be decrypted by using the similar concept as that of the encryption. The encrypted data will be obtained in bytes and again this data will be divided into blocks based on the hash-message length and this encrypted data will be multiplied with the hash-message in order to obtain back the original data. The file that was shared by the user by doing the encryption will be decrypted by the destined user. The comparison is done with the original data and the decrypted data to see if the data was decrypted correctly according to the original. The decryption time for different file sizes is given as follows: for 20 Mb file, the time taken is 0.608 seconds. For the 40Mb file the time taken for the decryption is 1.066 seconds. For 80Mb the time taken will be 2.006seconds. For 100 Mb file the time taken is 2.488seconds. The decryption time will increase as the increase in the size of the file. This is same case in the encryption. This is because the time required for the hashing increases with the increase in the size of the file. The graphs for these encryption and decryption of file is given below in Fig2 and Fig3.

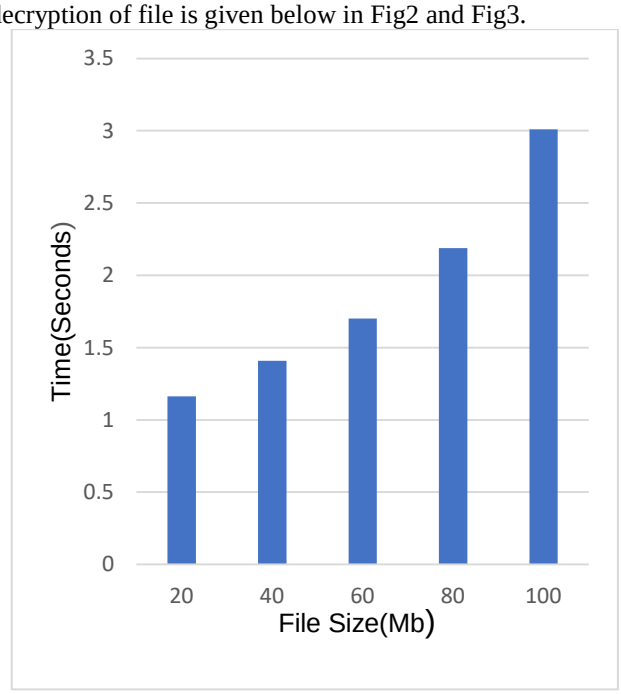

Fig2: File size vs Encryption time

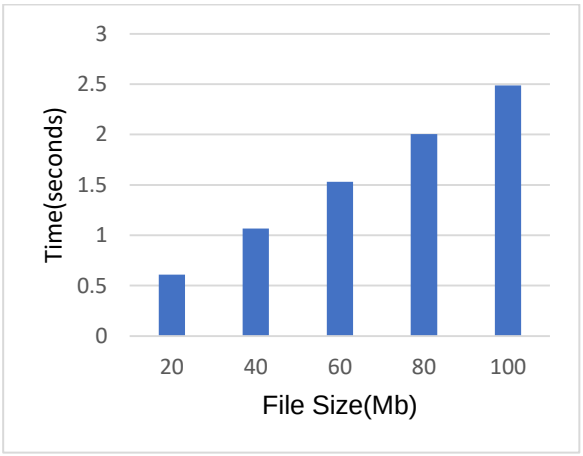

Fig3: File size vs Decryption time

The data-sharing is done between different users by generating the common group-key and through different phases as mentioned in the section4. There includes three phases for the group-key generation and then the messages get exchanged between different participants. The time cost for different phases is important factor that distinguishes between our methodology and the existing method of the group data exchange which is the protocol which is an identity based fault-tolerant approach that is used for exchanging of data between different users. The time cost for our PSM(proposed methodology) and the IBFTA [18] protocol is compared in different phases.

The time taken for each phase is added up to determine the overall time taken by the methodology of the group-data exchanging. This forms the simulation time for the execution of the phases overall. In this way multiple simulation is done in order to find if out PSM is better or the IBFTA [18] is better. This is done by keeping the number of users fixed and checking the time cost for different number of simulations done.

The number of participants is fixed and this is obtained by taking the value of i which is the number of participants in each block to 11. Thereby the number of users overall is obtained as per the equation (3) as $np = i^2 + i + 1$ as n=133. The comparison of the simulation times for our PSM and the IBFTA [18] protocol for up to 100 simulations and time cost is shown in the graph fig-4. The time cost is compared each time a simulation is done and till 100 times.

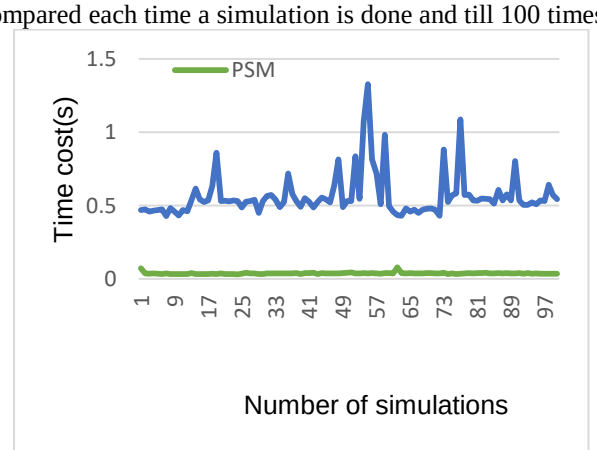

Fig4: The time cost comparison for different simulation times

The graph depicts that the PSM i.e. our proposed methodology is much more efficient in terms of time cost than that of the IBFTA [18] protocol. This is because the IBFTA [18] protocol will require more amount of pairing in initial –phase which is the weil-pairing required will be 132 and it requires 2-point multiplications. But in out proposed methodology, it requires only 2 weil-pairing and the modular-exponentiations required is also less which is 11. While considering the key-agreement phase, the IBFTA [18]-protocol will require 132 weil-pairings whereas our technique will require 33 modular-exponentiations. Finally in the authentication-phase, IBFTA [18] protocol will require 4-point multiplications whereas our technique again requires 33 modular-exponentiations. The time difference at some specific points are given. When simulation is done only once, the time difference that we see from ours and the IBFTA [18] is 0.397seconds. Similarly when the simulation is done for about 14-times, the time difference observed is about 0.582seconds. When the simulation is done for about 19times, the difference is about 0.826seconds. Similarly there is huge difference observed when 55 times the simulation is done and that is about 1.289seconds. For 96 times the difference is about 0.497seconds in the simulation times of both the methodologies. Through this, we can conclude that our scheme requires less cost w.r.t time cost than the IBFTA [18]-protocol. The performance of our PSM is much more stable than the IBFTA [18] protocol.

V. CONCLUSION

The sharing of health-care data is achieved by the group-data sharing model which is based on the block-based design. The users who wish to share the data form the group and by the block-based design the users are placed in particular block and respective column. Algorithm for giving particular positions according to number of users is proposed. The encryption and decryption of data is done and the time for encryption and decryption according to different file sizes is given. The proposed method involve different phases in order to generate the common group-key. The comparison of our model is done with the existing IBFTA [18] protocol with respect to the time cost of different number of simulations. Our method requires less time-cost and when the simulation is done for 100 times, the difference observed with the existing protocols simulation time-cost was 0.5084 seconds. Therefore our model is more stable than IBFTA [18] scheme.

REFERENCES

1. GiuseppeAceto, ValerioPersico, AntonioPescapé, “The role of information and communication technologies in healthcare :taxonomies, perspectives and challeges, journal of network and computer applications, volume 107.
2. Mehedi Masud,M. Shamim Hossain ,“Secure data-exchange protocol in a cloud-based collaborative health care environment”
3. E.SmithJ.H.P.Eloff, “A Prototype for Assessing Information Technology Risks in Health Care”, Published in, Journal, Computers and Security, Volume 21 Issue 3, June, 2002
4. Mr. Pramod & Dr. B R Prasad Babu, “Portable Tpm Based User Attestation Architecture for Cloud Environments ”, Global Journal of Computer Science and Technology: B Cloud and Distributed Volume 15 Issue 1 Version 1.0 Year 2015 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350
5. Lei Chen, Ji-Jiang Yang, Qing Wang, Yu Niu, “A framework for privacy-preserving healthcare data sharing presented at 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services.
6. Danan.T, Yu Zhao, Surya.N, Rafael A. Calvo, Abelardo Pardo” protecting and analyzing health-care data on cloud”, presented at 2014 Second International Conference on Advanced Cloud and Big Data.
7. Levina, T., Lingareddy, D.S., & Dhruve, K.D. (2013). DYNAMIC EXPIRATION ENABLED ROLE BASED ACCESS CONTROL MODEL FOR CLOUD COMPUTING ENVIRONMENT.
8. R. Shiny Sharon ,Dr. R Joseph Manoj , “ E-health care data sharing into the cloud based on de-duplication and file-hierarchy mechanisms ”, Advanced Cloud and Big Data (CBD), 2014 Second International Conference
9. Haiping Huang, Tianhe Gong, Ning Ye, Ruchuan Wang and Yi Dou, “Ning Ye, Ruchuan Wang and Yi Dou, IEEE transactions on industrial informatics, volume13 ,issue 3
10. Noman M, Samira B, Dima A, Rui C,” Secure and private management of health-care databases for data mining” presented at the IEEE 28th International Symposium on Computer-Based Medical Systems
11. Richard Ssembatya and Anne V.D.M. Kayem, Rondebosch,” Secure and Efficient Mobile Personal Health Data Sharing in Resource Constrained Environments” presented at IEEE 29th International Conference on Advanced Information Networking and Applications Workshops,2015
12. Chin-Ling Chen, Jin-Xin Hu, Chun-Long Fan, Kun-hao Wang, ” Design of a secure medical data sharing system via an authorized mechanism”, 2016 IEEE International Conference on Systems, Man, and Cybernetic,2016
13. Nikhil Chaudhari, Mohit Saini, Ashwin Kumar,” A review on attribute based encryption”, presented at the 8th international conference on computational intelligence and communication networks, 2016
14. Amang S, Mike Y, and Haryadi Amran , “A Secure Data Sharing Using Identity-Based Encryption Scheme for e-Healthcare System” presented at 3rd International Conference on Science in Information Technology (ICSITech), 2017
15. Van Hu, Fangjie Lu, Israr Khan, Guohua Bai, A Cloud Computing Solution for Sharing Healthcare Information, presented at the 7th International Conference for Internet Technology and Secured Transactions
16. S.K.Sonkar, Ms.S.P.Wakchaure, “Group data searching and sharing using key aggregate cryptosystem”, presented at the International Conference on Global Trends in Signal Processing, Information Computing and Communication,2016
17. Mazhar Ali, Revathi Dhamotharan Eraj Khan, Samee U. Khan Athanasios V. Vasilakos Keqin Li Albert Y. Zomaya, “SeDaSC: Secure Data Sharing in Clouds”, IEEE Systems Journal , 2017,Volume: 11 Issue: 2
18. Xi Yi,""Identity-based fault-tolerant conference key agreement",IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3,pp. 170–178, 2004

AUTHORS PROFILE

Prof. Uma Hombal is an Assistant Professor in Department of Computer Science and Engineering. Her field of expertise is curriculum and mentoring. She was presented the best paper award for her MTech Thesis titled “Secure Sharing of Personal Health Records in Cloud Environment “ at National conference in Communication and Signal Processing, SJEC, Mangalore in the year 2014. Her research interests are Image processing and cloud computing.

Dr. Dayananda R. B is a Professor in Department of Computer Science and Engineering, KSIT, Bengaluru. He is also the Director of IQAC, KSIT. He has academic experience of 17 years, holding various posts as HOD and Vice Principal at Prestigious Engineering Institutions. His research mainly focuses on Design and Development of a Cloud Computing Architecture for data security. He has been felicitated with Governor’s Award-a National award for Excellence in Research and Development. His other achievements include:

1. SHIKSHA RATAN Award for talented personalities presented on Saturday 24th September 2016 at New Delhi.
2. Research supervisor at VTU GUIDING 7 STUDENTS AT PRESENT
3. Certificate of appreciation in rolling out Infosys campus connect Foundation program
4. Research committee member at Global Research Academy, a center of excellence, approved by ministry of Science and Technology, Govt of India
5. Represented SBIT, Tiptur at 'sankara channel' in TURNING POINT Program
6. Organized 29th CSI State level student convention at GSSSIETW, Mysuru
7. Organized in association with CSI, the International conference CONSEG-2011 on Software engineering at Chancery pavilion, residency road, Bangalore-25
8. He is reviewer at Springer Journal (Cluster Computing) and also reviewed many papers of Conferences and symposiums.