AN EFFICIENT ENCRYPTED MEDICAL DATA STORAGE USING TWO CLOUDS WITH DUPLICATE DATA GENERATION TECHNIQUES

K.Balasubramanian[1], D.Madhuri[2], S.Muthukarthiga[3] , S.Preetha[4]

[1]Assistant professor, Dept of CSE , E.G.S.Pillay Engineering College ,Tamil Nadu, India
[2]UG student, Dept of CSE , E.G.S.Pillay Engineering College ,Tamil Nadu, India
[3]UG student, Dept of CSE, E.G.S.Pillay Engineering College ,Tamil Nadu, India
[4]UG student, Dept of CSE, E.G.S.Pillay Engineering College ,Tamil Nadu, India

---***---

Abstract: *In cloud secure personal data sharing is the important issues because it creates several securities and data confidentiality problem while accessing the cloud services. Many challenges present in personal data sharing such as data privacy protection, flexible data sharing, efficient authority delegation, computation efficiency optimization, are remaining toward achieving practical fine-grained access control in the Personal Information Sharing system. Personal records must be encrypted to protect privacy before outsourcing to the cloud. Aiming at solving the above challenges, here propose an efficient data sharing mechanism for Personal Data Sharing, which not only achieves data privacy, fine-grained access control and authority delegation simultaneously. Proposed methodology is presented to secure patients' MHR (Medical Health Record) in the healthcare cloud using the duplicate generation technique with a two server based computing facility. Duplicate server serves as a second gallery to contain duplicate MHR that appear to the attacker as if it is the original MHR. When user uploading a file on original server, corresponding duplicate file will be stored on another server. In this method, the decoy files are called when an attacker is detected as accessing the system, in our proposed methodology the duplicate files are retrieved from the beginning to ensure better security. In proposed approach RSA algorithm is implement to encrypt the medical record*

1.INTRODUCTION

Cloud computing is definitely a promising model for business computing. It's describes important infrastructure to have an up-and coming type of service provision which includes the benefit of reducing expense by sharing computing and storage sources. Currently, Cloud Computing is really a huge technology that is exceeding all of the earlier technologies of computing of this competitive and demanding Information technology industry.

Cloud computing is consistently growing and there are many main cloud computing providers including Amazon, Google, Microsoft, Yahoo and many others who are offering solutions including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a- Service and Infrastructure-as-a-Service (IaaS). In addition, considering the possibility to substantially minimizing expenses by optimization and also maximizing operating as well as economic effectiveness, cloud computing is an excellent technology. Furthermore, cloud computing can tremendously boost its cooperation, speed, and also range, thus empowering a totally worldwide computing model on the internet infrastructure. On top of that, the cloud computing has advantages in delivering additional scalable, fault tolerant services.

Cloud computing handles resource management in a better way since the user no longer needs to be responsible for identifying resources for storage. If a user wants to store more data they request it from the cloud provider and once they are finished they can either release the storage by simply stopping the use of it, or move the data to a long-term lower-cost storage resource. This further allows the user to effectively use more dynamic resources because they no longer need to concern themselves with storage and cost that accompany new and old resources.

II. EXISTING SYSTEM

The key assignment scheme (KAS) was first considered to achieve cryptographic access control. Designed a space-efficient key assignment scheme based on a binary tree and proposed a tree-based cryptographic access control mechanism. Existing system introduced the cryptographic hierarchical access control for dynamic structures and how to achieve access control in publicly verifiable outsourced computation based on KAS. This explored the relations between all security notions for hierarchical key assignment schemes. Proposed two hierarchical and shared key assignment schemes based on symmetric encryption and public key threshold broadcast encryption separately. Since the security classes in KAS should be set in advance, the access policy must follow the set security classes. Attribute based encryption (ABE) can achieve flexible access control over encrypted data. It was formalized two forms of ABE: key-policy ABE (KP-ABE) and ciphertext policy ABE (CP-ABE). In KP-ABE, the secret key is associated with an access policy, while an access policy is assigned to the ciphertext in CP-ABE. A user can decrypt a ciphertext if the set of attributes satisfies the access policy. Role Based Access Control (RBAC) provides efficient access control mechanism for each participant in EMR system. Here access controls are assigned and key sharing based on users role.

III.PROPOSED SYSTEM

Proposed system adopt two different public cloud servers to achieve secure outsourced computation, such as outsourced key generation/encryption/re-encryption key generation/ decryption. Actually, one public cloud server (e.g., public cloud 2) is sufficient for outsourced decryption, but not enough for other operations, because all the secret will be exposed to the unique cloud server. The access control model consists of five entities: private key generator (PKG), public cloud 1, public cloud 2, data owners and data consumers. Proxy Re-encryption is used to re-encrypt the data before sending it to the data consumer. Here propose an efficient data sharing mechanism for Personal Data Sharing, which not only achieves data privacy, fine-grained access control and authority delegation simultaneously, but also optimizes the computation efficiency and is suitable for resource constrained servers. Most of the data consumers are honest, while few of them are corrupt and will leakage their secret keys in the collusion. On the contrary, PKG and data owner are assumed to be fully trusted. Besides, public cloud 1 and public cloud 2 cannot collude with each other. The non-collusive assumption is reasonable, because the client can demand that two cloud servers cannot reveal users' information by contract. In proposed work, PR-ABE (Attribute Based Encryption with Proxy Re-encryption) technique implements to provide secure encryption of medical data. To improve the access control, here partial key sharing scheme will be implement. Using this, data owner can send partial secret key for the requested user. This approach overcomes the key guessing attack in data retrieval process. Proposed system will be implementing using PHP as front end and SQL is for back end process.

IV.MODULEDESCRIPTION

Data Acquisition

In this module crypto currency data has been acquired which consists of crypto coin rate data and its variations. Large number of data is present in the acquired datasets, which is efficiently used to monitor and predict crypto coin rates in past and as well as in future.

Preprocessing

Acquired datasets are preprocessed and results are attained with better efficiency using ANN algorithm. ANN deeply analyses the entire data and datasets that are acquired and preprocessing has been done as a step by step process. As a result an initial level conclusion can be attained.

Classification

Preprocessed data are classified based on its structure or based on the rate prediction. For classification SVM has been proposed which compares and classifies large number of values in datasets and data present in the entire process. Classification is a process that has been carried out throughout the process which ensures next step to segment data.

Segmentation

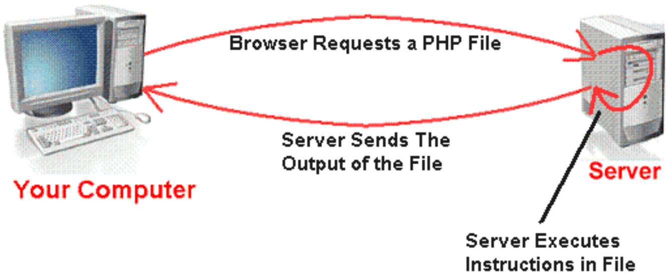
Classified data results are segmented ad gathered as a group of data and information that has been present in the large number of datasets.As a result of segmentation of data classified results that are similar are grouped and predictions has been done with quiet better efficiency.

Feature Extraction

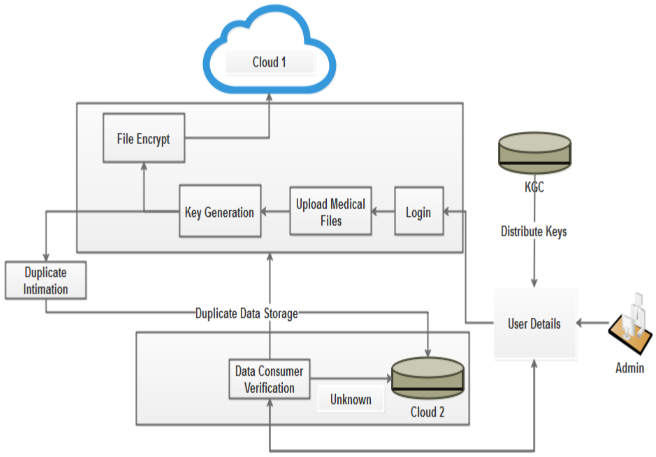
After segmentation an unique data from datasets are attained which are extracted from a series of data that are segmented.Whereasfeatureextractsprocesscompetesandprovidesaccurate extraction of crypto-coin data that are involved in the system. Due to extraction of large amount of data using ANNand SVM accuracy has been attained upto91%.

Performance Evaluation

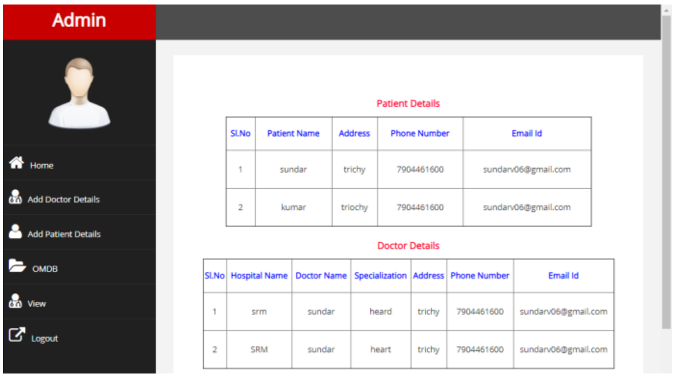
By performing entire operation and its special features the performance evaluation of crypto currency predictions are attained with better results which enhances the Complete system with higher order efficiency and attained results based on past and present are accurate which enormously enhances the procedures and attained results are maintained with better efficiency


Browser Requests a PHP File
Server Sends The Output of the File
Your Computer
Server
Server Executes Instructions in File

Accessing a PHP Page



Accessing an HTML Page

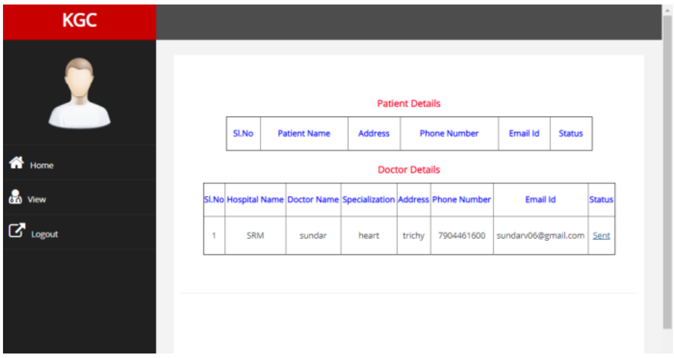


Patient Details

Sl.No	Patient Name	Address	Phone Number	Email Id
1	sundar	trichy	7904461600	sundarv06@gmail.com
2	kumar	triochy	7904461600	sundarv06@gmail.com

Doctor Details

Sl.No	Hospital Name	Doctor Name	Specialization	Address	Phone Number	Email Id
1	srm	sundar	heard	trichy	7904461600	sundarv06@gmail.com
2	SRM	sundar	heart	trichy	7904461600	sundarv06@gmail.com

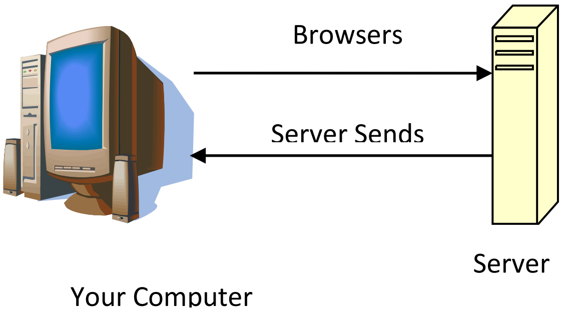


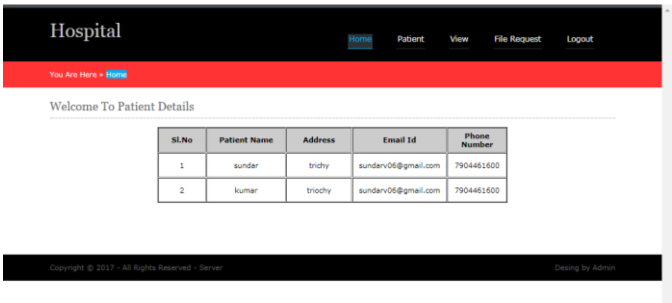
Patient Details

Sl.No	Patient Name	Address	Phone Number	Email Id	Status

Doctor Details

Sl.No	Hospital Name	Doctor Name	Specialization	Address	Phone Number	Email Id	Status
1	SRM	sundar	heart	trichy	7904461600	sundarv06@gmail.com	Sent

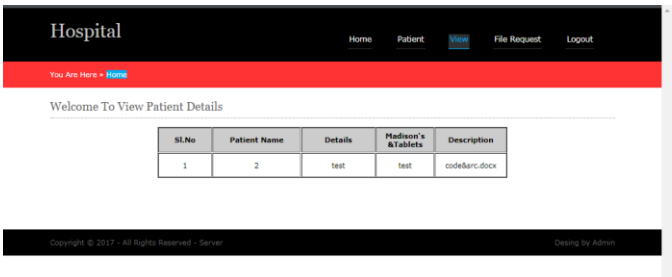




Welcome To Patient Details

Sl.No	Patient Name	Address	Email Id	Phone Number
1	sundar	trichy	sundarv06@gmail.com	7904461600
2	kumar	triochy	sundarv06@gmail.com	7904461600

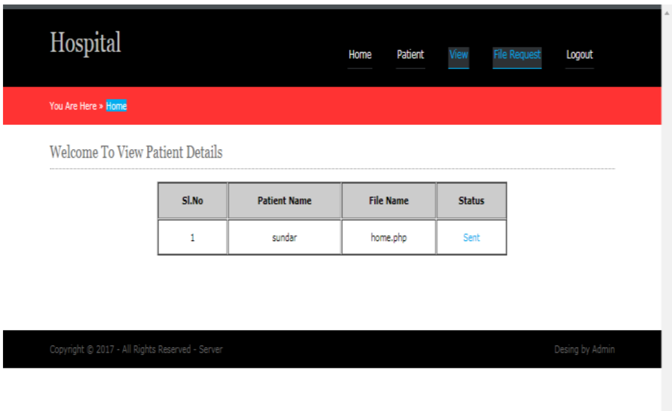
Copyright © 2017 - All Rights Reserved - Server Desing by Admin



Welcome To View Patient Details

Sl.No	Patient Name	Details	Madison's &Tablets	Description
1	2	test	test	code&src.docx

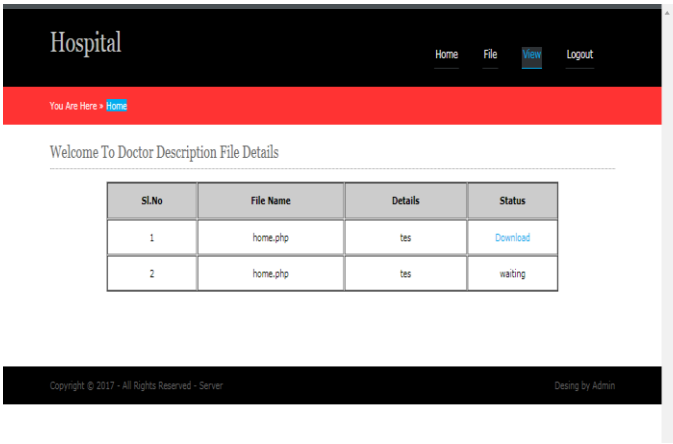
Copyright © 2017 - All Rights Reserved - Server Desing by Admin



Welcome To View Patient Details

Sl.No	Patient Name	File Name	Status
1	sundar	home.php	Sent

Copyright © 2017 - All Rights Reserved - Server Desing by Admin



Welcome To Doctor Description File Details

Sl.No	File Name	Details	Status
1	home.php	tes	Download
2	home.php	tes	waiting

V. Conclusions

In this project proposed a new mechanism is proposed to protect the healthcare data in the cloud. This system has a double layer protection in which the EHRs are stored in the cloud. Encryption/ Decryption will be done in one layer and in the other layer, duplicate files will be created and stored. To this end, two cloud storages are generated for different purpose. The original medical files are kept secretly in the cloud and the duplicate cloud is used as duplicate file storage. Therefore, instead of retrieving the duplicate medical files only when unauthorized access is discovered, the user, by default, accesses the duplicate files in cloud 2. The original server is only accessible by a user after verifying the authenticity of the user. Thus, the original multimedia data become more secure by setting the default value of the duplicate storage, while the original medical files are kept in a secure hidden cloud.

REFERENCES

[1] Tiwari, Deepnarayan, and G. R. Gangadharan. "SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation." International Journal of Communication Systems 31, no. 5 (2018): e3494.

[2] Zhang, Y., Zheng, D., Li, Q., Li, J., & Li, H. (2016). Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing. Security and Communication Networks, 9(16), 3688-3702.

[3] Alderman, James, Jason Crampton, and Naomi Farley. "A framework for the cryptographic enforcement of information flow policies." In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, pp. 143-154. 2017.

[4] Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 (2018): 1-12.

[5] Castiglione, Arcangelo, Alfredo De Santis, Barbara Masucci, Francesco Palmieri, Aniello Castiglione, Jin Li, and Xinyi Huang. "Hierarchical and shared access control." IEEE Transactions on Information Forensics and Security 11, no. 4 (2015): 850-865.

[6] Alderman, James, Christian Janson, Carlos Cid, and Jason Crampton. "Access control in publicly verifiable outsourced computation." In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp. 657-662. 2015.

[7] G. Rathi, Abinaya. M, Deepika. M, Kavyasri. T," Healthcare Data Security in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2015 Copyright to IJIRCCE 10.15680/ijircce.2015.0303089 1807

[8] R. Josephius Arunkumar 1 , R. Anbuselvi2, "Enhancement of Cloud Computing Security in Health Care Sector ", International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IMPACT FACTOR: 6.017 IJCSMC, Vol. 6, Issue. 8, August 2017, pg.23 – 31.

[9] Kushan Shah, Rui, and Ling Liu. " Security for Healthcare Data on Cloud." In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 268-275. IEEE, 2010.

[10] Raval, Divya, and Smita Jangale. "Cloud based Information Security and Privacy in Healthcare." International Journal of Computer Applications (IJCA), ISSN (2016): 0975-8887.