ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Aadhaar Card Based Health Records Monitoring System

B. Sreesaila[1], K. Abinaya[2], M. Swarnalatha[3], Dr.R.Sugumar[4]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1,2,3]

Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [4]

ABSTRACT: Cloud computing is an emerging as a new computing paradigm in the medical sector besides other business. Storing the medical data in cloud makes the treatment efficient by retrieving patient's medical history from the database.This system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. This handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored using Aadhaar Number and an identification number will be generated when the patient's data are stored into the database for the first time after the implementation of the system. Whenever the patient go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the license number along with the identification number of the person whose record has to be stored.Wepropose a scheme to help enterprises to efficiently share confidential data on cloud servers using Hierarchical attribute based encryption algorithm.

KEYWORDS: Hierarchical Attribute-Based Encryption Algorithm, Cipher-text policy Attribute-Based Encryption, Hierarchical Identity-Based Encryption, Aadhaar card Number, Identification Number, License Number

I. INTRODUCTION

Cloud computing has rapidly become a widely adopted model for delivering services over the internet. In this proposed system, Jelastic cloud is used.**Jelastic** is a cloud services provider that combines PaaS (Platform as a Service) and CaaS (Container as a Service) in a single package for hosting providers, telecommunication companies, enterprises and developers. The platform is available as public cloud in more than 60 data centers worldwide, private cloud (virtual and on premise), hybrid and multi-cloud. Jelastic provides support of Java, PHP, Ruby, Node.js, Python, .NET, Go environments and custom Docker containers. Cloud service provider must provide the trust and security, as there are large amount of important and sensitive data stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. With the emergence of sharing confidential corporate data on cloud servers, it is essential to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data[2]. In this paper, we first propose a Hierarchical Attribute-Based Encryption (HABE) model by combining a HIBE system and a CP-ABE system, to provide fine-grained access control and full delegation. Based on the HABE model, we construct a HABE scheme by making a performance-expressivity tradeoff, to achieve high performance. Finally, we propose a scalable revocation scheme by delegating to the CSP most of the computing tasks in revocation, to achieve a dynamic set of users efficiently. Ciphertext-Policy Attribute-Based Encryption (CP-ABE), as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. However, a CP-ABE system may not work well when enterprise users outsource their

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

data for sharing on cloud servers, due to the following reasons: First, one of the biggest merits of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device, such as thin clients with limited bandwidth, CPU, and memory capabilities,Wang[5]. Therefore, the encryption system should provide high performance. Second, in the case of a large-scale industry, a delegation mechanism in the generation of keys inside an enterprise is needed. Our main design goal is to help the enterprise users to efficiently share confidential data on cloud servers. Specially, we want to make our scheme more applicable in cloud computing by simultaneously achieving fine-grained access control, high performance, practicability, and scalability. Cloud based health system's main focus is the patient's data collection, storage, access,analysis and presentation etc. The current patient data collection techniques are time consuming,inefficient, laborious for the staffs[3]. It is also obvious that currents technique is violating the real time data access for monitoring the patients. Cloud computing is emerging as a promising paradigm for computing and is drawing the attention from both academia and industry. The cloud-computing model shifts the computing infrastructure to third-party service providers that manage the hardware and software resources with significant cost reductions. It is emerging as a new computing paradigm in the medical sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Storing the medical data in cloud makes the treatment efficient by retrieving patient's medical history from the database before going for the treatment and get to know about the health issues of the patient.

II. RELATED WORKS

[1] In 2014,Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geo-distributed clouds for e-health monitoring system with minimum service delay and privacy preservation,In this, resource allocation scheme significantly reduces the service delay compared to two other alternatives using jointly the short queue and distributed control law[1].

[2] In 2014,Y. Yang, H. Li, L. Wenchao, H. Yang, and W. Mi, "Secure dynamic searchable symmetric encryption with constant document update cost," in Proceedings of GLOBECOM. With the development of cloud computing, data sharing has a new effective method, i.e., outsourced to cloud platform. In this case, since the outsourced data may contain privacy, they only allow to be accessed by the authorized users. In this paper, we leverage the secure k-nearest neighbor to propose a secure dynamic searchable symmetric encryption scheme. Our scheme can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in Dynamic Searchable Symmetric Encryption (DSSE) area. In addition, we evaluate the performance of our proposed scheme compared with other DSSE schemes. The comparison results demonstrate the efficiency of our proposed scheme in terms of the storage, search and update complexity[2].

[3] In 2013, M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

[4] In 2012, H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, An smdpbased service model for inter-domain resource allocation in mobile cloud networks. Mobile cloud computing is a promising technique that shifts the data and computing service modules from individual devices to geographically distributed cloud service architecture. In this paper, we propose a service decision making system for inter domain service transfer to balance the computation loads among multiple cloud domains. To this end, we formulate the service request decision making process as a semi-Markov decision process. The optimal service transfer decisions are obtained by jointly considering the system incomes and expenses. Extensive simulation results show that the proposed decision making system can significantly improve the system rewards and decrease service disruptions compared with the greedy approach.

[5] In 2012, C. Wang, K.Ren, S. Yu, and K. M. R. Urs, Achieving usable and privacy-assured similarity search over outsourced cloud data. In this paper, we investigate the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. We formally prove the privacy-preserving guarantee of the proposed mechanism under rigorous security treatment. To demonstrate the generality of our mechanism and further enrich the application spectrum, we also show our new construction naturally supports fuzzy search, a previously studied notion aiming only to tolerate typos and representation inconsistencies in the user searching input. The extensive experiments on Amazon cloud platform with real data set further demonstrate the validity and practicality of the proposed mechanism.

III. PROPOSED SYSTEM

Cloud based health system solution is based on the concept of “Cloud Computing” a distributed computing system where a pool of virtualized, dynamically-salable, managed computing power, storage, platforms, and services are delivered. This system provides an environment where patient’s records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. This handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored using Aadhaar Number and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system.A person who are interested to donate their organs can also register in patient registration module. Whenever they go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the license number along with the identification number of the person whose record has to be stored.

a)SYSTEM DESIGN

As shown in Fig.1, our schemes consists of three entities.
Trusted authority: A trusted authority is a trusted third party. We use it to generate hierarchical attribute-based encryption key to encrypt the medical documents.
HH

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

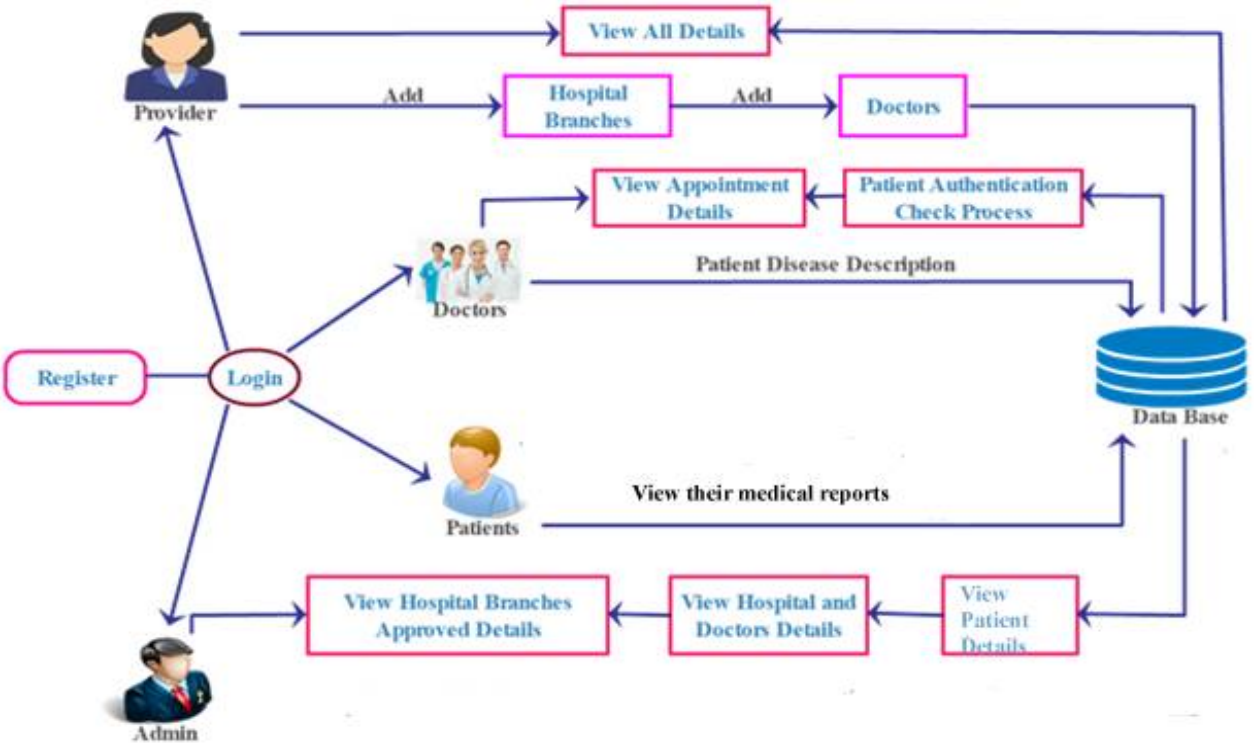


Figure 1: Overall System Design

Hospital: An authorized doctor can obtain the secret key from the patient, where this key can be used to generate trapdoors and sends it to the cloud server. Then he/she receives the matching document collection from the cloud server and decrypts them with the Hierarchical attribute based encryption key received from the trusted authority. After getting the health information of the patient, the doctor can also outsource medical report to the cloud server by the same way.

Patient: To protect the data privacy, the patient encrypts the original documents under an access policy using Hierarchical attribute-based encryption.

Hospital Registration subsystem

In this subsystem, every provider must have a unique hospital details and doctor list.In this, hospitals can register their hospitals details in cloud. Some of the following details is needed to register. They are Hospital name, Provider name, License number, Password, Security questions, Address, City, Pin-code, hospital email_id, Year_of_starting. Then hospitals can login using License number and password.This system is implemented in NetBeans. NetBeans is a software development platform written in Java. The NetBeans Platform allows applications to be developed from a set of modular software components called modules. The NetBeans IDE is primarily intended for development in Java, but also supports other languages, in particular PHP, C/C++ and HTML5.NetBeans is cross-platform and runs on Microsoft Windows, Mac OS X, Linux, Solaris and other platforms supporting a compatible JVM.Back end – MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

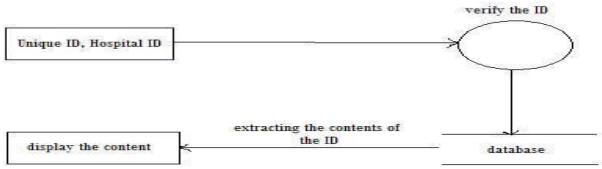


Figure 2:Hospital Registration subsystem

User Registration Subsystem

In this subsystem, user should register their details using Aadhaar Number. Then the identification number will be generated in user emails. If the user is interested or willing to donate organs then they have to register it in Organ Donor subsystem.Using Aadhar_id and user identification number, patient can able to view their details. In this subsystem, each and every details of the patients will be encrypted to provide security. If the patient need to encrypt the particular details then they have to click the check box in the user registration module. User can login the page by using their Aadhaar Number and identification number. The main goal of the module denotes security for viewing our personal information to all roles in an application. To prevent that we had proposed to use Hierarchical Advanced Encryption Algorithm for the access to encrypt the Selected Details to Restrict to view by others. When doctor login the hospital module then the patient login module will be automatically opened. After that Patient medical details are added by doctors.The merits of an Encryption Algorithm are achieving data confidentiality and identity privacy with high efficiency, efficiently realizing access control of patient's personal health information,resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

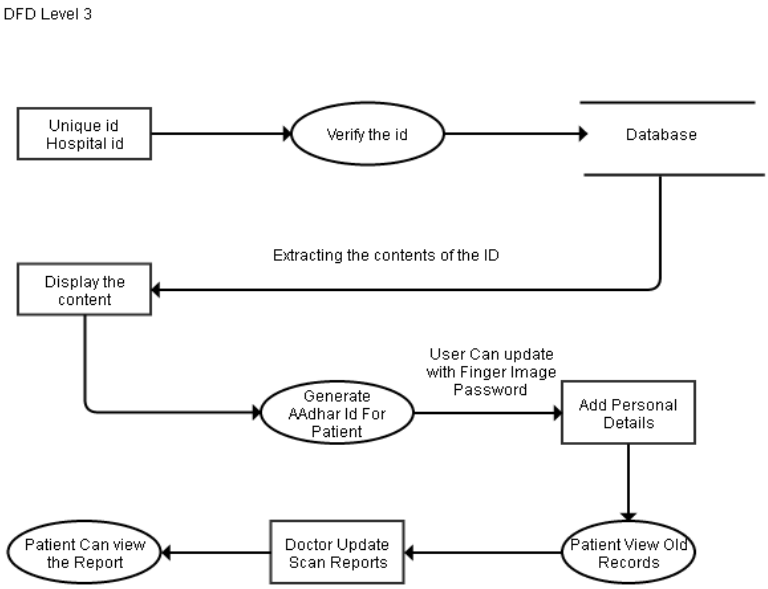


Figure 3: User Registration Subsystem

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Admin Page Subsystem

Admin can add, delete and update hospital details and patient details in cloud. In this subsystem, all hospital details and patient details are added in centralized cloud. So users can show their past medical details to any other hospitals within his/her country. User must Authorised in an application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users. Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information. Admin can able to view overall users report, users personal Records and User Counselling Records.A cloud server is an intermediary entity which stores the encrypted documents and the corresponding indexes received from patients, and then provides data access and search services to authorized search doctors. When a search doctor sends a trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.

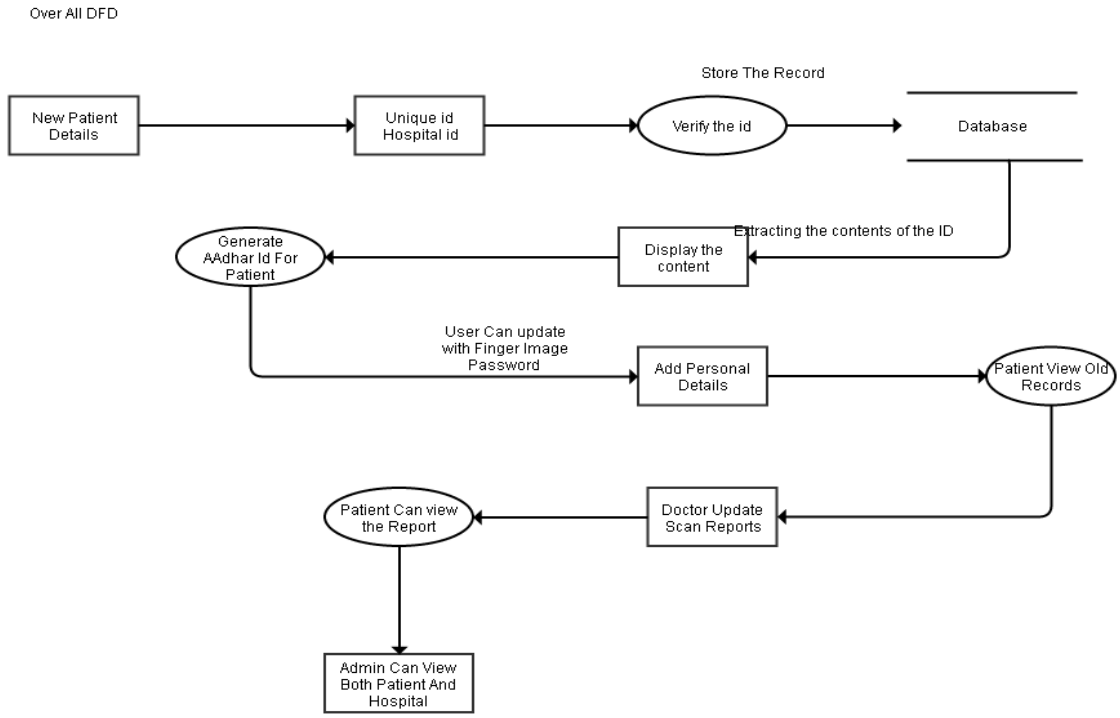


Figure 4: Admin Page Subsystem

b)ALGORITHM

The Hierarchical Attribute-Based Encryption (HABE) is derived by Wang et al The HABE model consists of a Root Master (RM) that corresponds to the Third Trusted Party (TTP),Multiple Domain Masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. This scheme can satisfy the property of fine grained access control, scalability and full delegation. It can share data for users in the cloud in an enterprise environment. Furthermore, it can apply to achieve proxy re-encryption. But in practice, it is unsuitable to implement. Since all attributes in one conjunctive clause in this scheme may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

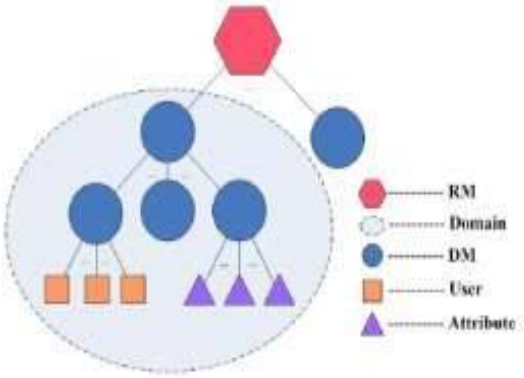
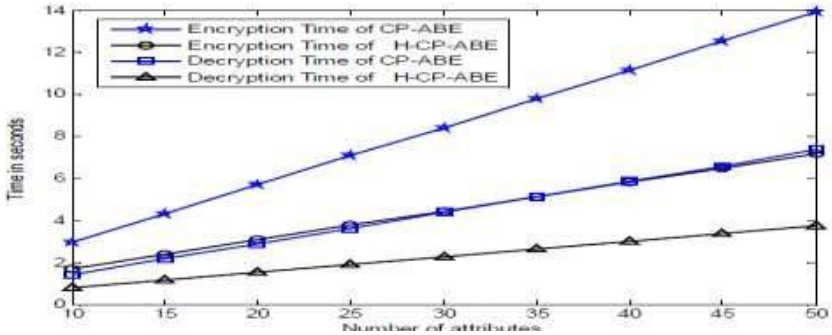


Figure 5: A three-level HABE Model

In HABE model, the RM's role closely follows the root private key generator (PKG) in a HIBE system, is responsible for the generation and distribution of system parameters and domain keys. The DM, whose role integrates both the properties of the domain PKG in a HIBE system and AA in a CP-ABE system.



It is responsible for delegating keys to DMs at the next level and distributing keys to users. Specifically, we enable the leftmost DM at the second level to administer all the users in a domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute. Also other DMs administer an arbitrary number of disjoint attributes, and have full control over the structure and semantics of their attributes. In the HABE model, we first mark each DM and attribute with a unique identifier (ID), but mark each user with both an ID and a set of descriptive attributes. Then,as Gentry et al 2002, we enable an entity's secret key to be extracted from the DM administering itself, and an entity's public key, which denotes its position in the HABE model, to be an ID tuple consisting of the public key of the DM administering itself and its ID.

IV. RESULTS

Hospital Registration Subsystem:

As shown in Figure 6 for hospital registration – hospital name, provider name, license number, password, address, city, pin-code, email-id, year of starting are required to register the hospital in cloud. After filling the above details, click the register button then popup message will appear like "your registration is successful" if the given details are valid. Otherwise it shows invalid data. After registration, hospital can login the page using license number and password.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

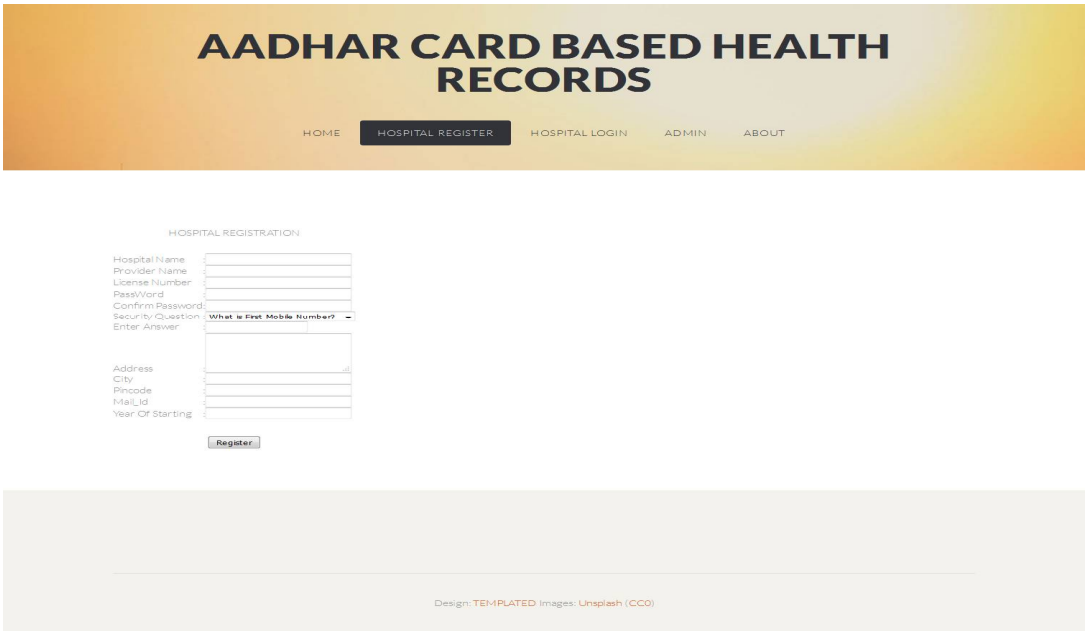


Figure 6: Hospital Registration Subsystem

User Registration Subsystem:

For user registration as shown in the figure 7 – Patient image, Aadhaar Number, Patient name, Gender, Date of Birth, Contact Number, Address, City, Pin-code, email-id, Patient finger image are required. After registration, patient can login the page using Aadhar Number and password.

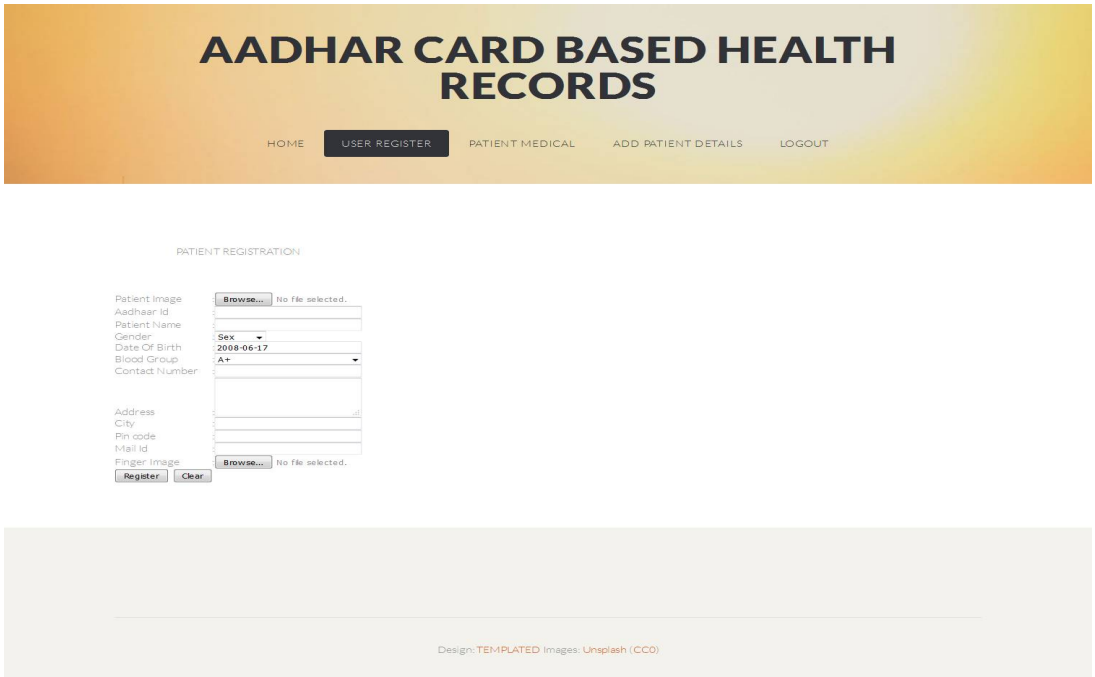


Figure 7: User Registration Subsystem

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Patient Reports Subsystem

As shown in the figure 8 – Patient reports are added like x-ray report, ECG report, Scan report etc.., using patient Aadhaar number and password. Date of entering the patient reports are very important because using date only doctor can search and view the previous reports of the patient.

Data's are encrypted using Hierarchical attribute based encryption algorithm.

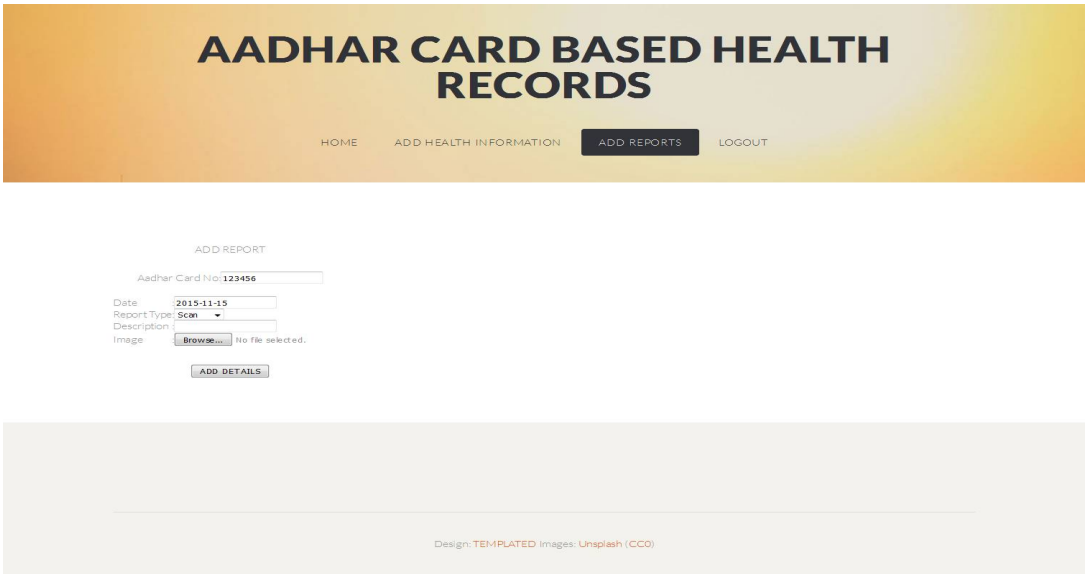


Figure 8: Patient Reports Subsystem

Patient Medical Subsystem

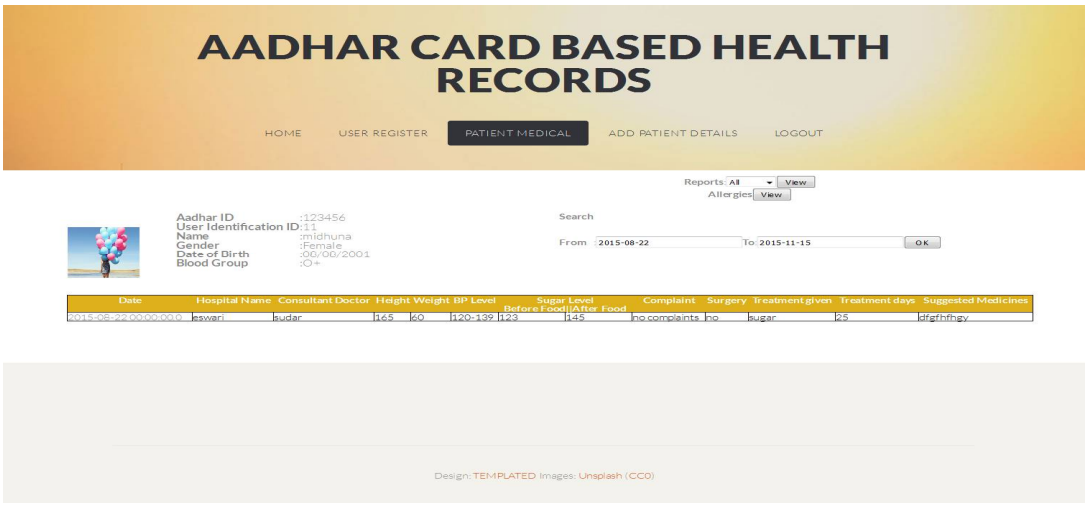


Figure 9: Patient Medical Subsystem

As shown in the figure 9 – Patient full details can be viewed in Patient Medical Subsystem. In this Subsystem, search button is used to search the previous medical details of the patient. If the patient report view button is clicked then one time password will be generated in the patient email. Using OTP only, doctor can view the patient reports.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Admin Page hospital details

In this subsystem, all hospital details are displayed which is registered in the cloud.Admin can add, delete or update the hospital details. Using Hospital license number, admin can search required hospital details.

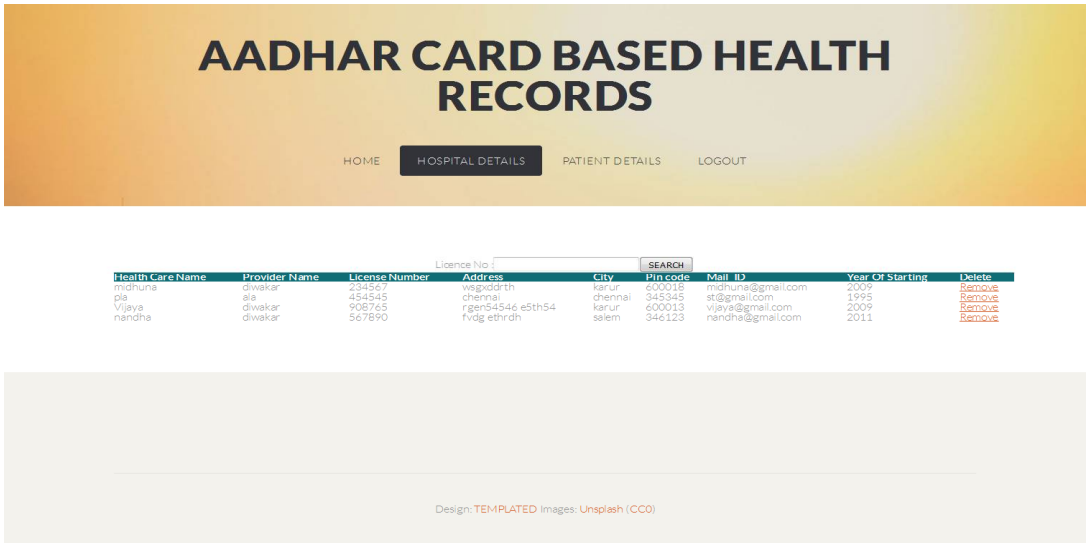


Figure 10: Admin page hospital details

Admin Page Patient Details

In this subsystem, all patient details are added or deleted by admin. Search button is used to search a particular patient details using Aadhaar Number. Store vast amount of medical data, Efficient treatment through the data reference,Reduce the difficulties to keep the data safe are the merits of this system.

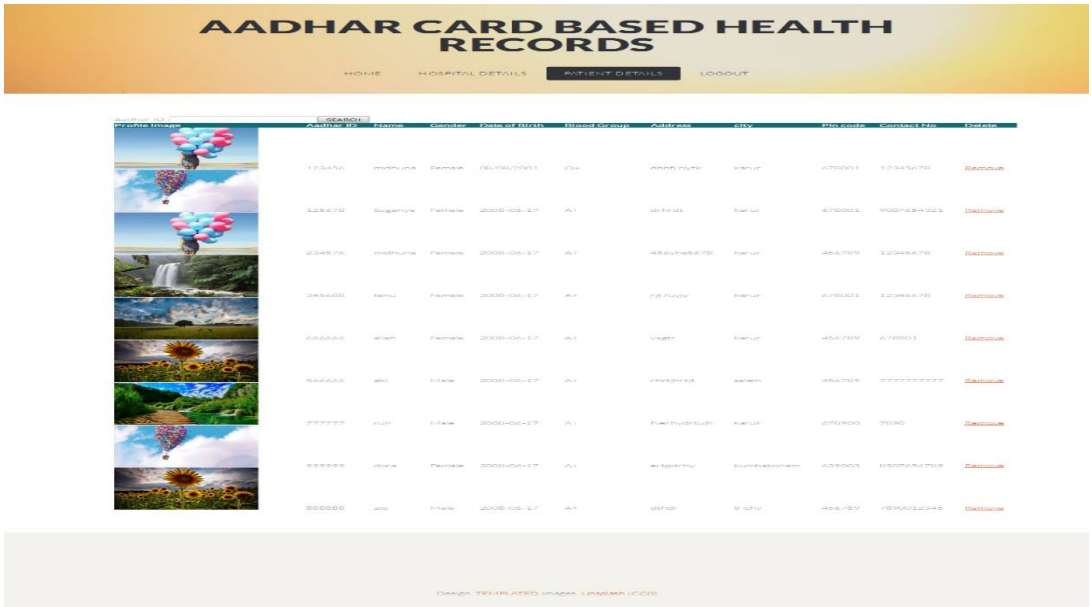


Figure 11: Admin page patient details

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

V. CONCLUSION

A proposed system which monitors the health care details of each individual of the country. It comprises of modules like generating the unique ID and store and retrieve data of a person. Performance evaluation demonstrates that the proposed schemes can achieve better efficiency than the existing works in terms of storage, search and updating complexity. The cloud computing is an emerging computing mode. It promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. The nature of cloud computing is useful for constructing the data center. To the new generation of cloud based health system, cloud computing is better approach in the future.

REFERENCES

1. Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geodistributed clouds for e- health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and HealthInformatics, vol. 18, no. 2, pp. 430–439, 2014.
2. Y. Yang, H. Li, L. Wenchao, H. Yang, and W. Mi, "Secure dynamic searchable symmetric encryption with constant document update cost," in Proceedings of GLOBECOM. IEEE, 2014, pp. 775–780
3. F. Hahn and F. Kerschbaum, "Searchable encryption with secure and efficient updates," in Proceedings of CCS. ACM, 2014, pp. 310–320.
4. X. Yuan, X. Wang, C. Wang, A. Squicciarini, and K. Ren, "Enabling privacy-preserving image-centric social discovery," in *Proceedings ofIEEE ICDCS*, 2014, pp. 198–207.
5. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.
6. Changji Wang and JianfaLuo," An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length", Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2013, Article ID 810969, 7 pages.
7. H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An smdpbased service model for interdomain resource allocation in mobile cloud networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 2222–2232, 2012.
8. C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in Proceedings of IEEE INFOCOM, 2012, pp. 451–459.
9. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.
10. S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2011.
11. J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, "Self-Protecting Electronic Medical Records Using Attribute-Based Encryption," Cryptology ePrint Archive, Report 2010/565, http://eprint.iacr.org/, 2010.
12. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.
13. Franke, C., Robinson, P.: Autonomic provisioning of hosted applications with level of isolation terms. In: 2010 Seventh IEEE International Conference and Workshops on Engineering of Autonomic and Autonomous Systems, pp. 131–142 (2008)
14. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.
15. Chase M., "Multi-Authority Attribute Based Encrypt-Ion," in Proceedings of the 4th Conference on Theory of Cryptography, Berlin, pp. 515-534, 2007.
16. J. Bettencourt, A. Sahai, and B.Waters "Ciphertext-Policy Attribute Based Encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.
17. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings o ACM CCS, 2006, pp. 79—88.
18. Volume 2013, Article ID 810969, 7 pages 6. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98, October 2006.
19. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology–Eurocrypt. Springer, 2004, pp. 506–522.
20. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.