AN EFFICIENT ATTRIBUTE BASED CRYPTOGRAPHIC ALGORITHM FOR SECURING TRUSTWORTHY STORAGE AND AUDITING FOR HEALTHCARE BIG DATA IN CLOUD

J. K. Karthika, V. Maria Anu and A. Veeramuthu
Department of Information Technology, Sathyabama University, Chennai, India
E-Mail: karthikakanniah@gmail.com

ABSTRACT

A Medical Information System (MIS) is an emerging patient-driven strategy for medical data platform, which is for the most part circulated to outsource at an outsider, such as cloud suppliers. Be that as it may, there have been a lot of security worries as individual medicinal data should be uncovered to outsider servers and to unapproved parties. To guarantee the patients' entrance to their own Medical Records, it is a most commonplace strategy to scramble the Medical Records before outsourcing. Yet, concerns, dangers of security system, adaptability in key technique, dependable access and productive client renouncement, have dependably been the most imperative objectives toward accomplishing fine grained and cryptographically authorized information access privacy control. This paper, we proposed secured sharing of individual medical reports in cloud computing. Considering reliable cloud servers, to accomplish fine-grained access we perform Attribute Based Encryption (ABE) specifically Rijndael method encrypting the Medical Information System (MIS) data, so that the trustworthy is maintained. We ensure by auditing the process to prove the security. One of a kind from past works in safe keeping information outsourcing, we receive the various information proprietor situation, and split the clients in the Medical Information framework into a few security spaces that extraordinarily diminishes the key system basic for proprietors and clients. A higher positioning of patient trust and security is ensured in the meantime by abusing multi-power ABE. Our plan likewise outlines dynamic adjustment of access benefits or document properties, bolsters proficient on-interest client/characteristic repudiation and break-glass access under crisis situations. Sufficient of exploratory results are spoken to which demonstrate the security, adaptability, reliable and effectiveness of our proposed plan.

Keywords: attribute-based encryption, cloud suppliers, patient-driven strategy, medical information system, rijndael, fine-grained, cryptography.

INTRODUCTION

Huge information alludes to high volume, fast, and huge combination information resources that need a new sorts of taking care of enabling enhanced form decision making, understanding disclosure and methodology progression. Because of its high volume and many-sided quality, it gets to be hard to prepare Big data utilizing close by database administration devices. A powerful choice to store enormous information in cloud, as cloud has capacities of putting away huge information and preparing huge volume of client access demands in a productive way. While facilitating enormous information into the secure cloud, the information security turns into a noteworthy worry as a cloud servers can't be completely trusted by information proprietors.

Attribute Based encryption (ABE) has developed as a promising method to guarantee the end-to-end information security in distributed storage framework. It permits information proprietors to characterize access strategies and encode the information under the approaches, such that just clients whose qualities fulfilling these entrance arrangements can decode the information. Whenever more associations and endeavors outsource information into the cloud, the arrangement overhauling turns into a critical issue as information access strategies might be changed powerfully and every now and again by information proprietors. Be that as it may, this arrangement upgrading issue was not measured in presented attribute based access control plans.

The policy upgrading is a troublesome issue in the attribute-based access control frameworks, in light of the fact that once the information proprietor outsourced information into the cloud, it would not keep a duplicate in neighborhood frameworks. At the point when the information proprietor needs to change the entrance approach, it needs to exchange the information back to the neighborhood site from the cloud, re-encode the information under the new get to arrangement, and after that move it to the cloud server. Thusly, it brings about a high correspondence overhead and substantial calculation trouble on information proprietors. This inspires us to build up another technique to contract out the errand of strategy overhauling to the cloud server.

As more insightful information is shared and put away by outsider destinations on the Internet, there will be a need to scramble information put away at these locales. We add to another cryptography system for the fine grained secured sharing of scrambled information that we call key policy based attribute encryption. In cryptography system, figure writings are marked with sets of qualities and the private keys are connected with access control structures that control which figure messages a client can unscramble. Given the assortment, sum, and significance of data put away at these locales, there is reason for worry that individual information will be traded off. This stress is raised by the surge in late assaults and lawful weight confronted by such administrations.

RELATED WORK

The cloud server is interested regarding the put away information and messages it got amid the administrations Attribute-based encryption has risen as a hopeful procedure to guarantee the back-to-back information security in distributed storage framework [1]. The proposed systems are proficient and secure technique that permits information proprietor to ensure that the cloud server was upgraded the Cipher messages accurately or not. The examination demonstrates that the approach upgrading outsourcing plan is right, finished, secure and effective. A proficient system was created to outsource the approach upgrading to the cloud server, which can fulfill every one of the necessities. Here additionally, we proposed the expressive attribute based access control plan for huge information in the secured cloud, and composed strategy overhauling calculations for various sorts of access approaches. Besides, the proposed a system which empowers information proprietors to check the accuracy of the figure content overhauling. The investigation additionally made with the plan as far as rightness, fulfillment, security and execution.

Decentralized key approach ABE [2] where every power can issue the mystery key to client freely with no collaboration of a focal power. It implies that that there is no compelling reason to trust on to the focal power because of this regardless of the fact that various powers are tainted they can't gather the client’s traits by following clients GID. In decentralized key-characteristic based encryption both the client mystery key and the figure content are mark with set of various property. Message can be encode under arrangement of characteristic so in the event that anybody need decode the figure message the collector must acquire information just when there is match between his mystery key and trait recorded in the figure content. In multi power ABE mystery key of various clients from various powers must be attached to his worldwide identifier (GID). The proposed decentralized key strategy plan to ensure the clients protection in this plan every power can issue emit key to clients independently without having any thought of his GID.

The rising cloud innovations, because of their different exceptional and appealing properties, are quickly being embraced all through the IT business. It has officially drawn enormous consideration, and its advantages have pulled in number of clients to outsource their nearby server farms to remote secured cloud servers regardless of its notoriety, in any case, distributed computing has elevate a scope of critical security system and protection concerns which prevent its reception in delicate situations. To guarantee the client control over the entrance to their own information, it is a promising technique to encode the information before outsourcing on the cloud. Fundamental issues, for example, security, versatility in key administration, adaptable access and productive client renouncement which are the most critical contemplations for increasing fine grained and cryptographically utilized information access control [3].

Cloud computing, as a developing processing worldview, empowers clients to slightly store their information into the cloud in order to appreciate versatile administrations on-interest. Be that as it may, permitting cloud service providers (CSPs), which are not in the same expected areas as big business clients, to deal with private information, might raise potential security and protection issues. To keep the delicate client information classified against un-trusted CSPs, a characteristic route is to apply cryptographic methodologies, by uncovering decoding keys just too approved clients. Another plan helps undertakings to proficiently share private information on cloud servers. We accomplish this objective by first consolidating the various hierarchical identity-based encryptions (HIBE) framework [4] and the cipher text policy attribute-based encryption (CP-ABE) framework, and afterward making an execution expressivity tradeoff, at last applying intermediary re-encryption and languid re-encryption to our plan.

Symmetric key calculation utilizes same key for both encryption and decoding. The pillar of this is to propose another decentralized access control plan [5] for secure information stockpiling in mists that backings unknown verification. The proposed hiding the access policy to the client utilizing question based calculation and utilizing SHA calculation we are concealing the client’s characteristics. Dispersed access control of information put away in cloud so that just approved clients with legitimate traits can get to them. The validation of clients who store and adjust their information on the cloud and the entrance control and verification are both arrangement safe, implying that no two clients can connive and get to information or verify themselves, in the event that they are separately not approved. The identity of the client is shielded from the cloud amid validation. By plan a client can make a document and store it safely in the cloud.

The security and protection is the fixed and enormous testing problem in huge information storage. There are numerous approaches to bargain information on account of inadequate authentication, authorization, and audit (AAA) controls, for example, erasure or modification of records without a reinforcement of the first substance. The proposed formal analysis system called full grained updates [6] and it incorporates the effective looking for downloading the transferred record furthermore concentrates on outlining the inspecting convention to enhance the server-side security for the proficient information privacy and information accessibility.

The healthcare services checking framework ought to be viable and solid such that it accurately underpins the cloud-helped information recuperation, while ensuring both the private information tests and the substance of the recouped information from the cloud. Regardless of the expanding prevalence, how to successfully prepare the continually developing medicinal services information and all the while secure information protection, while keeping up low overhead at sensors, stays testing. To address the issue, we propose a privacy-aware cloud-helped medicinal services observing framework [7] by means of compressive detecting, which coordinates diverse area strategies. The entire procedure is protection guaranteed such that data from neither the specimens nor the basic information substance will be uncovered.

Cloud storage administration permits information proprietor to have their information in the cloud and through which give the information access to the clients. Since the cloud server is not reliable in the distributed storage framework, we can't depend on the server to direct information access control. In this paper, we outline an entrance control structure in distributed storage frameworks and propose a fine-grained access control plan in light of Cipher text Policy Attribute-based Encryption (CP-ABE) approach [8]. It is a standout amongst the most suitable advancements for information access control in distributed storage frameworks, since it gives the information proprietor more straightforward control on the access approaches and the arrangement checking happens inside of the cryptography. The information proprietor is responsible for characterizing and implementing the entrance approach without depending on any helper access control by the server.

Information access control is a powerful approach to guarantee the information security in the cloud. Be that as it may, because of information outsourcing and un-trusted cloud servers, the information access control turns into a testing issue in distributed storage frameworks. The proposed DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), a successful and secure information access control plan with effective decoding and renouncement [9]. This characteristic denial system brings about less correspondence cost and less calculation expense of the repudiation, where just those segments connected with the disavowed trait in the mystery keys and the figure content should be overhauled.

As Cloud Computing gets to be predominant, more delicate data are being concentrated into the cloud, for example, messages, personal health records, organization fund information, and government reports, and so forth. The way that information proprietors and cloud server are no more in the same trusted space might put the outsourced decoded information at danger. To secure information protection, sensitive cloud information must be encoded before outsourced to the business open cloud, which makes successful information use benefit an exceptionally difficult errand. Positioned seek enormously improves framework ease of use by empowering item importance positioning as opposed to sending undifferentiated results, and further guarantees the record recovery exactness [10].

To ensure clients private information included in the calculations then turns into a noteworthy security concern. We define the issue in the calculation outsourcing model for safely explaining solving large-scale systems of LE by means of iterative systems, and give the protected component plan which satisfies input/output security, swindling versatility, and productivity [11]. This is particularly suitable for the application situation, where computational compelled clients need to safely saddle the cloud for taking care of extensive scale issues.

The coming of cloud computing, information proprietors are propelled to outsource their complex management information administration frameworks from nearby destinations to the business open cloud for awesome adaptability and financial investment funds. Be that as it may, for ensuring information security, sensitive information must be scrambled before outsourcing, which obsoletes customary information usage in light of plaintext catchphrase seek. The testing issue of security saving multi-keyword ranked search over encrypted cloud information (MRSE).We build up an arrangement of strict protection prerequisites for such a safe cloud information use framework [12].

Clients can remotely store their information and appreciate the on-interest amazing applications and administrations from a mutual pool of configurable figuring assets, without the weight of neighborhood information stockpiling and upkeep. Empowering open auditability for distributed storage is of basic significance with the goal that clients can turn to a third party auditor (TPA) to check the uprightness of outsourced information and be straightforward [13]. Cloud computing makes these points of interest more engaging than any other time in recent memory, it additionally brings new and testing security dangers towards clients' outsourced information. Since cloud service providers (CSP) are independent authoritative elements, information outsourcing is really surrendering client's definitive control over the destiny of their information. Considering TPA might simultaneously handle various review sessions from various clients for their outsourced information records.

Client protection has been a noteworthy worry against the across the board reception of the cloud innovation. We recognize the significance and difficulties of planning security guaranteed, adaptable and for all intents and purposes productive quest components for outsourced cloud information administrations [14]. Late research propels in this field are studied, which propose that accomplishing semantically rich, usable and effective hunt on encoded information is conceivable without giving up much protection ensure.

PROPOSED METHODOLOGY

a) Problem description

To protect the personal medical data on the third party software like cloud is not trust worthy and many more techniques / methods are available to secure the information in the cloud but, still data security not yet fulfilled, so it need a powerful mechanism for securing the sensitive information in the cloud.

b) System architecture

With a specific end goal to secure the individual medicinal information put away on a semi-trusted server, we embrace attribute-based encryption (ABE) particularly as a fundamental encryption primitive. Medical Record proprietor herself ought to choose how to encode her documents and to permit which set of clients to get access to every record.

We propose a novel plan that empowering productive access control with approach redesigning for huge information in the cloud. We concentrate on building up an outsourced strategy upgrading technique for ABE frameworks. Our strategy can avoid the transmission of encoded information and minimize the calculation work of information proprietors, by making utilization of the beforehand scrambled information with old access plans.

Medicinal Records document ought to just be accessible to the clients who are given the relating decoding key, while stay private to whatever is left of clients. We propose a productive and secure technique that permits information proprietor to check whether the cloud server has overhauled the figure messages accurately. Besides, the patient should dependably hold the privilege to concede, as well as repudiate access benefits when they feel it is essential. We develop an expressive and proficient information access control plan for enormous information, which empowers effective element arrangement overhauling. Unique in relation to the single information proprietor situation considered in the greater part of the current works, in a Medical Information framework, there are various proprietors who might encode as per their own particular manners, potentially utilizing diverse arrangements of cryptographic keys. Giving every client a chance to obtain keys from each proprietor who's Medical Record she needs to peruse would confine the availability since patients are not generally online.

The system consists of following components which are profile development, MIS manipulation, Multi-Authority implementation, Emergency Care Implementation, and auditing which are shown in Figure-1.

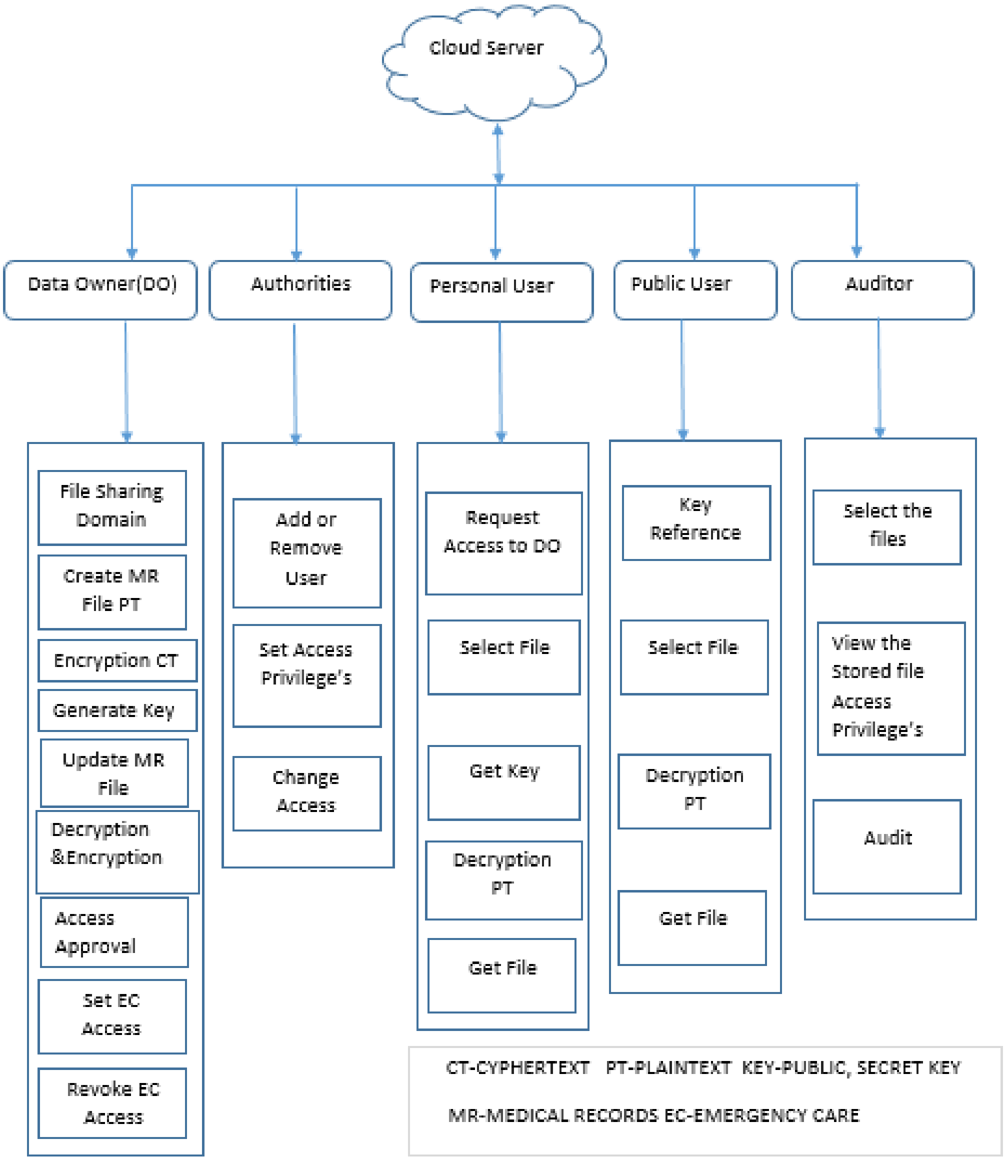


Figure-1. System architecture.

i) Profile development

The profile creation is the main Authority of Scalable and Secure Sharing of Medical Information System. The Core Development is responsible of registering MIS owners and MIS users and theirs Login processes. It is also responsible for Profile maintenance of MIS owners and MIS users. Registering and removing accounts of MIS owners and MIS users in our framework. After complete user registration the verification link will be send to the registered email id and get back to the link user can be verified successfully. To enable login and logout processes for MIS owners and MIS users accordingly. In login model we have security specialty, it is a two factor authentication type. It sent OTP to registered phone number. User has to enter the OTP each of logins for access user account more securely. The MIS owners, Personal users, Public users, Authorities and Auditors can maintain their profile. All users can modify their profile such as edit, show or remove their profiles.

ii) MIS Manipulation

The MIS proprietor ought to choose how to encode her records and to permit which set of clients to get access to every document. We allude to the two classifications of clients as individual and expert clients, separately. With a specific end goal to secure the individual restorative information put away on a semi-trusted server, we embrace attribute-based encryption (ABE) particularly Rijndael strategy as the primary encryption primitive. Utilizing ABE, access benefits are communicated in light of the traits of clients or information, which empowers a patient to specifically share her Medical Records among an arrangement of clients by scrambling the document under an arrangement of characteristics, without any knowledge of the clients.

MIS owners can able to create theirs MR file and can set its properties such as type, category with their own desire. They can encrypt any number of records and store it in our framework. The MIS owners can maintain their records. They can able to update records with latest changes. They can able to produce keys for decrypt records and distribute them for personal domain users.

They can set access privileges to their records and set permissions for accessing records. They can reset access privileges to their records and can maintain record history. Utilizing ABE, access approaches are communicated taking into account the qualities of clients or information, which empowers a patient to specifically share her Medical Records among an arrangement of clients by encoding the document under an arrangement of properties that can capable for element change of access plans.

iii) Multi-Authority implementation

To utilize multi authority ABE (MA-ABE) to enhance the security and maintain a strategic distance from key escrow issue. Every attribute authority (AA) in it administers a disjoint subset of client part properties, while none of only them can control the security of the entire framework. We propose components for key conveyance and encryption so that MIS proprietors can indicate customized fine-grained part based access strategies amid document encryption.

Giving every client a chance to obtain keys from each proprietor whose Medical records she needs to peruse would restrain the availability since patients are not generally on the web. The MA s, such as, the American Medical Association (AMA), the American Board of Medical Specialties (ABMS), and the American Hospital Association (AHA) and Insurance Domains and Medical Companies are need to request the MIS owners for obtaining decryption keys for reading the Medical Record file. Public users have to obtain their secret key from multiple AAs by request them. The MA check the user's credential and may provide keys to them. Using the keys the user can access Medical Record file.

iv) Emergency-Care implementation

The MIS owner might dependably hold the privilege to concede, as well as revoke access benefits when they feel it is essential. The Emergency Care (EC) responsible for provide break-glass key, for access Medical Records file due to the emergency. The emergency key set by the MIS owner while encrypting the Medical Records file.

At the point when a emergency was happens, the customary access plans might never again be appropriate. To handle this circumstance, break-glass access is expected to achieve the casualty's Medical Records. In our structure, every proprietors of MIS get to right is likewise assigned to a emergency care. To keep from abuse of break-glass choice, the crisis staff needs to contact the EC to confirm her personality and the crisis period, and accomplish brief read keys. After the emergency is over, the MIS proprietor can renounce the new get to through the EC and the new break-glass key will be made.

v) Auditing

Separate Login initiative for Auditing purpose to ensure trustworthy of the services offered in MIS. The process Audit the file system by viewing its privilege's and encryption process and how secure system handle the Information. And check to that audit is successful.

c) Algorithm

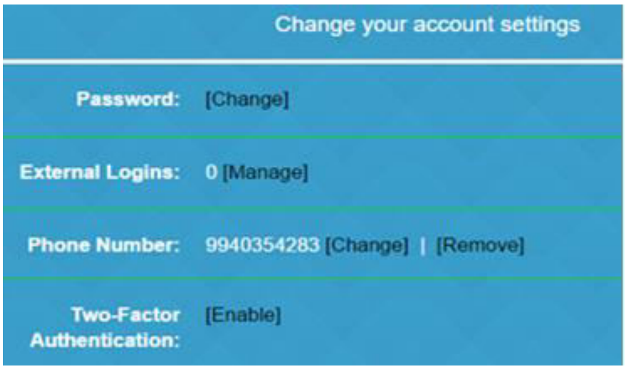
The particular TPA initial retrieves the actual report point t levels. According to the process described, the actual TPA certifies the actual signature as well as quits simply by emitting FALSE if the confirmation is not able. Otherwise, the actual TPA recovers identify. Now comes to actual center section of the auditing procedure as well as make the battle communication with the examiner, the actual TPA selects a hit-or-miss element from the subset. For each element i ∈ I, the actual TPA likewise decides a hit-or-miss benefit. The particular communication challenge specifies the actual jobs in the obstruct that are necessary to become looked at. The particular TPA transmits challenge communication towards server. About obtaining challenge communication, the actual server goes protection technique to make a response evidence of files storage devices correctness. Specifically, the actual server decides a hit-or-miss element r ← Zp, as well as calculates R = e(u, v)r ∈ GT. Let μ′ denote the actual linear mix of experienced obstructs chosen within challenge communication. To help sightless μ′ having r, the actual server computes: μ = r+μ′ mod p, wherever r= h(R) ∈ Zp which are given in Algorithm 1 for public auditing mode.

```
Input: Auditing information
Output: Challenge message generated
Begin
        Recover file tag t, check the identity and exit if fail.
        Produce the arbitrary challenge c
                $c = \{(i, v_i)\}i \in I$
        Calculate the $\gamma = h(R)$, then check $\{\mu, \sigma, R\}$ using the given formula,
                $R = e\left(\left(\prod H(W_i)\, v_i\right) u, v\right)$
        Calculate $\mu' = \sum \sum_{i \in} I\, v_i\, m_i$ and $\sigma = \prod_{i \in I} \sigma_i^{vi}$
        Arbitrarily pick r←$Z_p$ and compute $R = e(u, v)^r$ and $\gamma = h(R)$
        Calculate $\mu = r + \gamma\mu'\, modulus\ p$
End
```

Algorithm 1: Auditing mode

EXPERIMENTAL RESULTS AND DISCUSSIONS

In our medical information system was highly secured from miss uses of unauthorized persons which is shown in Figure-2 enabling the two factor authentication your account becomes more securable so that you get a verification code that indicate the users can manage their own accounts and Figure-3 verifying the OTP code each time when you access the medical information system.



Change your account settings

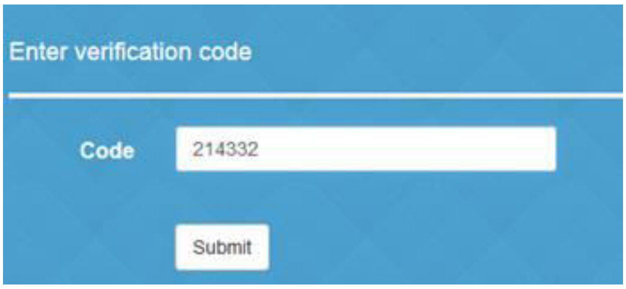
Password: [Change]

External Logins: 0 [Manage]

Phone Number: 9940354283 [Change] | [Remove]

Two-Factor Authentication: [Enable]

Figure-2. Account management.

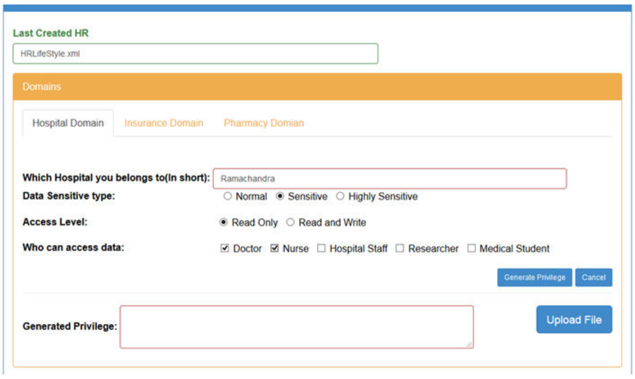


Enter verification code

Code: 214332

Figure-3. Verify OTP authentication code.

The access control privileges for each file provided for the every user before encryption and then it is uploaded in the system which is shown in Figure-4. So, the file can be accessed only by them in secured manner. When an emergency occur user in EC will request for access to the data owner for the specific person, the data owner immediately process and update the form and provide the keys for accessing the file which is shown in Figure-5. Finally, the auditing process is successful for each file system in the medical information system which is shown in Figure-6.



Last Created HR: HRLifeStyle.xml

Domains

Hospital Domain | Insurance Domain | Pharmacy Domian

Which Hospital you belongs to(In short): Ramachandra

Data Sensitive type: ○ Normal ● Sensitive ○ Highly Sensitive

Access Level: ● Read Only ○ Read and Write

Who can access data: ☑ Doctor ☑ Nurse □ Hospital Staff □ Researcher □ Medical Student

Generated Privilege:

Figure-4. Access control privileges.

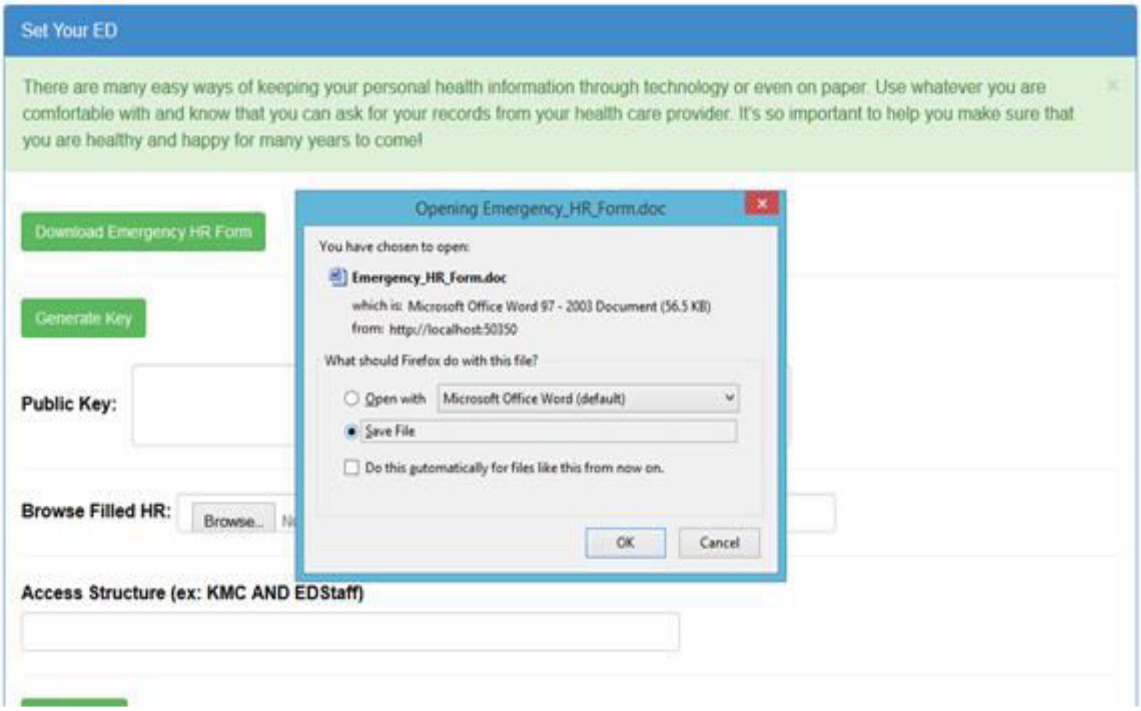
PERFORMANCE ANALYSIS

In Table-1 demonstrates the examination among our modified Rijndael and three existing algorithms, which are all taking into account the cipher content re-encryption to accomplish the trait disavowal. We direct the examination as far as the backing of multi-power, the calculation productivity (encryption on the proprietor and decoding on the client), the repudiation correspondence cost, the denial security, the disavowal implementer and the figure content updater/re-encryptor. From the given table, we can observe that modified Rijndael causes fewer calculation rates for the unscrambling on the client and less correspondence cost for the denial. In modified Rijndael, the quality repudiation is controlled and upheld by every authority freely; however the cipher text writings are redesigned by the semi-trusted server, which is enormously decrease the workload on the proprietor. For the given security of attribute repudiation, modified Rijndael can accomplish both forward security and in reverse security efficiently.

Table-1. Performance comparision of various algorithms.

Algorithms	Authorities	Computation	
		Encrypt	Decrypt
ABE	Single	$O(t_c + \log n_u)$	$O(t_u)$
DACC	Multiple	$O(t_c)$	$O(t_u)$
DAC-MACS	Multiple	$O(t_c)$	$O(t_1)$
Modified Rijndael	Multiple	$O(t_{c-1})$	$O(t_1)$

We direct the execution investigation between our modified Rijndael and the DACMACS algorithm under the measurements of computation cost, communication cost, and storage overhead. We reproduce the calculation time of encryption, decoding and cipher-text content re-encryption/redesign in both our modified Rijndael and DAC-MACS plan. The communication cost of the ordinary access control is just about the same between our adjusted Rijndael and DAC-MACS plan. The storage overhead is a standout amongst the most noteworthy problem of the access control plan in cloud storage frameworks. Our method will outperform all the cases of encryption and decryption efficiently.



There are many easy ways of keeping your personal health information through technology or even on paper. Use whatever you are comfortable with and know that you can ask for your records from your health care provider. It's so important to help you make sure that you are healthy and happy for many years to come!

You have chosen to open:

Emergency_HR_Form.doc

which is: Microsoft Office Word 97 - 2003 Document (56.5 KB)

from: http://localhost:50350

What should Firefox do with this file?

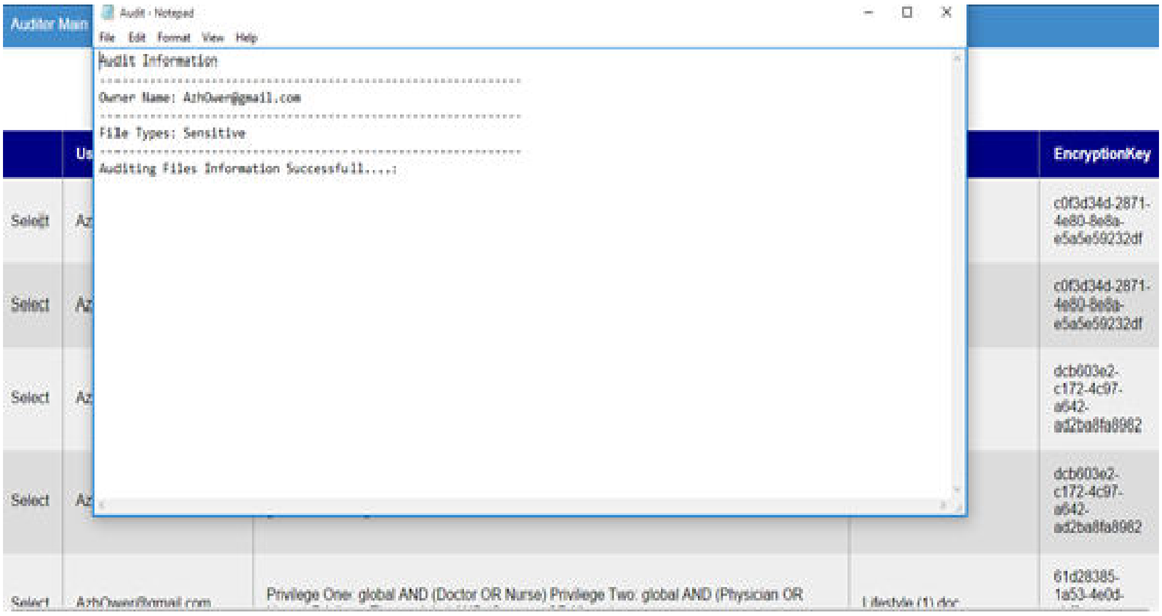
○ Open with Microsoft Office Word (default)

● Save File

□ Do this automatically for files like this from now on.

Access Structure (ex: KMC AND EDStaff)

Figure-5. Generate key for emergency form.



```
Audit Information
-----------------------------------------------------------------
Owner Name: AzhOwer@gmail.com
-----------------------------------------------------------------
File Types: Sensitive
-----------------------------------------------------------------
Auditing Files Information Successfull....:
```

c0f3d34d-2871-4e80-8e8a-e5a5e59232df

c0f3d34d-2871-4e80-8e8a-e5a5e59232df

dcb603e2-c172-4c97-a642-ad2ba8fa8982

dcb603e2-c172-4c97-a642-ad2ba8fa8982

Select AzhOwer@gmail.com Privilege One: global AND (Doctor OR Nurse) Privilege Two: global AND (Physician OR Lifestyle (1).doc 61d28385-1a53-4e0d-

Figure-6. Auditing file system.

CONCLUSIONS

In this paper, considering dependable cloud servers, to get fine-grained access we use Attribute-based Encryption (ABE) particularly Rijndael methodology to encode and decode the Medical Information System (MIS) information, so that the security is kept up. A high level of patient protection is ensured at the same time by using multi-power ABE. Our plan additionally empowers dynamic change of access arrangements or record properties, underpins productive on-interest client/ characteristic repudiation and break-glass access under crisis situations. By means of providing Auditing system we can prove the trustworthy of our System. Broad diagnostic and exploratory results are introduced which demonstrate the security, adaptability, reliable and productivity of our proposed method. In future the process can be converted to mobile centric application and also can handle Auditing by using Hash values. Thus our system ensures the trustworthy of the Medical Information System.

REFERENCES

[1] Kan Yang, Xiaohua Jia, and Kui Ren. 2015. Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud. IEEE Transactions on Parallel and Distributed Systems. 26(12): 3461-3470.

[2] Kishor B.Badade, Dr.S.S. Lomte, R.A.Auti. 2015. Protecting User Privacy by Using Decentralized Key-Policy Attribute-Based Encryption. International Journal of Computer Science and Information Technologies. 6: 880-888.

[3] Hulawale Kalyani, Paikrao Rahul, Pawar Ambika. 2014. Achieve Fine Grained Data Access Control in Cloud Computing using KP-ABE along-with Lazy and Proxy Re-encryption. International Journal of Emerging Technology and Advanced Engineering. 4(2): 457-461.

[4] Guojun Wang, Qin Liu, Jie Wu. 2010. Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services. ACM 978-1-4503-0244-9/10/10.

[5] S Sankareswari, S.Hemanth. 2014. Attribute Based Encryption with Privacy Preserving using Asymmetric Key in Cloud Computing. International Journal of Computer Science and Information Technologies. 5: 6792-6795.

[6] G. Janani, C.Kavitha. 2015. Public Auditing of Dynamic Big Data Storage with Efficient High Memory Utilization and ECC Algorithm. International Journal of Innovative Research in Computer and Communication Engineering. 3(3): 2150-2156.

[7] Cong Wang, Bingsheng Zhang, Kui Ren, Janet M. Roveda, Chang Wen Chen and Zhen Xu. 2014. A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing. IEEE.

[8] K. Yang and X. Jia and K. Ren. 2013. Attribute-based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems. Proc. of the 8th ACM Symposium on Information, Computer, and Communications Security (ASIACCS).

[9] K. Yang, X. Jia and K. Ren. 2013. DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems. Proc. of IEEE International Conference on Computer Communications (INFOCOM'13).

[10] C. Wang and N. Cao and K. Ren and W. Lou. 2012. Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data. IEEE Transactions on Parallel and Distributed Systems.

[11] C. Wang, K. Ren, J. Wang and K. Urs. 2013. Harnessing the Cloud for Securely Outsourcing Large-scale Systems of Linear Equations. IEEE Transactions on Parallel and Distributed Systems. pp. 1-14.

[12] N. Cao, C. Wang, M. Li, K. Ren and W. Lou. 2013. Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems.

[13] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou. 2013. Privacy-preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers. pp. 1-12.

[14] M. Li, S. Yu, K. Ren, W. Lou and T. Hou. 2013. Toward Privacy-Assured and Searchable Cloud Data Storage Services. IEEE Network.