An Empirical Research for Secured Storage and Protecting Unauthorized access of Organ Donor Details

Geetha A, S.SobithaAhila,V.S.VidhyaLakshmi,S.Kalpana Devi

Abstract---- Cloud computing is the on-demand availability of computer system resources, particularly data storage and computing power, without direct active management by the user. Here an online organ donation system is developed with the help of the aforementioned technologies. The main aim of the paper is to make sure that the organs of the people, who have come forward to donate, reach the respective individual in need of the particular organ. Since everything is stored in the cloud, anybody can access it anytime, which in turn puts the data at risk. The secured sharing of donor detail is necessary. Encryption is done at two levels to provide security, one while the data is entered and the other done by a third party providing proxy re-encryption. Now, whenever a brain-dead patient is in the hospital, after thorough verification for any complications, the deciding parameters such as the organs that can be transplanted, blood group, presence of HIV positive and location, is compared with the cloud database using query filtering, which results in the nearest organ donor available meeting the requirements. The performance enhancement of cloud data using encryption schemes is of high potential.

Keywords: - cloud computing; proxy re-encryption; query filter.

I. INTRODUCTION

Cloud computing in today's world has enormous usage and it is becoming a trend to make everything available to all users at any time, now that the internet is available at every town and city. Another reason cloud computing is growing is that of the easy and cheap solutions to a lot of services provided by cloud services. Most of these services are the pay-for-use basis and so there's no requirement for payment of a huge sum for services that people don't even use.

Despite the ubiquitous and agile services offered by cloud the main disadvantage in availing cloud services and why most people fear to use it is because of the violent threats and attacks that hackers do to the data on the cloud. Even though encryption of data can be done, it has become an easy task for the intruders and hackers to decode the encryption to retrieve the data. So it necessary to deploy encryption at newer levels and different algorithms to maintain the secrecy of information on the cloud. It is the main reason many companies do not reveal their security measures to the outside world. In order to extensively make use of cloud services, we must concentrate on providing a high-security measures with high-speed data store.

Organ donation can be done more extensively in India but there comes a need for a more agile system to easily locate the availability of organs and to find the corresponding donors before the organs get deceased. There are several difficulties in this process, such as knowing whether the patient is an organ donor, whether he/she is HIV positive, what blood group he belongs to, and the organs that can be donated. These are the parameters that are considered for the effective way to notify the hospitals about the organs that are currently available for transplantation.

II. TECHNIQUES

A. Encryption Techniques

The process of encrypting the data by a proxy, after it has been encrypted at user side i.e. proxy re-encryption is being implemented to ensure the security of data by keeping the decryption key with the proxy itself. So whenever anyone wishes to access the encrypted data they must request the proxy for the key to decrypt. The access list must be set at proxy in order to issue to keys to only those who are in that list. But as the proxy cannot be trusted with the data, there comes a need to encrypt the data initially and send it to the proxy. By encrypting the data at system side we can avoid the attack from others to some level. With the help of proxy re-encryption system, we can avoid both insider and outsider attacks to an appreciable level. Insider attacks can be prevented because the encryption being applied at proxy is unknown to anybody but the proxy itself. This type of encryption is being implemented in the below architecture.

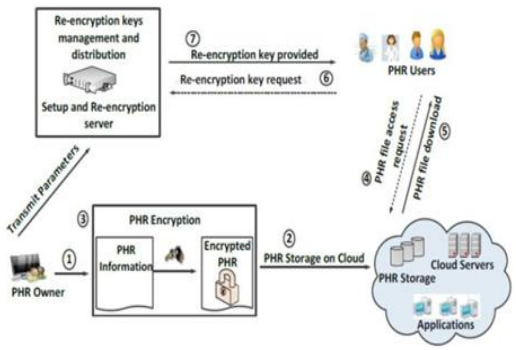


Figure 2.1 Encryption and Proxy re-encryption

Revised Manuscript Received on 14 August, 2019.

Ms. Geetha A, Assistant Professor, Department of Computer Science & Engineering, Easwari Engineering College, Chennai, Tamil Nadu, India.

Dr. S. SobithaAhila, Associate Professor,Department of Computer Science & Engineering, Easwari Engineering College, Chennai, Tamil Nadu, India.

Ms. V.S.Vidhya Lakshmi, Assistant Professor, Department of Computer Science & Engineering, Easwari Engineering College, Chennai, Tamil Nadu, India

Ms. S. Kalpana Devi, Assistant Professor, Department of Computer Science & Engineering, Easwari Engineering College, Chennai, Tamil Nadu, India

Here, the Personal Health Record (PHR) of users are being encrypted with El-Gamal encryption and sent to a Setup and Re-encryption Server (SRS) for the proxy encryption. After encryption, it is stored in the cloud. Whenever the user wants to access the PHR they first obtain the file from the cloud by using the public key available to all users in the system. To decrypt the second level of encryption, users must request the key from the SRS. Now, the SRS will check for the key that belongs to the particular user. After confirming the user with the access list, the corresponding key will be provided, with which the decryption is done. By performing two levels of encryption, we can provide security to the system to a certain level. To access this encrypted data, we must need two keys. One is the public key that is available to all users in the system and the other is the private key which is available only at the proxy. So to obtain the data we must get the key from SRS and then decrypt it. This is the encryption technique used in our system.

B.Access Control

Access control is defined as the process of assigning the accessibility rights to certain specific people, who have permission to read or make changes to that file. There are three types of access control available. They are

Discretionary Access Control.

Mandatory Access Control.

Role Based Access Control.

Out of these Role Based Access Control (RBAC) is widely used in cloud computing for restricting those who can access particular data. Anybody else not mentioned in the access control list will be denied permission to enter the system or whatever activity that has been restricted. The main advantage of using this access control system is that nobody else can cause damage to the system. It maintains the privacy and confidentiality of user data. By the efficient implementation of the access control we can easily protect it from attackers. But there is one exception when the attacker pretends to be someone with the access permission and tries to gain access into the system. This can be avoided when several parameters are taken into account such as the location of the user, with which we can make sure whether it is the user that seeks permission or somebody else.

C.Cloud platform

There are various providers of cloud such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud platform, etc. Since the website uses C#.NET with Visual Studio, we are moving with Microsoft Azure for the cloud services for our system. In this paper, we discuss a model that makes use of SQL database cloud service for the storage of highly sensitive information about the organ donors in India and also the organ requirement list collected from various hospitals, which contain the information about those people having deceased or malfunctioning organs. As sensitive data comes into use, the security measures applied must be highly effective and efficient. The usage of cloud ensures the availability of details at all respective hospitals and so the effective distribution of available organs become feasible. As cloud platforms are pay-per-use-basis, any platform which meets the user needs can be used.

III. LITERATURE SURVEY

There are several task scheduling approaches that have already been proposed in cloud computing environments. Some of them are studied and the important results are being briefed for reference. In the following, we explain some of the previous studies.

[1] Mazhar Ali et al [2018] proposed a system where the Personal Health Records (PHRs) of individuals are securely stored in the cloud by performing two levels of encryption. The cloud storage used for this system was Amazon Simple Storage Services (Amazon s3). In SeSPHR, initially encryption is done and this encrypted data is sent to a setup and proxy re-encryption server (SRS), which is a Trusted Third Party. Here the encrypted file is again encrypted with a key, which will be unknown to the users in the system. In case anybody wants to access the data from the system, they need two keys out of which one is available to all the users i.e. the public key and the key is present only at SRS. In order to obtain it, one must request the setup and proxy re-encryption server for the key. The main technique used is the proxy re-encryption for issuing the keys to authenticated users. Java Paring Based Cryptography (JPBC) was used to perform encryption of PHRs. The encryption algorithm used in this system is the El-Gamal encryption scheme. The turnaround time for encryption is given as $TT{-}up{=}tEnc{+}tup$ and the turnaround time for decryption is given as $TT{-}down{=}tDec{+}tdown$. The major factor affecting the turnaround time is the encryption and decryption part as the uploading and downloading time is minimal effect. The formal analysis and verification part was done with High-Level Net (HLPN), Z3 solver and SMT-lib. The system ensures the confidentiality of and provides access control of records that even some part of the data is not even accessible by those in the system. The performance analysis is done based on time consumed. It was found that the decryption phase was 24.38% lesser than that of encryption.

[2] Bony H.K. Chen et al [2016] proposed a secured processor architecture, Cyber DB, in order to securely store the encrypted data and to execute queries over the encrypted data. This architecture uses the AES encryption scheme but in two different modes: AES-CRT and AES-OFB. The former is the counter mode of AES and the latter is the feedback mode of AES. The usage of these modes is to offload the encryption and decryption work and to transform block cipher into a stream cipher. The Cyber DB provides the most common operations of any database, which are the creation of table, insertion, deletion, and updating of records. The performance is evaluated with DBmBench, TPC-H queries. During all the evaluation process the overhead was only minimal and the security was highly ensured. The major issue with the AES modes is that seeds must be unique for each datum. Otherwise, the system is vulnerable to “two-time” pad attack. It can also be done by sending the wrong seed by the adversary to the seed register. It introduces on an average of 10% performance overhead, which can be further reduced by using register sharing of

attribute seed and program execution.

[5] Lan Zhou et al [2016] put forth a role-based encryption technique to develop a large scale secured EHR (Electronic Health Record) system, which is called PCEHR (Personally Controlled Electronic Health Record). It was designed by the Australian government but with several security issues. The issues were met by the proposed PCEHR system as it captures practical access policies based on roles in a flexible manner and provides the security of data storage. This patient-centric health record system uses ISAAC symmetric encryption system and 160-bit elliptic curve. It uses jPBC and PBC as pairing based crypto library. JPBC wraps the PBC library to generate MNT curve. With this system, it can be seen that the cipher text size remains the same when the number of ancestor role changes. This system has an access list which has the organizations/companies that the users have granted permission to access his/her records. It provides two levels of access: Basic access control and advanced access control. With the former the user need not provide explicit access to organizations but the system itself will assign with all Healthcare organizations. The latter provides a Provider Access Consent Code (PACC) which any organization must possess in order to access the records of user. The code is set and controlled by the users.

[7] Ahmed I. Sallam et al [2017] introduced a High-Efficiency Video Coding (HEVC) selective encryption system that encrypts the highly sensitive part of the video with Rivest Cipher 6 block cipher technique. It provides low complexity overhead and faster encoding time for real-time applications. This technique should maintain the video format compliance, same bit rate, and real-time constraints. In this paper, they also compared RC6 with every mode of AES to prove the efficiency of using RC6 over AES. In order to avoid a brute force attack, a larger key space must be employed and by using RC6 in this technique, which is a 128-bit key length encryption, we obtain 2^{128} key space size. It provides immunity against brute force attack. The histogram analysis of the plain video and encrypted video shows that both of them are very different, which supports the security feature. The RC6 encryption enhances faster encoding as it is less complex and simple when compared to the AES. With the help of HEVC SE, we can securely transmit a video file very quickly and with high level of security to receiver end.

[3] Chenhao Lin et al [2018] improvised the existing robust thin-plate spline (RTPS), which was used to match the legacy contact based fingerprints to contactless fingerprint databases. The problem this RTPS had was some deformations and accuracy issues. Moving to the contactless fingerprint is a need because we want to provide much secure, hygiene and accurate fingerprint detection. In order to remove any deformations that occurred in the conversion a robust thin-plate spline based Deformation Correction Model (DCM) has been proposed by Chenhao Lin. By the usage of DCM we can achieve results in accurate alignment of key minutiae features that was observed in both the methods. The results suggest that the contact based fingerprint matching using the deformation correction model and the robust thin-plate spline provides more accurate findings with equal error rate (EER) as 4.46 % whereas the thin-plate spline from other researches had significantly higher EERs.

[8]Xuefeng Liu et al [2013] proposed a multi-owner data sharing scheme known as Mona to overcome the hindrances while sharing the data in a multi-owner environment such as preserving the data and identity privacy. By using this multi-owner sharing scheme we can make the storage overheads independent of the number of revoked users. The computational cost of Mona is very less when compared to other schemes. It is significantly reduced stating the efficiency of this multi-owner data sharing scheme. Also, the computational cost increases as the number of users revoked increases but the computational cost for the basic operations being done are almost the same for smaller and larger files. The total storage of each user in the system is 572 bytes. He clearly explains the operations such as file generation, access, and deletion. Along with this, the file updating option is also available. Mona, a secure multi-owner data sharing system is cost efficient and with very less memory overhead.

[4] Ke Li et al [2015] did a security analysis on the one-to-many order-preserving encryption based cloud data search. In order to perform ranked search in encrypted cloud data, a tool called order-preserving encryption (OPE) is used. But while using deterministic OPE, the cipher texts started to show relevance, which is not encouraged in any encrypted data. Therefore a probabilistic approach called one-to-many OPE. This scheme employs a random probabilistic method to assign the cipher texts. A bucket m is picked and then randomly any value in the bucket is chosen as cipher text. This one-to-many OPE can be developed in many ways including dividing the plaintext of the same value into several sets and dividing the corresponding set into sub-buckets. By doing so, we improve the security of the data and pose a challenge for the attacker to decrypt it.

[9] ParthaDutta et al [2014] proposed C-Cloud, a cost-efficient cloud for surplus cloud computing resources, which is a democratic infrastructure of cloud for renting and sharing cloud resources. It also includes the non-cloud equipment such as PCs, laptops, etc. With the help of C-Cloud large amounts of cloud resources can be shared thereby making the owners of the machines earn a lot of cash by subletting their idle system for the use of others. An incentive mechanism is being used in this system for exceptionally standing out of other systems. The main disadvantage of this model is that the interaction between the C-Cloud and those who periodically shared their resources to check the status. In this an open source distribution for volunteer computing has been used for the interaction purposes.

IV. PROPOSED SYSTEM

Our paper proposes a system which securely stores the organ donor details and allows accessing of the same only at a particular time. The system and functional architecture of the model are described below:

A. System Architecture:

In order to perfectly keep track of the organ donors, we store the details of the donor over the cloud, so that it is available everywhere. As the data are highly sensitive, we perform encryption on them before storing it in the cloud. It is done because in case of an accident if the patient goes into the brain dead situation, there is no way to know if he's a pledged donor. To know this efficiently we built a new system, which will read the fingerprint of the brain dead patient and cross-check with the fingerprints in the database. If a match is obtained then, the particular patient is an organ donor. Then the donor's details are extracted, once they are successfully decrypted. For the successful implementation of the system, we need the requirement list of organs that are currently needed, which will be collected from various hospitals. Now the extracted donor details are run against this list to find the matching donors. The parameters that are used for finding the matching donors are blood group, HIV status, organs and finally location. The requirement from the hospitals that satisfy all the above parameters is shortlisted. With the obtained list we send the notifications to the respective hospital to indicate the availability of organs.

The major components of our model (Fig. 4.1) include the mobile application, website, Setup and Re-encryption Server, cloud database. The mobile application is used to get the details from the pledged organ donors; website is used at hospitals in order for them to enter the organ requirement details and to find the details of the organ donor; Setup and Re-encryption Sever to provide the decryption keys to the hospitals while accessing the organ donor details; cloud database to store all the details on the cloud for easy access to the data anywhere anytime. At the end of the entire process, hospitals will obtain notification about the availability of organ as per the requirement provided by that hospital.

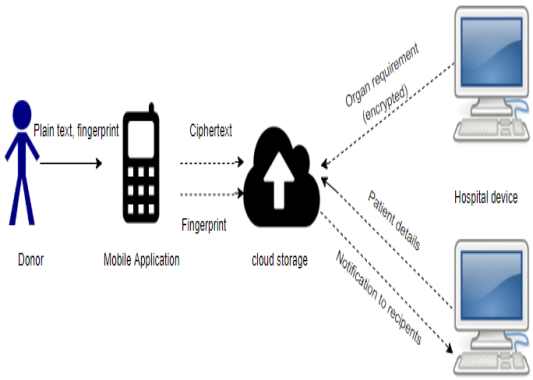


Figure 4.1 System Architecture of the system

B.Functional Architecture:

The functional architecture (Fig.4.2) gives the entire functional modules of our system. The system can be briefly classified into three modules, each of them performing some task to reach the final output or goal. The modules are,

- Donor data encryption
- Donor authentication
- Notification generation

Donor data encryption:

The donor data encryption module mainly encrypts the data and stores in the cloud database. Initially, the organ requirement list must be collected from the hospitals. The requirement list data are encrypted and then stored securely in the database. Any hospital in the system can access this list as they are allowed to do so. Now, an Android application is created to read the data from the pledged organ donors. In order to connect the mobile application with the web, a service API is being used. It is where the actual encryption of data is done. The encryption algorithm used in this system is Rivest Cipher 6 (RC6) encryption (Fig. 4.2.1), which is derived from RC5. RC6 is a 128-bit block cipher with key sizes varying between 128, 192 and 256. RC6 requires more CPU and memory resources for encryption but it results in higher efficiency when the encryption speed is taken into account. After encryption, the encrypted data are sent to a proxy to perform the proxy re-encryption. When the second level of encryption is also done, the data are stored in the cloud database. Once the encryption phase is over, all the encrypted details along with fingerprints and requirement list are stored in the cloud.

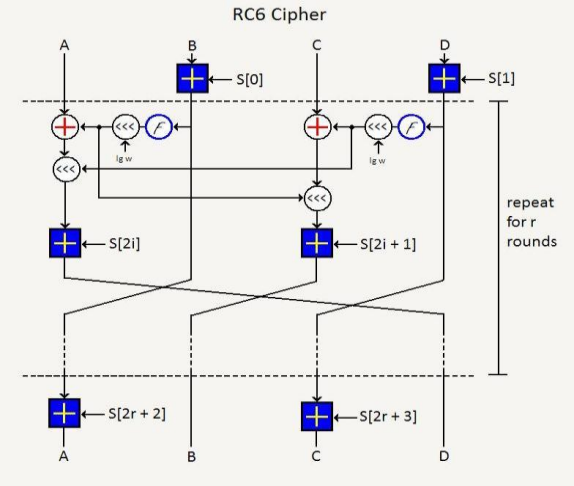


Figure 4.2.1 RC6 implementation

Donor authentication:

In case an accident occurs and the patient is diagnosed to be brain dead or any person who wants to donate organ, in order to verify whether they have signed up as an organ donor, we must read their fingerprint. Once it is done, it is cross-checked with the fingerprints stored in our cloud database of pledged organ donors. In case of a match, the details of the patient are extracted after decrypting the two levels of encryption. Now to decrypt the first level of encryption, we must request the key from Setup and Re-encryption Server (SRS). Once the SRS has authenticated the request as positive, it will issue the key. With the public key which is available to all hospitals in the database, we can decrypt the second level of encryption. Now we can obtain the details of the organ donor in a matter of time.

Notification generatio

With the collected details of the donor, we perform SQL query filtering on the cloud database containing the organ

requirement list. The major fields to be considered are blood group, HIV positive or negative, organs that are needed and location. If all the fields match, then the concerned hospital providing that detail is notified the availability of organs. All the notifications are sent directly to the website that the hospital uses. Then the hospital contacts the particular individual and carries out the procedures. By this way, we may increase the chances of survival as there is no time wasted trying to contact the patient's family to check if he is an organ donor.

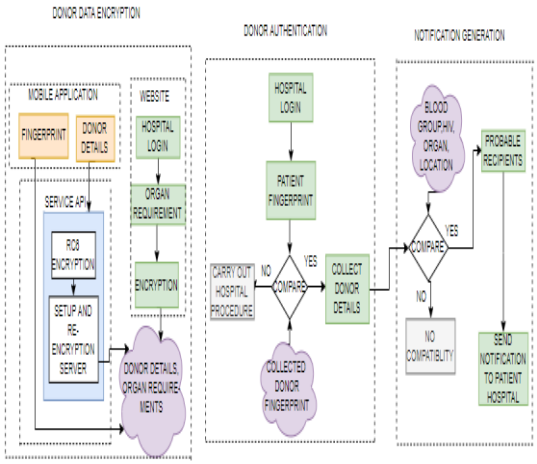


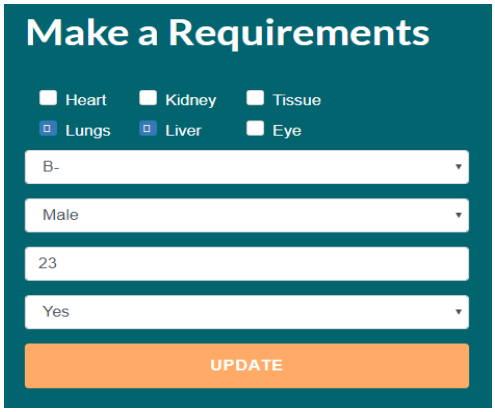
Figure 4.2 Functional architecture of the entire system

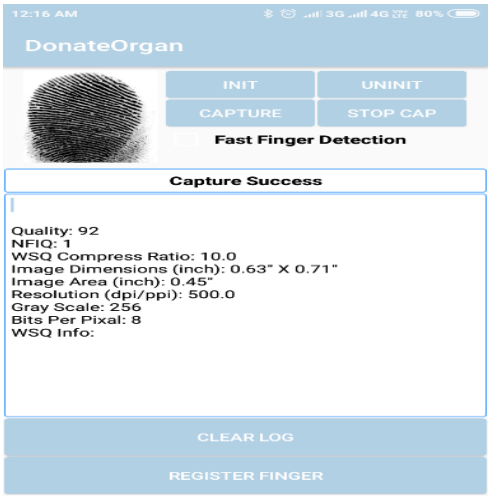
C.System implementation:

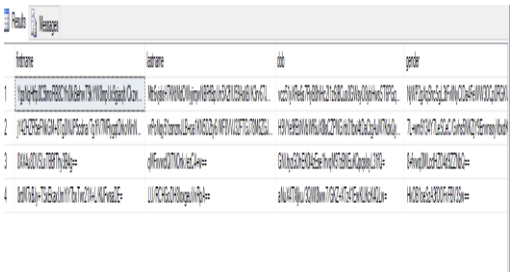
The proposed system has been implemented for certain hospitals from which the requirements are gathered and to which notifications are sent when matching donors are found when an organ donor who died being in the hospital. The modules defined are implemented to support our project.

Donor Data Encryption:

The output of this donor data encryption module is the successful storage of organ donor details and the requirement list from the hospital over the cloud. The main part is the encryption of the details carefully to avoid attackers to view the original data of the donors. The organ donor details are collected using an android application from the pledged donors. The fingerprint is read using a fingerprint reader and the threshold is set to maintain the quality of the fingerprint. In case it does not meet the specified threshold then it is asked to scan the fingerprint again. The requirement list is collected from the hospitals using a website. The following screenshots show the result of this module.





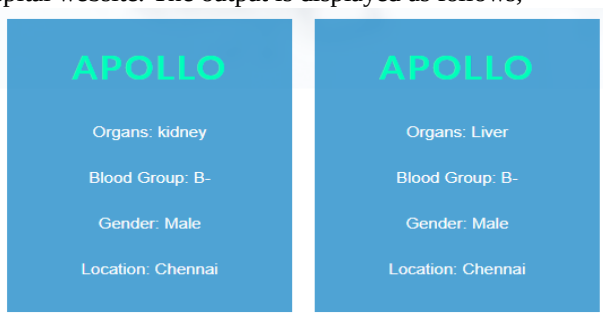


Donor Authentication:

The result of this module is the collection of the organ donor details from the database if the patient admitted is an organ donor. It is done by comparing the fingerprint of the patient with those in the database and if a match is found, then the hospital requests the Setup and Re-encryption Server for the decryption key. Once the key is issued to the hospital it can decrypt the outer encryption and with the public key available to hospitals in the database the inner encryption is decrypted. Now we can obtain the organ donor's details.

Notification Generation:

The final module produces the notification to the hospitals following some parameters. Firstly, the collected details of the organ donor are compared with the requirement list from the cloud. The parameters taken into account are blood group, matching organs, HIV positive or not and finally the location. Once the parameters are satisfied, the notification is sent to the corresponding hospital which provided the matching requirement. The result of this module is the display of notification in the hospital website. The output is displayed as follows,

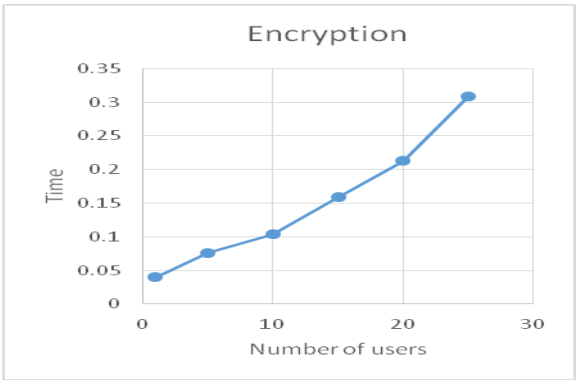


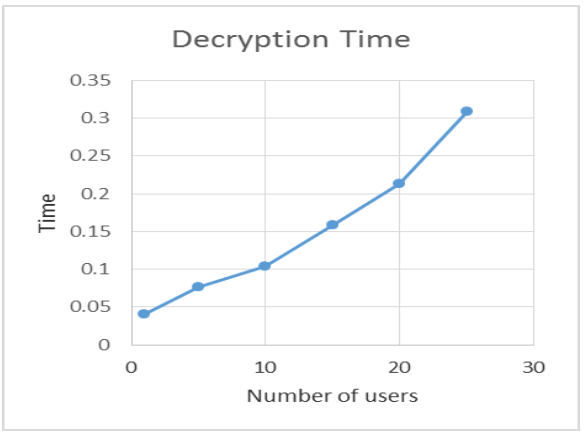
A notification is like will be displayed in the respective hospital's website login itself. After that, the hospital carries out further procedures like calling the patient in and arranging for the organ transplantation.

V. PERFORMANCE ANALYSIS& RESULTS

In this section, we are going to study about the system's performance and accuracy that has been achieved. The dataset for the system is given manually since all the organ donors are asked to register themselves in the android application. The organ requirement list must be obtained from the hospitals from the website itself. We are ensuring the privacy and confidentiality of the data provided with our encryption techniques. The RC6 encryption is proved to be one of the most secure encryption algorithms and the EER (equal error rate) of this algorithm is only 4.46 % which is comparatively lower than most other algorithms. With the usage of Setup and Re-encryption Server, we provide added security to the organ donor details.

The encryption time required for the system is a bit longer than other models since our model uses two levels of highly secure encryption algorithms- Advanced Encryption Scheme (AES) and Rivest Cipher 6 (RC6). But on the other hand decryption time is shorter because these algorithms we used are block ciphers and only during encryption the operation needs to be done block by block but during decryption, there is no need for such mechanism. Parallelism can be implemented depending upon the processor we are using to decrease the decryption time. The graph 5.1 shows the encryption time for several numbers of users while graph 5.2 shows the decryption time required for the same number of users.





Graph 5.1 Encryption time required for users
Graph 5.2 Decryption time required for users

The above graphs prove that even though the time taken for encryption is higher than many systems the decryption is comparatively very low because once the key has been issued by the Setup and Re-encryption Server (SRS), it can be decrypted very quickly. Therefore the performance of the system can be increased as the rate at which decryption occurs is 26% faster than earlier systems.

VI. CONCLUSION AND FUTURE WORK

Although many existing systems have implemented the system, they were not able to successfully find the match and availability of organs at the needed time. Our proposed system successfully finds the available organs and sends the notification to the hospitals where there are people in need of organs. It can be extended in many directions. One of them is to increase the location accuracy to find the nearest hospital midway between the donated organ and the recipient in real-time. By doing so we increase the success of organ transplant as the time available for the transplantation process can be increased.

REFERENCES

1. Mazhar Ali, Assad Abbas, Muhammad Usman Shahid Khan, and Samee U. Khan, 2018, "SeSPHR: A methodology for secure sharing of personal health records on cloud", IEEE Transactions on Cloud Computing, Vol. :14, Issue: 8
2. Bony H.K. Chen, Paul Y.S. Cheung, Peter Y.K. Cheung and Yu-Kwong Kwok, 2016, " Cyber DB: A novel architecture for outsourcing secure database processing", IEEE Transactions on Cloud Computing, Vol. :6, Issue: 2
3. Chenhao Lin and Ajay Kumar, 2018, "Matching contactless and contact-based conventional fingerprint images for biometrics identification", IEEE Transactions on Image Processing, Vol. :27, Issue:12
4. Ke Li, Weiming Zhang, Ce Yang, and Nenghai Yu, 2015, "Security analysis on one-to-many order preserving encryption based cloud data search", IEEE Transactions on Information Forensics and Security, Vol. :10, Issue: 9
5. Lan Zhou, Vijay Varadharajan, and K. Gopinath, 2016, " A secure role-based cloud storage system for encrypted patient-centric health records" IEEE Journal of Computer, Vol. :59, Issue: 11
6. Maria Alejandra Rodriguez, and Rajkumar Buyya, 2014, " Deadline based resource provisioning and scheduling algorithm for scientific workflow on clouds", IEEE Transactions on Cloud Computing, Vol. :2, Issue: 2
7. Osama S. Faragallah, El-Sayed M. El-Rabaie, and Ahmed I. Sallam, 2017, "HEVC Selective Encryption using RC6 block cipher technique, IEEE Transactions on Multimedia, Vol. :20, Issue:7
8. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, 2013, "Mona : Secure multi-owner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, Vol. : 24, Issue :1
9. Partha Dutta, Tridib Mukherjee, Vinay Gangadhar Hegde and Sujit Guhar, "C-Cloud: A cost-efficient reliable cloud for surplus computing resources", IEEE
10. 7TH International Conference on Cloud Computing, September, 2014

11. Niansheng Liu, Jianjun Cai, Xiaojuan Zeng, Guanhua Lin, and Jiaoru Chen, "Cryptographic performance for Rijndael and RC6 block ciphers", IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), October, 2017
12. Cong Wang, Nin Cao, Kui Ren, and Wenjing Lou, 2012, "Enabling secure and efficient ranked keyword search over outsourced cloud data", IEEE Transactions on Parallel and Distributed Systems, Vol.: 23, Issue:8
13. Christian Esposito, Aniello Castiglione, and Kim-Kwang Raymond Choo, 2016, " Encryption-based solution for data sovereignty in federated clouds", IEEE Cloud Computing, Vol.: 3, Issue:1
14. Po-Wen Chi, and Chin-Laung Lei, 2018, "Audit-free cloud storage via deniable attribute-based encryption", IEEE Transactions on Cloud Computing, Vol.:6, Issue:2
15. Chang Liu, Liehuang Zhu, and Jinjun Chen, 2017, "Graph encryption for top-K nearest keyword search queries on cloud", IEEE Transactions on Sustainable Computing, Vol.: 2, Issue:4
16. Linmei Jiang, and Donghui Guo, 2017, "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage", IEEE Access, Vol.:5

AUTHORS PROFILE

Ms.A.Geetha working as Assistant Professor in Easwari Engineering College, Chennai, She received her B.Tech. Degree from Anna University, Chennai in the year 2005, M.E. Degree from Anna University, Chennai in the year 2009. She has more than 13 Years teaching experience and her areas of specializations Machine Learning, Cloud security. She has 7 research publications and 6 conference proceedings in her account.

Dr.S. SobithaAhila working as Associate Professor in Easwari Engineering College, Chennai,She received her B.E. Degree from Madurai Kamaraj University in the year 1997, M.E. Degree from Bharathidhasan University, Trichy in the year 2002 and Ph.D degree from Anna University,Chennai in the year October 2016.She has more than 16 years teaching experience and her areas of specializations are Data Analytics,CloudSecurity,Web Mining, Multi agent System.She has 20+research publications and 15+conference proceedings in her account.

Ms.V.S.Vidhyalakshmi currently working as assistant professor at Easwari Engineering College, Chennai. She received her B.E. Degree from Anna University in the year 2009, M.E. Degree from Anna University, Chennai in the year 2017.She has 2.5 years of teaching and 3.5 years of IT experience. Her areas of interest include Machine Learning, Block Chain, Data Analytics. Currently she is working on block chain uses cases in finance and healthcare domain

Ms.S.KalpanaDevi working as Assistant Professor in Easwari Engineering College, Chennai, She received her B.E. Degree from Madras University, Chennai in the year 2004, M.Tech Degree from Dr.M.G.R Educational and Research Institute , Chennai in theyear 2008. She has more than 14 years teaching experience and her areas of specializations are Design and Analysis of Algorithms,Networkingand Machine Learning. She has 11 research publications