Design Efficient Intrusion Detection System for Cloudlet Based Medical Data Sharing

Ms Mayuri S Taley
ME 2nd Year Computer Science and Engineering
Dept.of Computer Science Rajashri Shahu
College of Engineering, Buldana, India

Prof A.P.Kankale
Assist.Professor & Head
Dept. of Computer Science Rajashri Shahu
College of Engineering Buldana ,India.

Abstract

Data security when sharing and storing of data on the cloud. Proposed work discusses efficient cryptography techniques for providing stronger security. To design an efficient system i.e. an important part of the proposed security framework. This research work security scenario for the cloud computing where to provide the hybridization of symmetric techniques such as AES and 3DES. To develop data storage system on the cloud for storing and sharing users data safe and secured. The proposed system is the combination of two different symmetric key security algorithms. AES and 3DES is the symmetric key algorithm is used for the encryption and decryption of data.

Keywords—CLOUD COMPUTING, AES,DES etc .

1 INTRODUCTION

Healthcare organizations are building their IT infrastructures to be more flexible and scalable to meet the growing data demand. With value-based incentives for data analytics and the increased number of connected medical devices constantly collecting data, organizations are challenged with storing clinical data. Cloud data storage options offer a flexible and scalable environment at a lower cost than on-premise deployments, which is appealing to covered entities. Organizations exploring data analytics are expecting their storage requirements to steadily increase as Internet of Things (IoT) and mobile devices collect data that needs to be stored. Cloud computing supports mobile and collaborative applications and services. Increased storage, high automation, flexibility, and reduced cost are a few advantages cloud computing offers. Using cloud computing can Improve healthcare services delivery for patients. In this paper, the categories and service models of cloud computing, its technology intelligence, diverse applications in medical services and healthcare.

Cloud computing is a business model and technology platform, which is the result of evolution and convergence of many created and independent computing methods and technologies, including utility computing, on-demand services, grid computing and software-as-a service [12]. Cloud computing has a dynamic and flexible architecture that makes it possible for a scalable information technology capacity to be provided in services and delivered over the Internet to a number of external users. Services and information exist in a shared, dynamically scalable set of resources based on virtualization technologies and/or scale-out application environments [13]. An important feature of cloud computing is scalability, a key technology that enables the virtualization [14]. In the most general sense, the concept of virtualization describes the development environment and methodology for the sharing of computer resources into multiple independent execution environments or associations of several resources in a smaller environment. It applies one or more different concepts or technologies such as software division, time-sharing, partial or complete hardware simulation, emulation, and many others, with the aim of separating the logical interfaces from physical resources [12].

OBJECTIVES

I. To develop a techniques to prevent data loss during data sharing.
II. To develop a secure Passwords to the users and create an efficient techniques for sharing data fastest.
III. Prevent data access from unauthorized access.
IV. To develop techniques / algorithms in cloud computing environments to secure data and communications.
V. To Improve the Performance evaluation of the existing system in a minimum cost in cloud computing environments.

SCOPE

i. The files stored on these services can often be used on any synchronized computer and may be accessible via any modern web browser.
ii. Effective & Secure Storage System.
iii. Store and shared data can't be accessible by unauthorized user or intruders.

iv. Store and shared data can be design and implemented by Third party Mediator (Security Mediator).
v. Implementation of effective Algorithm for Securing, Storing and sharing data.
vi. The data or information Security is protected during access and sharing by only the authorized users.
vii. The security needed on the protected data are controlled by the data owner and attached to the actual data.

MOTIVATION

Cloud computing is free prevalent systems connected by composite networks in the distributed environment, which makes security huge dispute. Cloud computing technology has grown into beloved alternative to traditional computing technologies. This technology supplied a new approach of a pay-per-use service model of computing resources established primarily on virtualization technology.
The cloud provider has to attempt the large security of data to the cloud user to improve the faith. The cloud technology is elaborating day by day encryption related to the cloud computing should be progressive. The perceptive working principle of cloud encryption is the key to considerate the security of the cloud. To increase the security level different cryptographic algorithms are used.

EXISTING SYSTEM

- The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection,
- First utilize Number of method to encrypt user's body data collected by User Interface.
- Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet.
- The trust model also helps similar patients to communicate with each other about their diseases.
- Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection.
- Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS).

LIMITATION

- Practically, medical data sharing is a critical and challenging issue.
- No Trust.
- Existing Data sharing used only Text Files.
- Existing files may be hack by hackers.
- DDOS Attack is more challenge when used Cloud Computing.
- Existing System Used Only Software Implementation Algorithm i.e (AES).

II PROPOSED IMPLEMENTATION

PROPOSED METHODOLOGY

1. Study of Problems occurs while storing and sharing data.
2. Data collection and Literature Survey.
3. Study of Cloud Computing environment.
4. Develop techniques for data retrieval and store in cloud computing environment.
5. Develop an algorithm to secure the data in the cloud computing environments via security mediators.
6. Analysis of the developing Techniques.
7. Develop tools to obtain required resources.
8. Result

PROPOSED DESIGN

The proposed system allows to search over encrypted files which would be encrypted with different keys for different data owners.
The scheme allows new data users to enter this system without affecting other data users by registering the system and then the users can store and sharing the data.
The system ensures that only authorized users can perform correct searches.
To prevent the hackers from snooping the secret keys and pretending to be legal data users submitting searches.
A hybrid algorithm is proposed to provide security for data on cloud computing with high performance and low processing time.

Advantage

- Medical data sharing is Fully Secure and Authenticate.
- Full Trusted Model.
- Proposed Data sharing use to share Audio, Text, Vedio Files.
- Data Protection by hackers.
- DDOS Attack is Handle by Intrusion detection System
- Proposed System Software Implementation as well as Hardware Implementation Algorithm i.e (AES,3DES).
- Proposed system is Efficient Search.
- Dynamically generate decryption key send to email.

PROPOSED ARCHITECTURE

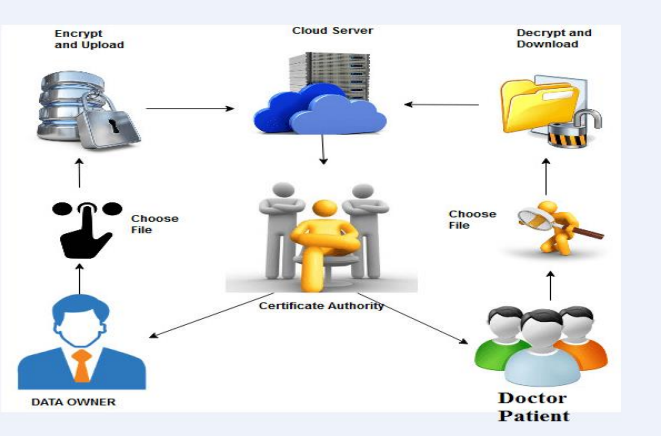


Fig 1 Cloud Server External Interaction Flow

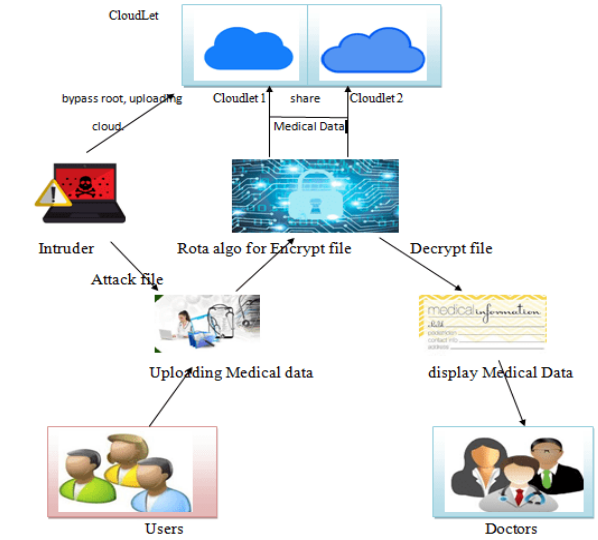


Fig 2 Cloud Server Internal Interaction Flow

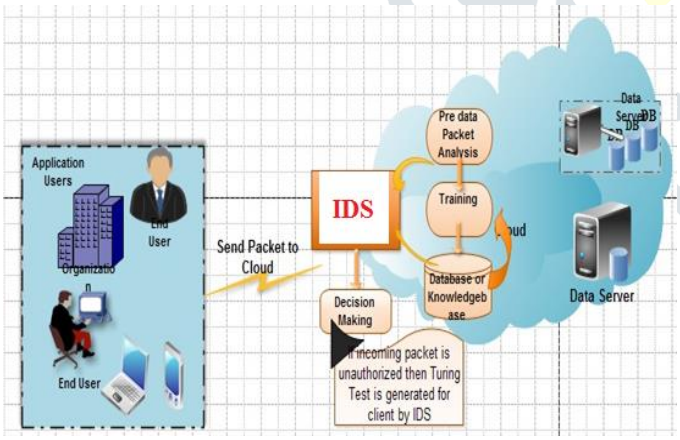


Fig 3 Proposed design of IDS

PROPOSED WORKFLOW

The target of data security is to gain confidentiality by the cryptography and availability by the access control. Data security uses the cryptography when sending data such that data is inadequate to unauthorized persons. There are two cryptographic methods are available such as Symmetric and asymmetric. A framework is designed to increase security while storing and accessing data on the cloud. Before sending the data on the cloud it encrypted by using the symmetric algorithms and then encrypted data upload on the cloud. For this purpose integrated combination of AES + 3DES are used. In proposed system firstly AES generate the keys and 3DES encryption algorithm used to encrypt the data files. The secret key is used for the authentication which is send on the email and the OTP is send on the registered mobile number of the authorized users, if the two keys matches same then the data would downloaded.

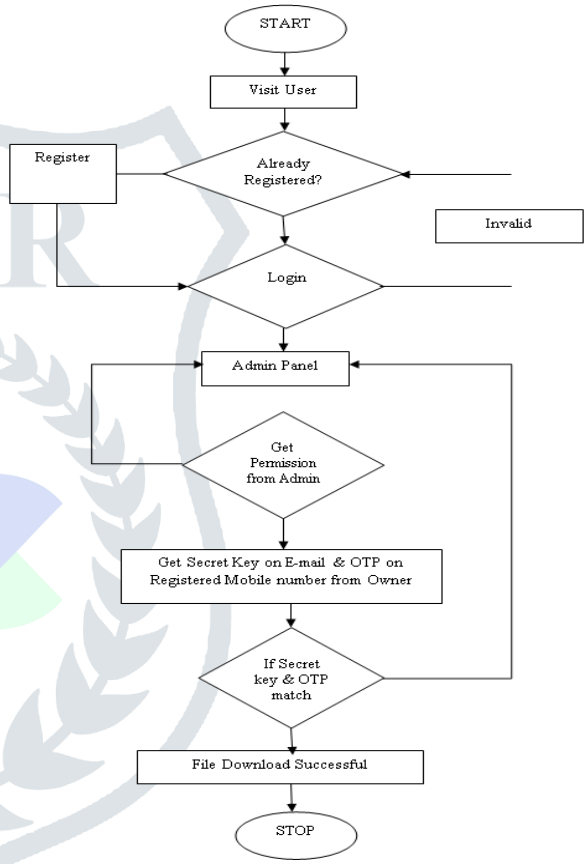


Fig 4 Flowchart of Proposed System

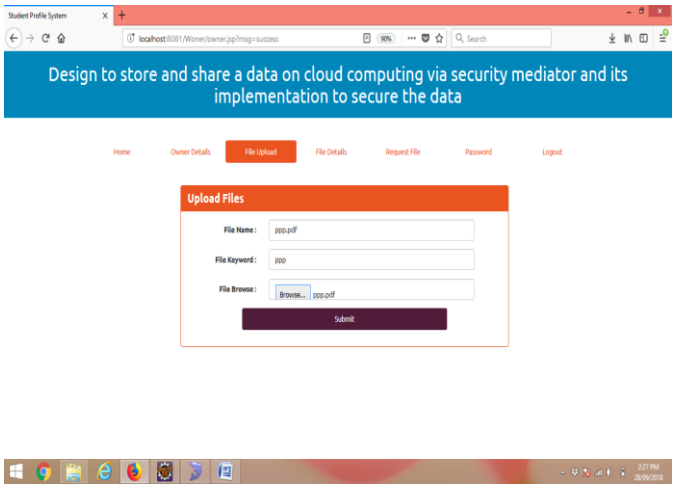
TECHNOLOGY USED

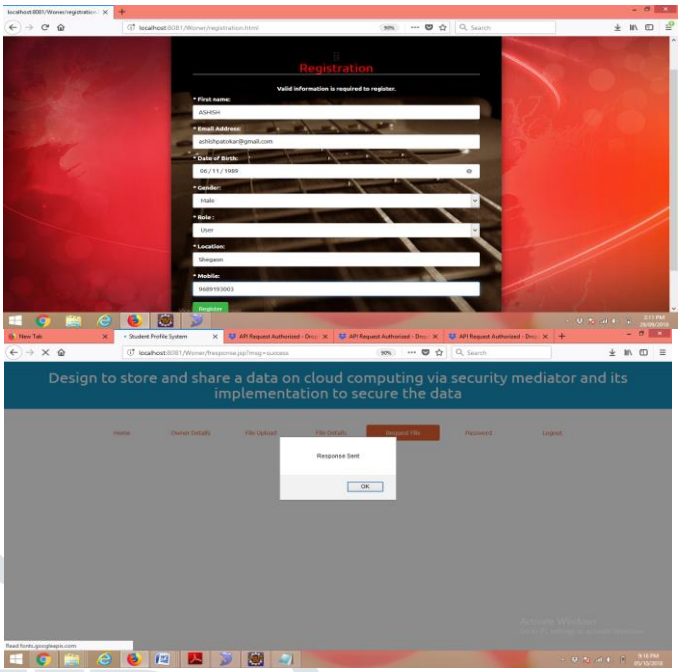
The current Cryptography techniques are used to implement the research work. Cryptography is the security engineering meets mathematics and provides the tools that control the current security protocols. The essential terminology is that cryptography that invoke to the science and art of designing ciphers and the cryptanalysis to the science and art of breaking them. The cryptology often compresses to just crypto; is the study of both and the input to an encryption process is commonly called the plaintext and output cipertext.

The proposed work used the symmetric cryptographic technology used for data security and

data sharing over cloud from authorized data users and also its user sharing group key mechanism with AES and 3DES encryption technique. In this technique file can be uploaded in to the cloud server after encryption of the content by the secret key and encryption techniques. File can be downloaded from the cloud server after decryption of the content by combination of keys and decryption techniques. In this research work security algorithms used in cloud computing, selected and compared to each other. The simulation was performed in order to record the performance of algorithm. Eclipse IDE (Servelets and JSP) used to run Java programs for the algorithms AES and 3DES cryptographic algorithms were implemented using Java programming language on the equal programming environment. The algorithm contains three phases: key generation, encryption and decryption. The Java program for each algorithm take separate inputs for data files, the sizes of data varies from each other. The scheme that was given in the simulation is the time and efficiency of each algorithm. The encryption and decryption time for size of data files for key generation, encryption and decryption were recorded.

SCRRENSHOTS

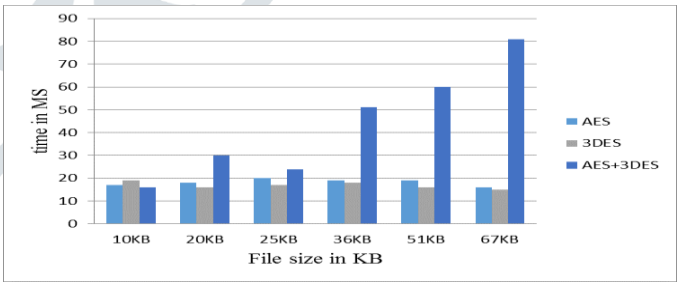




Performance analysis of proposed system

Proposed system of security algorithm for with data storage and sharing in cloud computing environment by simulations to obtain the performance of the algorithm. In this section discusses parameters related to the methodology such as system evaluation parameters, evaluation Platforms, and simulation constraints.

The performance evaluation of the symmetric encryption algorithms such AES + 3DES evaluate a table that the encryption ratio is high in using the both encryption techniques.



Performance Analysis

III EXPERIMENTAL RESULT AND ANALYSIS

In this use the hybrid algorithm such as AES, and 3DES implemented, and their performance compared by encrypting input files of varying contents and file sizes. The algorithm compared to each other by using the parameters and the experimental result is performed and the result shows the encryption, decryption time and the average encryption-decryption time by the simulation.

IV CONCLUSION

The proposed method is much stronger cryptosystem than the traditional methods. This work, presents an efficient approach to provide well-protected security for patients data.
Finally this method can be improved by distributing encrypted data by using 3 DES Algorithm to different data servers without being compromised even if any one of the data server gets attacked.

V FUTURE ENHANCEMENT

Future enhancement is IoT base remote cloud system where doctors can access data for disease diagnosis. A cloudlet based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Such as Mobile, Wears and IoT based sensor System.

VI REFERENCES

[1] Blessing E. James and P.O.Asagba," hybrid database system for big data storage and management", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol. 7, No. 3/4, August 2017DOI: 10.5121.
[2] Ms Jayshree D. Muley, Prof.Harsha R. Vyawahare "A Survey On Hybrid Approach For Information Retrieval Using Big Data Analytics ", International Journal of Ongoing Research in Science and Engineering (IJORSE)Volume 2 Issue 9 SEP 2018,ISSN 2456-8481.
[3]Jingwen Bian, Yang Yang, and Tat-Seng Chua. 2013. Multimedia summarization for trending topics in microblogs. In Proceedings of the 22nd ACM International Conference on Information and Knowledge Management. ACM, 1807–1812.
[4]Albert Bifet. 2013. Mining big data in real time. Informatica (Slovenia) 37, 1 (2013), 15–20.
[5] Schram, A., Anderson, K. M. (2012) "MySQL to NoSQL: data modelling challenges in supporting scalability" Proceedings of the 3rd annual conference on Systems, programming, and applications: software for humanity (SPLASH '12). ACM, New York, NY, USA, pp. 191-202.
[6] Indrawan-Santiago, M. (2012). "Database Research: Are We at a Crossroad? Reflection on NoSQL."Proceedings of the 15th International Conference on Network-Based Information Systems, pp 45-51.
[7] Tauro Clarence T.,Patil,Baswanth R., Prashant K.V.(2013). "A comparative analysis of different NoSQL databases on data model, query model, and replication model" Internal Conference on Emerging Research in Communication and Application ERCICA. Bangalor India
[8] Nayak, A. ,Poriya ,A.,Dikshay Poojary (2013)" Types of NoSQL databases and its comparison with relational databases". International Journal of Applied Information Systems Vol.5, No. 4 pp 16-19
[9]Grolinger,K.,Higashinow,T.Wari,Capretz,M.AM (2013)"Data Management in cloud environments: NoSQL and NewSQL data stores" Vo l2. No. 22.
[101] Porkony, J. (2013). "NoSQL databases: A step to database scalability in web environment.", International Journal of Web Information Systems • Vol. 9, No.1 pp 69-82.
[11] Wu, L., Yuan,L., Huai, Y. (2013). "Survey of large scale data management system for big data applications" Journal of Computer Science and Technology. Vol. 30 pp 163-183.
[12] Moniruzzaman, A .B., Hossain, S.A.(2013). "NoSQL database: New era of databases for big