ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cloud-Assisted Mobile-Access of Health Data With Privacy and Audit Ability

Nallabothula Aruna
M.Tech Student,
Department of CSE,
KLR College of Engineering and Technology.

R.Adinarayana
Assistant Professor,
Department of CSE,
KLR College of Engineering and Technology.

S.S.Madhavi
Associate Professor & HOD,
Department of CSE,
KLR College of Engineering and Technology.

Abstract:

Monitoring and advising patients via mobile health care system is the current trend in medical field that acts as a life saver due to its availability at anytime and anywhere. This e-healthcare system requires patient's private data to be available at cloud, outsourced data storage. This situation faces privacy issues. Hence the proposed approach focus on providing a private cloud for mobile users to ensure less cost, effective and secure storage. The data keyed in the mobile is transferred to private cloud, which in turn is processed and again transferred to public cloud. The sensitivity of the outsourced cloud data is maintained using Attribute based Encryption technique which restricts data access based on encrypt/decrypt of data with its access structures. The data privacy is ensured by PRF based key management and secure indexing methodologies. Personal Health records view ability access control to the actual data owner is the core idea of this project. The project segregates the access users in to Public Domain Users and Private Domain users.

Keywords:

e-Health, Privacy, Auditability, Access Control.

1.Introduction:

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or"autonomic computing" is to broaden horizons across organizational boundaries. Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption."

1.1 Cloud Computing Models:

Cloud Providers offer services that can be grouped into three categories.

A. Software as a Service (SaaS):

In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers" side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Sales force, Microsoft, Zoho etc.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

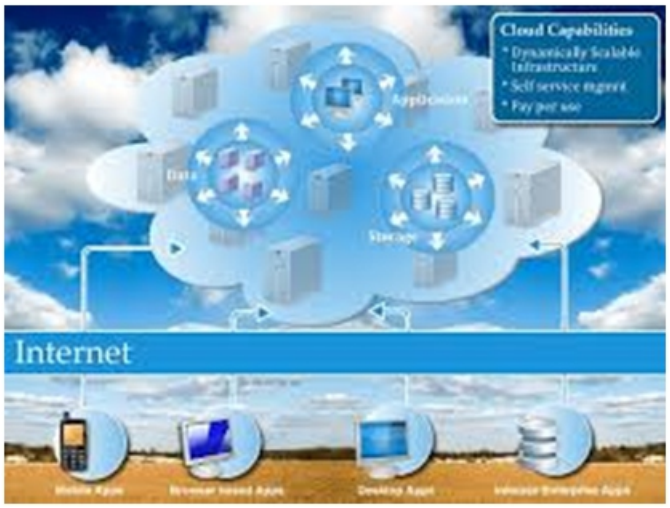


Figure 1: Overview of Cloud Computing

B. Platform as a Service (PaaS):

Here, a layer of software or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc. are some of the popular PaaS examples.

C. Infrastructure as a Service (Iaas):

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

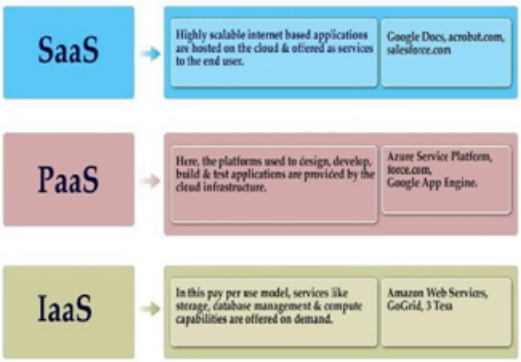


Figure 2: Cloud Models

1.2 Public, Private and Hybrid Clouds:

Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.

Public Cloud:

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private Cloud:

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud:

A.On-premise Private Cloud:

On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

B.Externally hosted Private Cloud:

This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Hybrid Cloud:

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

1.3 Cloud Computing Challenges:

Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. Some common challenges are:

Data Protection:

Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

Data Recovery and Availability:

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support

•Appropriate clustering and Fail over
•Data Replication
•System monitoring (Transactions monitoring, logs monitoring and others)
•Maintenance (Runtime Governance)
•Disaster recovery
•Capacity and performance management

If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

Management Capabilities:

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like Auto-scaling for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

Regulatory and Compliance Restrictions:

In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

1.4 Health Care Information System:

The e-healthcare system needs patient's non-public knowledge to be accessible at cloud, associate degree outsourced knowledge storage. Hence the planned approach specialise in providing a non-public cloud for mobile users to make sure less price, effective and secure storage. The info keyed within the mobile is transferred to non-public cloud that successively is processed and once more transferred to public cloud. The data privacy is ensured by PRF based mostly key management and secure compartmentalisation methodologies. Personal Health records read ability access management to the particular knowledge owner is that the core plan of this project. The project segregates the access users in to property right Users and personal Domain users.

2. Related Work:

The survey contains various details about cloud security, methods of encryption and decryption techniques, several issues and parameters were considered. According to A Rule-Based Framework for Role-Based Delegation and Revocation studied by Longhua Zhang et al.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[9] the protection of data privacy, sensitive data has to be Rule-Based Framework before outsourcing, which makes effective data utilization a very challenging task. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. Ranked searchable symmetric encryption gives an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). But this approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. The Rule-Based Framework cloud data have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic. HCPP - Healthcare system for Patient Privacy is based on cryptographic constructions and existing wireless network infrastructures studied by Jinyuan Sun et al. [3] specify the techniques that are provably secure.

The techniques provide provable secrecy for encryption, in the sense that the untreated server cannot learn anything about the plaintext given only the cipher text. The techniques provide controlled searching, so that the non trusted server cannot search for a word without the user's authorization. But, the drawbacks are it searches encrypted data without an index .This performs normal searchable scan method using pseudorandom generator for search techniques. A Security Architecture for Computational Grids by Ian Foster et al. [10] says that for protecting data grid, sensitive data has to be encrypted before outsourcing of grid, which obsoletes traditional data utilization based on plaintext keyword search.

There are large number of data grid and documents in cloud, it is crucial for the search service to allow multi-keyword grid and provide result similarity ranking to meet the effective data retrieval need. The merits are Coordinate matching-as many matches as possible. Inner product similarity -The number of grid keywords appearing in a document. The number of grid keywords appearing in the document to quantify the similarity of that document to the query. But this paper faces with these drawbacks. The Multi-keyword Ranked search algorithm provides multi keyword to search over cloud data provides numerous data results.

The selection criterion of required document search becomes highly difficult. The relevance between the search documents may differ from one another. An Identity-based Security System for User Privacy in Vehicular Ad Hoc Networks by Jinyuan Sun et al. [6] Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. To edit distance quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads.

The advantages of this work are to build the fuzzy keyword sets that incorporate not only the exact keywords but also the ones differing slightly due to minor typos, format inconsistencies, etc. Designing an efficient and secure searching approach for file retrieval based on the resulted fuzzy keyword sets. Yet this proposal faces with the problems of Search ranking that sorts the searching results according to the relevance criteria but even it produces too many search results. The extraction of exact file takes much time to solve the user needs. PracticalTechniques for Searches on Encrypted Data by Dawn Xiaodong Song et al. [5] explains about the data blocks and the file encryption happening in the system. One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud.

As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. In this paper they provide a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA). This scheme ensures that the storage at the client side is minimal which will be beneficial for thin clients. The advantages of this paper are the data will be proofed based on the Service Level agreement specified by the stack holders. Most of the data were diversified as blocks of encrypted data bits. But the drawbacks in this proposal are Practical implementation of this project is not focused clearly. Author provides a suggestion on the encryption process without any explanation on the steps to follow to incorporate this functionality in the cloud server.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3. Proposed Scheme:

The proposed approach stores patient information in the form of document and it is highly secured, as the document is stored in an encrypted format. Patient has the ability to set clear segregation of document access rights for his sensitive information. Documents can be searched using a keyword from the document.

Pattern classifiers are in place to ensure high security for the documents. In case of Emergency, patient's data are accessed fully and an automatic SMS will be sent to the patient indicating the user's data is accessed by the unsolicited person. Using optical character Recognition to store the patient details it makes more secure.

Merits of the Proposed System:

•The storage overhead is linear with the number of outsourced healthcare data files, while the communication overhead can be considered as constant per data request.
•The result indicates that the proposed scheme is efficient as well as scalable.

4. Architectural Design:

The major part of the project development sector considers and fully survey all the required needs for developing the project. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them.

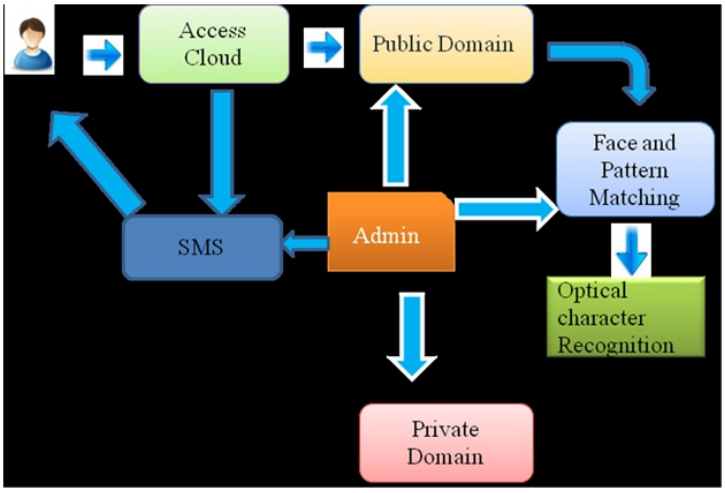


Figure 3: System Architecture

The above architecture diagram shows that the user (Patient, Acquaintances, Doctors, Other) logins into the cloud server and how information is provided to the relevant user. In case of illegal access an SMS alert is send to the user i.e., Patient and their acquaintances.

5. Methodology:

Following are the most frequently used project management Methodologies in the project management practice:

1.User Registration
2.Private Domain Specification
3.Public Domain Specification
4.Admin approval
5.Face Recognition
6.Optical character recognition
7. Performance evaluation

5.1.User Registration:

In this module, the user is the act of confirming the truth of an attribute of a datum or entity. This module includes the attributes define options like the user details will be uploaded. Option of user to add the data or the data will be uploaded by the Admin in the system. We are using DES Algorithm to encrypt the user's details in the system.

5.2 Private Domain Specification:

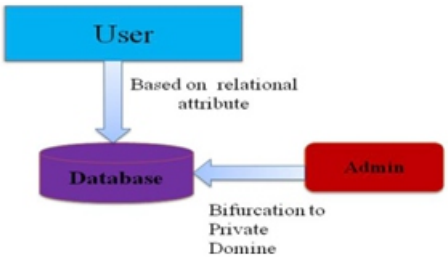
Specifying the data level of access to the user who are bit of relational in nature to the user were involved in this module.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The user is permitted to provide the level of access given to the relations (Based on the relational attribute) is detailed in this module. A bit of authorization nature of module which is specific for a particular user.

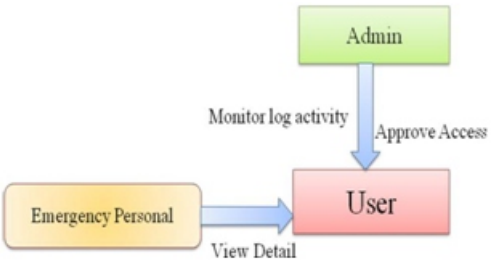
5.3 Public Domain Specification:

Articulating the data between various public domains in the core idea of this module. In this module, the user or Admin will decide the type of data to be shown to the public domain people. A clear bifurcation will be given between the different public domain people.



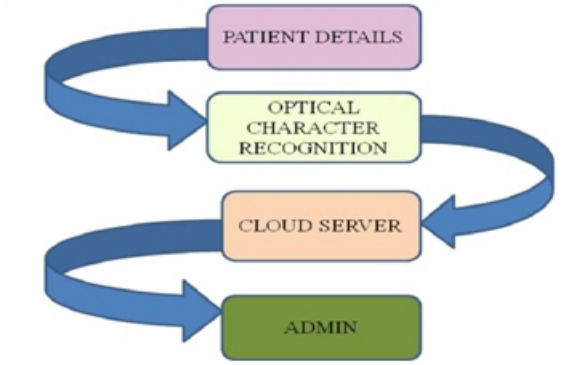
5.4 Admin Approval:

After specifying the data nature to be accessed by the variety of users, the admin will be given an option to approve the data flow and access nature on the user. Admin's nature of work is to validate the logging activities of the users and monitor the security breaches happening in the system.



5.5 Face Recognition:

Patient face is identified for security purpose using face recognition technique. Using Fractal detection to identify the face of patient is more secure than face recognition. It makes easier for public domain peoples to do the medical techniques for the patient. After face recognition, second security method is pattern scheme matching technique. This makes password more secure from the user side.



5.6 Optical Character Recognition

A patient detail is verified by the way of using optical character recognition. Optical character recognition convert printed text and images into machine readable format. Using this technique to scan the patient details and store the information in cloud. These patient details is monitored and verified by the admin of a Public Domain.

5.7 Performance Evaluation:

In this module we implemented the highly secured techniques to analyze the patient details and in case of emergency an automatic sms send to the patient directly. If it is in the case of any unauthorized person access the patient data is not allowed. To analyze the secureness over the data is performed by Admin. A secure and privacy-preserving opportunistic computing (SPOC) is used in the framework for mobile-environment Healthcare emergency, data to achieve the high reliability of PHI. (Personal Health Information).

6. Conclusion:

We have described an approach to cloud assisted mobile access in this article and pointed out their strengths and limitations. Cloud computing means to reach the full potential promised by the technology, it must offer solid information security. In network and information security, data protection and privacy we look at the security benefits of cloud computing and its risks. In this project we are going to protect the medical details in cloud. The patient has the ability to set clear segregation of document access rights for his sensitive information. Pattern classifiers are in place to make sure high security for the documents. This project provides more and more security protection and it becomes proposed scheme is efficient and well as scalable.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In a cloud-driven world, privacy and security issues will not only be real challenges but they will increase as well. Hackers will pursue new avenues to infiltrate corporate and personal computing. Our project going to solve the hacker's unauthorized access and provides a data protection. Future of this work is bright, that means using our proposed system in implemented level to modify the current cloud assisted system in more familiar.

7. Acknowledgement:

We would like to sincerely thank Assistant Prof. Mrs. T. P. Dayana Peter, for her advice and guidance at the start of this article. Her guidance has also been essential during some steps of this article and her quick invaluable insights have always been very helpful. Her hard working and passion for research also has set an example that we would like to follow. We really appreciate her interest and enthusiasm during this article. Finally we thank the Editor in chief, the Associate Editor and anonymous Referees for their comments.

References:

[1]L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for e-Health networks," in Proc. IEEE Intl. Conf. Distrib. Comput. Syst., Jun. 2012, pp. 224–233.

[2]J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.

[3]J. Sun, X. Zhu, and Y. Fang, "Privacy and emergency response in E healthcare leveraging wireless body sensor networks," IEEE Wireless Commun. vol. 17, no. 1, pp. 66–73, Feb. 2010.

[4]J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," in Proc. IEEE Global Telecomm. Conf., Dec. 2010, pp. 1–6.

[5]J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[6]Dawn Xiaoding Song, D. Wagner and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proc. IEEE 2000 IEEE Symposium on Security and Privacy., New York City, NY, USA, Sep. 2000, pp. 44.

[7]M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," presented at the 14th Int. Workshop Database Expert Syst. Appl., Prague, Czech Republic, 2003.

[8]L. Zhang, G. J. Ahn, and B. T. Chu, "A rule-based framework for role based delegation and revocation," ACM Trans. Inf. Syst. Security, vol. 6, no. 3, pp. 404–441, 2003.

[9]Ian Foster, Carl Kesselman, Gene Tsudik and Steven Tuecke, "A Security Architecture for Computational Grids," proc. 5th ACM conference on Computer and communications security, pp. 83–92, 1998.

[10]L. Zhang, G. J. Ahn, and B. T. Chu, "A role-based delegation framework for healthcare information systems," in 7th ACM Symp. Access Control Models Technol., Monterey, CA, USA, 2002, pp. 125–134.

Author's :

Ms. Nallabothula Aruna, M.Tech Student, Department of CSE, KLR COLLEGE OF ENGINEERING AND TECHNOLOGY.

Mr. R.Adinarayana, working as an Asst professor in the Department of Computer Science and Engineering, KLR COLLEGE OF ENGINEERING AND TECHNOLOGY, JNTUH, Hyderabad.

Mrs. S.S.Madhavi, working as an Associ-ate professor in the Department of Computer Science and Engineering, KLR COLLEGE OF ENGINEERING AND TECHNOLOGY, pursuing her Ph.D. in Computer Sci-ence and Engineering from JNTUH, Hyderabad. Her research area is BigData.