European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 02, 2020

Information Integrity and Authentication over Cloud Using Cryptographic Techniques

R. Vandana[1*], L. Bindhu Raj[2], B.J. Santhosh Kumar[3]

[1*,2,3]*Department of Computer Science, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru Campus, Karnataka, India.*

[1*]*vandana1156@gmail.com*

[2]*bindhuskb@gmail.com*

[3]*santhoshbj50@gmail.com, bj_santoshkumar@asas.mysore.amrita.edu*

Abstract: Symmetric key and asymmetric keys are used to encrypt and decrypt data, in order to accomplish the main idea of security i.e. to maintain integrity and give valid authentication. Information security and the guaranteed exchange of secure information is effectively achieved through cryptographic techniques. In cloud computing it is necessary to secure data transmission from sender to receiver from hacking, for that we make use of the effective service called the EC2, which is provided by Amazon web services. This allows us to compute in a scalable way in the Amazon cloud. S3, which is known as the simple storage security service is used to store data at any instant in any place. We proposed to develop a modified RSA algorithm to generate a pair key and digital signature to authenticate message. This paper mainly focuses on maintaining confidentiality between cloud and its users in addition to preventing it from attackers.

Keywords: SHA3, AWS, EC2, S3, RSA.

1. INTRODUCTION

Applied science and technology is scurry in the field of internet of things and Cloud Computing is the primary alteration recurring in the commercial environment. It takes part of a faction towards the concentrated, IT specialization. It just not brings convenience and efficiency issue, also effects greatly to make it safe and protect data from intruders. Security has been considered as a great issue in Cloud Computing. The different assets utilized inside the cloud incorporate programming, server, storage, software and network according to pay per usage.

Presently, clinical frameworks are encountering social changes from conventional ways to deal with modernized patient-driven methodologies. In customary methodologies, social insurance laborers assume a significant job. They have to visit the patient for the fundamental analysis and advices. The distributed computing is worked together with close to home social insurance framework so it turns out to be simple for specialists to get to the patient's data in a single pool.

Cloud based encryption is used to look for the information from the attackers which helps to protect perceptive data in cloud, which improves security. Information is made sure about, when it accomplishes confidentiality, integrity and authentication.

In this paper, different encryption algorithms are used to secure data from unauthorized and unauthenticated users, and a mechanism is proposed to secure data by using algorithms in a hybrid way which also comprises of RSA algorithm for digital signature.

2. Literature Review

Archana Bharadwaj [1] in her paper work considers few reports of a person's ECG, which is analyzed and validated in the database, before which the user has to validate the exact transaction ID with the finger prints. The comparison time is reduced and double level authentication is achieved. The text and image can be both encrypted and decrypted. This is not very suitable for huge and bulky file sizes. The monoalphabetic substitution algorithm makes it get exposed to attacks.

Ming Ming Wong [2]demonstrates a new inner f-permutation sub pipelining method. This approach makes way to reduce the memory space utilized and also efficiency is found to be maximum in this case. It is said that it can minimize the critical path in an effective way.

Manpreet Kaur[3] proposes data de-duplication in cloud computing to ease memory utilization by cloud database system. Uses a hashing and inherited algorithm to figure a new algorithm, which provides a unique property of the uploaded file. This work mainly focuses on file de-duplication in order to fulfill the stability.

Ismail Abdulkarim Adamu[4] defines text and image steganography using RSA algorithm, in which text steganography hides the communication in the text file and image steganography secures communication using cover image. This work helps to build a strong security structure in order to improve costumer's satisfaction and to attract more investors for cloud computing.

Hamed Aghili[5] this paper proposes a method involving Blowfish algorithm to ensure security along with a duplicate cloud storage. The image which is stored in the cloud can be encrypted within short period of time without making any changes to the original file.

N.Jayapandian[6]this paper provides a detailed report of encryption algorithms to secure the data using different cloud services. Analysis is made on existing work of encryption and decryption, in which this technique is useful for the real time encryption to provide efficient usage of services and is suitable for different application with its own merits and demerits.

Ramzi Guesmi proposes special color encryption method for images which uses one time key that is absolutely realiable on the chaos operator[7]

Ariel Roy L[8] conveys the usage of one-time passwords to complete a transaction in a secure way, which helps user access systems effectively, hence preventing the access of unauthorized users. Since the OTP generated are sent to mobile phone numbers this requires the user to have a mobile phone to receive the OTP.

Rohini[9] proposes a framework for security issues at authentication level to provide cloud storage. The cloud service models include SaaS, PaaS and IaaS and cloud deployment model includes various types of clouds to perform deployment.

N. Thillaiarasu[10]this paper aims to secure the transmission hint by victimization cryptography which is a combination of blowfish and RSA algorithm along with the digital signature on the data transmission. To convert data into code text writing methodology is intended for the purpose of customers to read and use the record.

Manoj Kumar, Manishankar S, Ranjitha PR [11] this paper provides an outline of data assimilation and processing of data which addresses many problems during data transmission. Network issue arises while performing off-load of data from one node to one more node. This algorithm proposes a methodology to perform offloading by providing energy and distances to the nodes in the cluster.

Santhosh Kumar BJ, Roshni Raj VK and Anjali Nair[12] this paper provides a detailed description of AES and RSA algorithm by taking into account special types of attacks on medicinal images. By comparing AES and RSA algorithms will provide more efficient for confidentiality and authentication.

3. PROPOSED WORK

The proposed work make use of Blowfish algorithm to achieve confidentiality, SHA3 algorithm for the purpose of integrity and Diffie-Hellman(DHKE) algorithm for key exchange process.

For cloud computing we have used AWS, EC2and S3 which is as below:

Amazon Web Services(AWS):

AWS is a subordinate of Amazon so as to provide cloud computing platform meant for company and government, these cloud computing network services afford a set of ancient conceptual technical communications and distributed computing construction blocks and equipment. To create a new AWS account user has to sign in to different account first and provide all the necessary account information and choose personal or professional after that will get a confirmation mail. Add a payment method using provided credentials.

Elastic Compute Cloud (EC2)

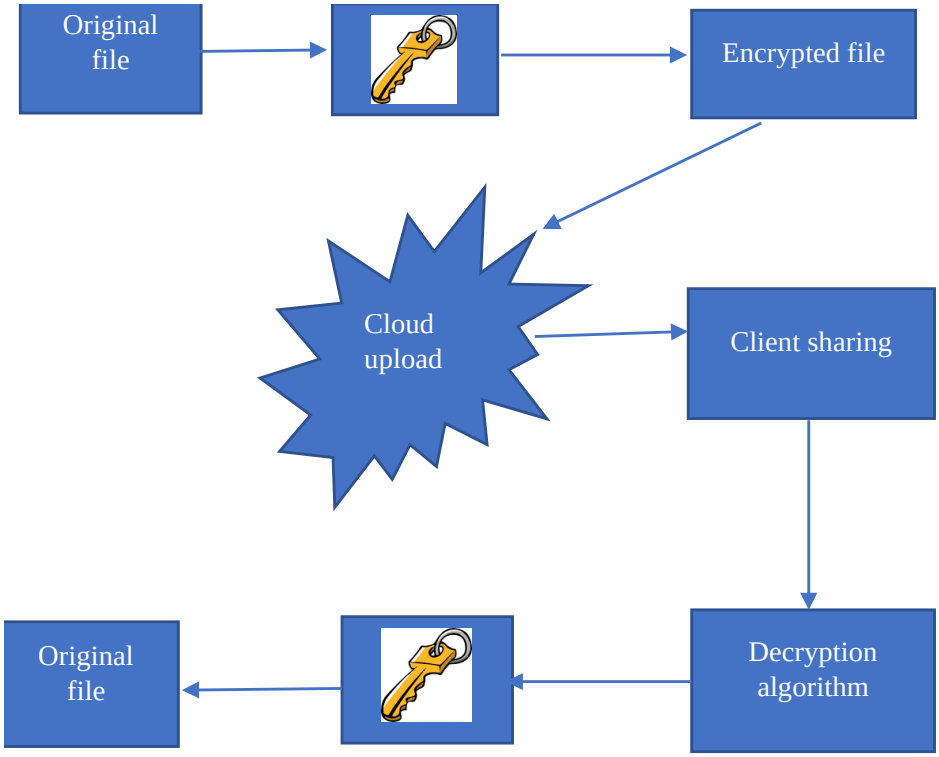

Fig. 1 Architecture Diagram of Proposed Work

EC2 provide scalable computing ability in the Amazon Web Services (AWS) cloud.

Simple Storage Services (S3)

- It provides a network service interface which is used to recover and store data of any size at any instance.
- Every time it splits into “buckets” which are wherever from one byte to two Giga byte

4. METHODOLOGY

The proposed work is a combination of Blowfish, SHA3, Diffie-Hellman and RSA algorithms used to secure database in personal health care system. The whole process is divided into four parts such as,

a. Hash code generation and digital signature
b. Encryption
c. Key exchange
d. Decryption
e. Cloud storage

Hash Code Generation and Digital Signature

When user uploads the file a hash code of variable length is produced with the help of SHA3 algorithm which works in single direction hence the process is irreversible.

Digital signature is a method to make sure the accuracy of digital message which gives the recipient a very strong reason to believe that the message was sent by the known user and ensures that message is not altered during the transaction.

Encryption

The content which is uploaded gets encrypted before actual transmission to prevent it from attacks and this is done using Blowfish algorithm.

Key Exchange Process

The key request is sent to the owner of the file to get access to the private and public keys. The keys exchange is done through the use of Diffie-Hellman key substitute algorithm. Once request is approved the keys are sent through a secure channel. The keys are revoked before the next access to the same content.

Decryption

The decryption method is the reversal of the encryption procedure which is carried out only in the presence of unique public and private keys.

Cloud Storage

The secret keys with the encrypted content are stored in the cloud. The simple storage service which is a very efficient service provided by AWS is utilized. The log files and user detail are stored in the cloud database.

5. RESULT AND ANALYSIS

In this, the whole process is runned through IP address provided by cloud where user has to register, upload files and the end user can download the file using the keys and can view the status of uploaded files. The information associated to the user will be available in server.

When user(a) registers and login with the provided credentials he can upload the files of any size, once he uploads the file, hash code is generated which is in hexadecimal and stored in database. The files uploaded by the user(a) will be visible to all the users who have registered in cloud. The user(b) has to register and to access the file he has to send request, user(a) will have the authority to accept or reject the request.

Once the request is aproved private and public keys are genrated which is one time keys and it is revoked automatically, user(b) should download keys and using those keys can download file. Every time the user wants access to the same file, a new request for the keys must be sent. A mail is sent to the user when requests are made by the end users.

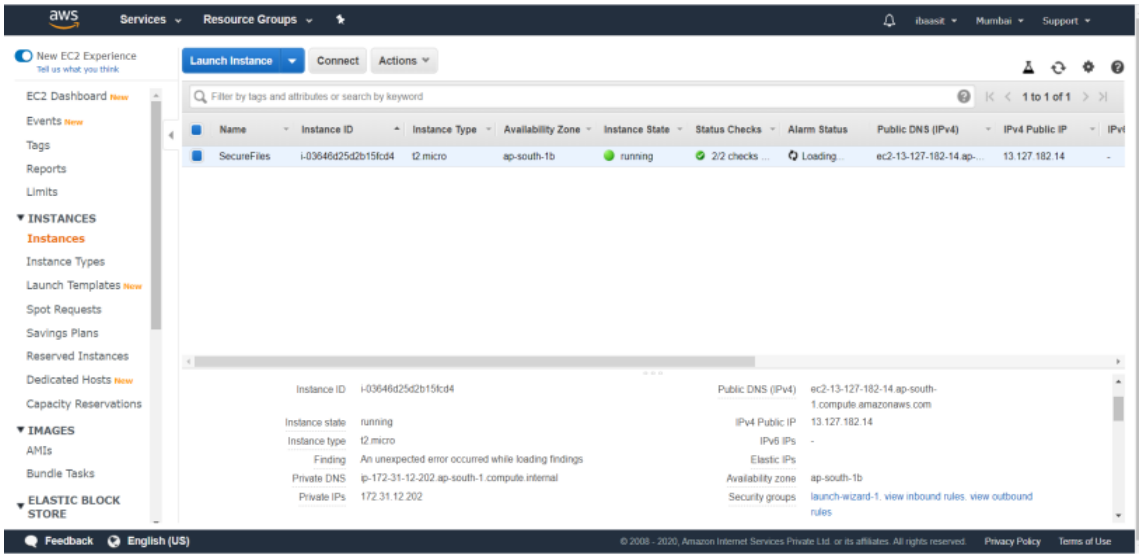

Fig. 2 Running Instance in Cloud

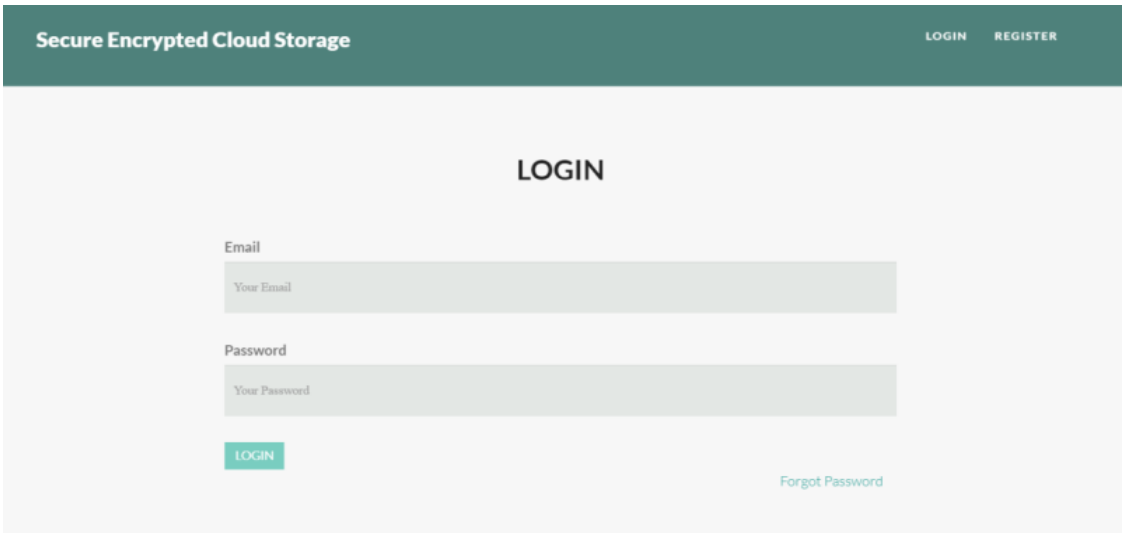

Fig. 3 User Login

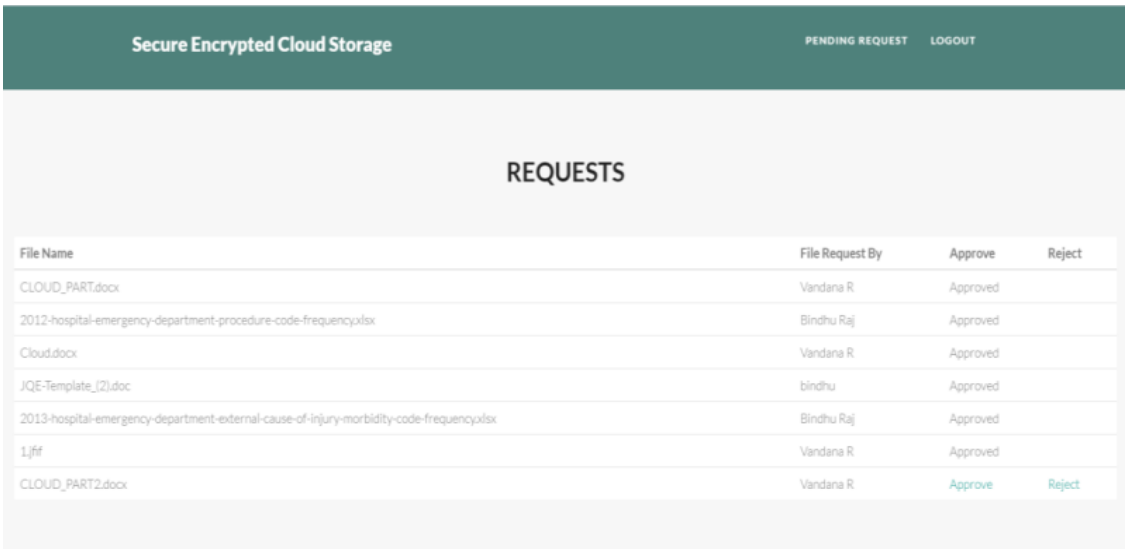

Fig. 4 Requested Files

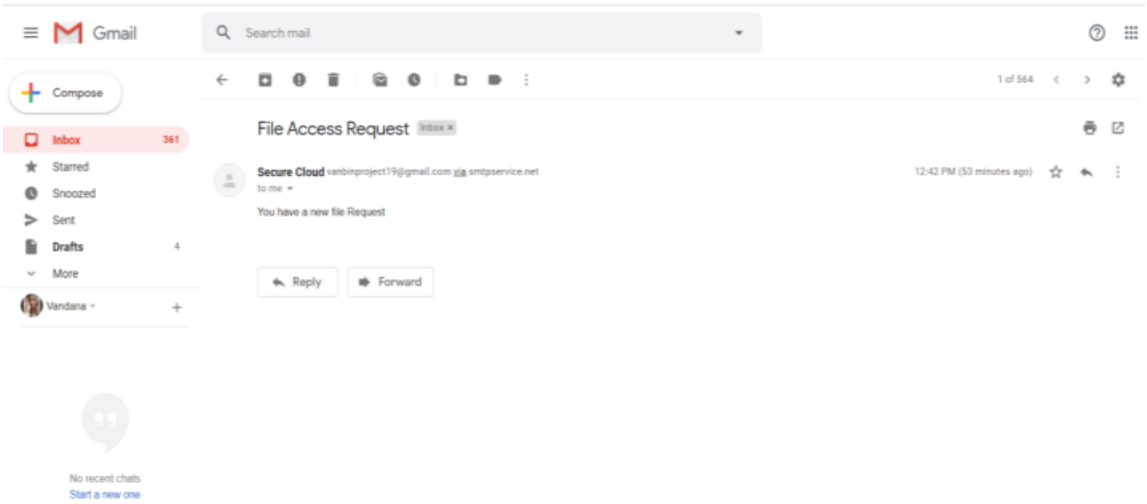

Fig. 5 A Mail Sent to User to Notify the Request

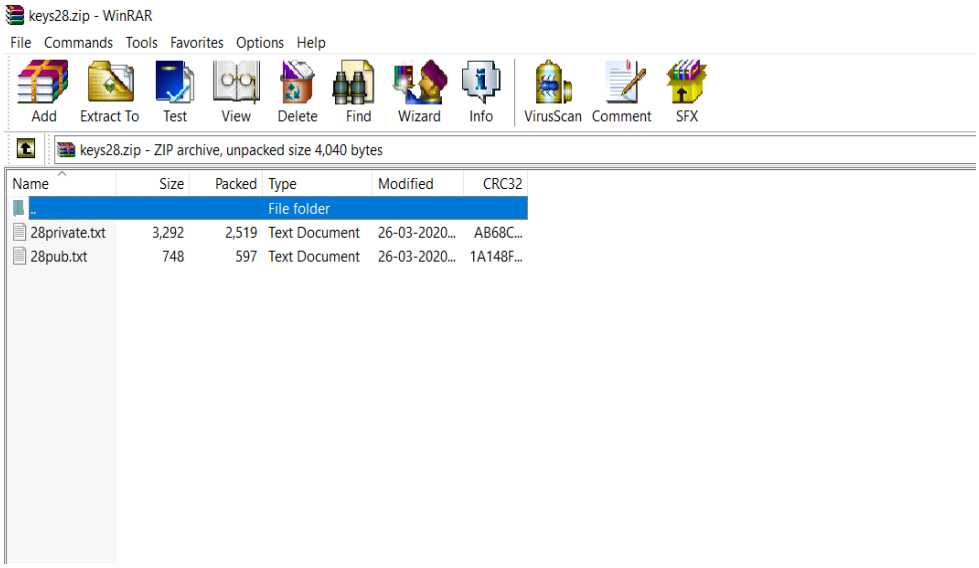

Fig. 6 Generated Private and Public Keys

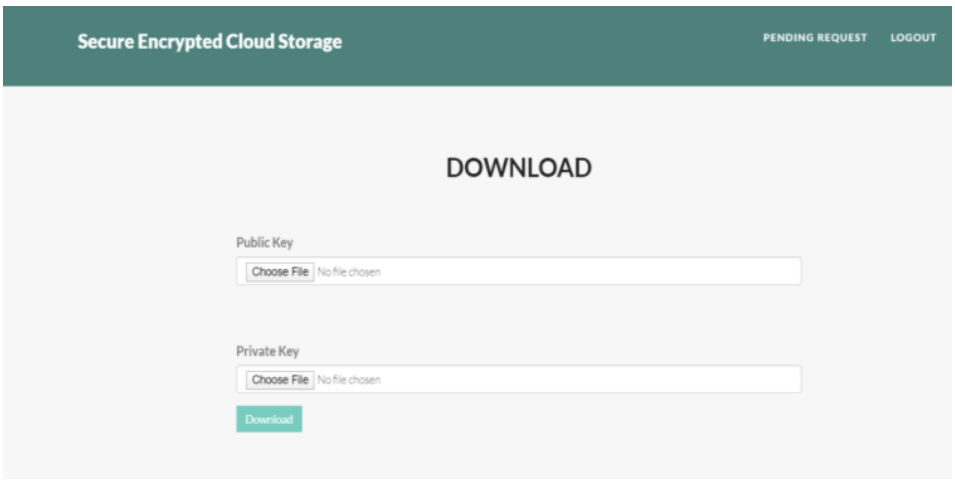

Fig. 7 Process of Downloading File by Uploading Keys

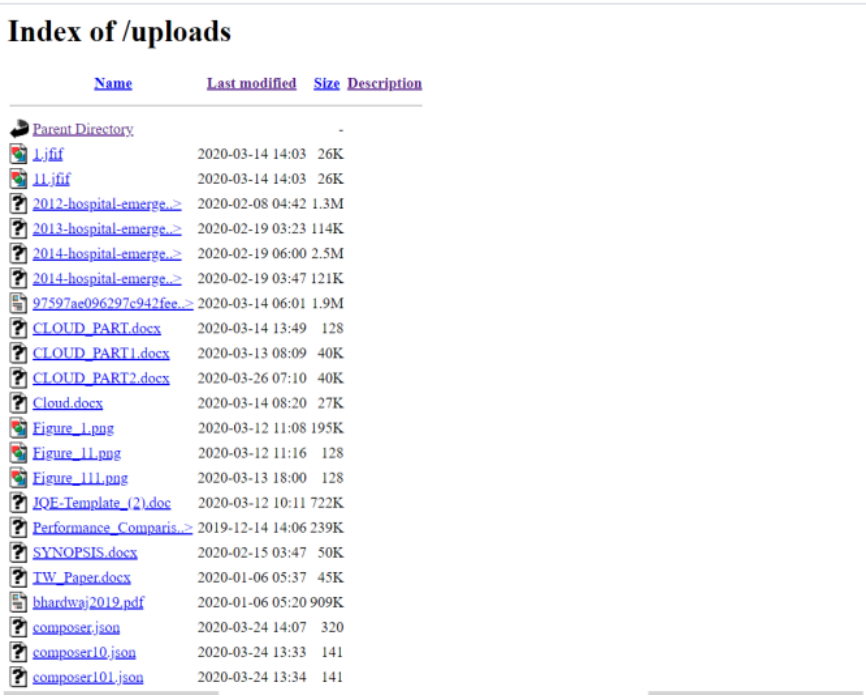

Fig. 8 List of Uploaded Files

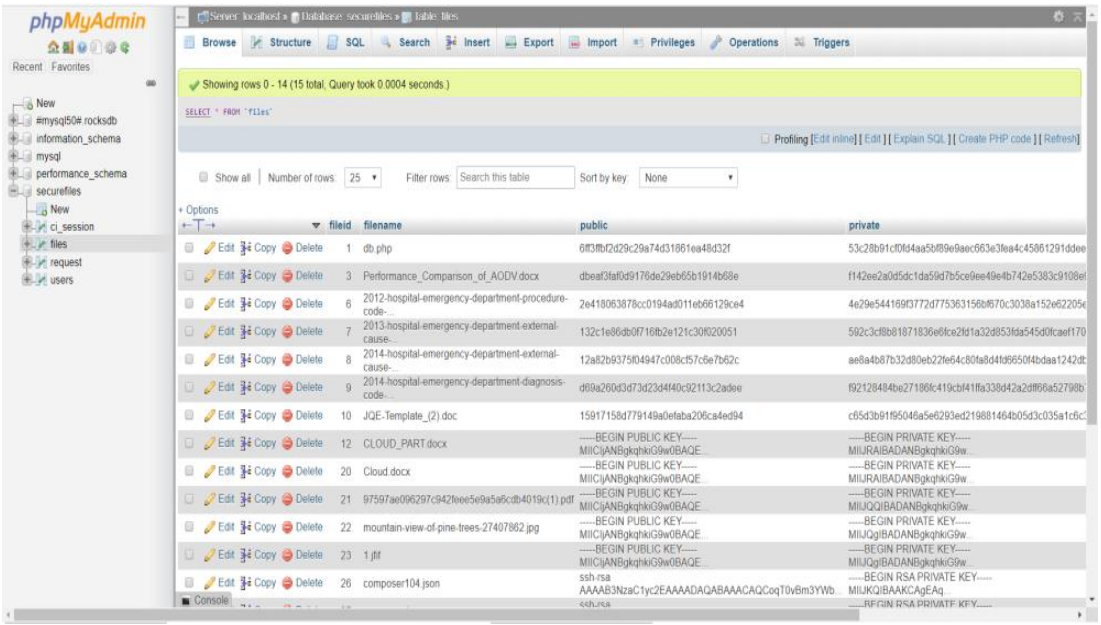

Fig. 9 Database of Files and the Users

This work shows that the automatic key revocation after each transaction, the data which has to be sent will be transacted in a confidential way by maintaining highest form of integrity**.**

6. IMPLEMENTATION

PHP5 is used for implementation in visual studio code editor. The design is done using the HTML 5 and CSS. MySQL 5.1 is used as database. The cloud used is from the Amazon Web Services.EC2 and the S3 services are used.

7. CONCLUSION

Cloud computing is a new trend in which many organizations and companies are moving towards cloud but lagging behind due to security harms. User that stores data on cloud, will have a major concern on service provider whether the file is correctly stored or not. Security of cloud relies on trust computing. In this work we have improved the security using SHA and RSA algorithms with minimum effort. In cloud SHA algorithm is used to generate keys and RSA to secure data without leakage of data which is stored in cloud. Thus, the research paper proposes a system to provide authentication and confidentiality to the stored data.

8. REFERENCES

[1] A. Bhardwaj, S. Chaudhary, and V.K. Sharma. "Biometric Authentication-Based Data Encryption Using ECG Analysis and Diffie–Hellman Algorithm," in *Advances in Intelligent Systems and Computing*, 2019. doi: 10.1007/978-981-13-5934-7_46.

[2] M.M. Wong, J. Haj-Yahya, S. Sau, and A. Chattopadhyay. "A New High Throughput and Area Efficient SHA-3 Implementation," *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2018-May, no. 1, 2018, doi: 10.1109/ISCAS.2018.8351649.

[3] M. Kaur, A. Jain, and A. Verma. "Optimized cloud storage capacity using data hashes with genetically modified SHA3 algorithm," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS 2017*, 2018. doi: 10.1109/ICECDS.2017.8390002.

[4] I.A. Adamu and B. Souley. "Performance Analysis of Text and Image Steganography with RSA Algorithm in Cloud Computing," *Int. J. Softw. Eng. Appl.*, 2018. doi: 10.5121/ijsea.2018.9106.

[5] H. Aghili. "Improving security using blow fish algorithm on deduplication cloud storage," in *Lecture Notes in Electrical Engineering*, 2019.

[6] N. Jayapandian, A.M.J.M.Z. Rahman, S. Radhikadevi, and M. Koushikaa. "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption," *in IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*, 2016, doi: 10.1109/STARTUP.2016.7583904.

[7] R. Guesmi, M.A. Ben Farah, A. Kachouri, and M. Samet. "Hash key-based image encryption using crossover operator and chaos." *Multimed. Tools Appl.*, vol. 75, no. 8, pp. 4753–4769, 2016. doi: 10.1007/s11042-015-2501-0.

[8] A.R.L. Reyes, E.D. Festijo, and R.P. Medina. "Securing One Time Password (OTP) for multi-factor out-of-band authentication through a 128-bit Blowfish algorithm," *Int. J. Commun. Networks Inf. Secur.*, 2018.

[9] Rohini and T. Sharma. "Proposed hybrid RSA algorithm for cloud computing," in *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, 2018. doi: 10.1109/ICISC.2018.8398902.

[10] N. Thillaiarasu, S. Chenthur Pandian, G. Naveen Balaji, R.M. Benitha Shierly, A. Divya, and G. Divya Prabha. "Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems," 2019.

[11] T.M. Kumar, S. Manishankar, and P.R. Ranjitha. "Data integration into cloud with efficient offloading of data from multiple nodes," in *Proceedings of 2017 International Conference on Intelligent Computing and Control, I2C2 2017*, 2018, doi: 10.1109/I2C2.2017.8321814.

[12] B.J. Santhosh Kumar, R.V.K. Roshni, and A. Nair. "Comparative study on AES and RSA algorithm for medical images," in *Proceedings of the 2017 IEEE International*

Conference on Communication and Signal Processing, ICCSP 2017, 2018. doi: 10.1109/ICCSP.2017.8286408.

[13] K.B.J. Santhosh and V. Kruthika. "Symmetric key based encryption and decryption using lissajous curve equations," *Int. J. Electr. Comput. Eng.*, 2017. doi: 10.11591/ijece.v7i1.pp285-288.

[14] B. Sindhushree, S. Manishankar and B.P. Dhanushya. "Cloud based healthcare framework for criticality level analysis." *Int. J. Eng. Adv. Technol.*, 2019.

[15] A.R.L. Reyes, E.D. Festijo, and R.P. Medina. "Blowfish-128 : A Modified Blowfish Algorithm That Supports 128-bit Block Size," no. Wcse, pp. 28–30, 2018.

[16] N. Thillaiarasu, S. Chenthur Pandian, G. Naveen Balaji, R. M. Benitha Shierly, A. Divya, and G. Divya Prabha. "Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems," 2019

[17] J. Hamdard, N. Delhi, P. Agarwal, J. Hamdard, and N. Delhi. "Cryptography Based Security for Cloud Computing System." *Int. J. Adv. Res. Comput. Sci.*, 2017.

[18] M.A.M. Isa, H. Hashim, S.F.S. Adnan, N.N. Mohamed, and Y.F. Alias. "Side-channel security on key exchange protocol: Timing and relay attacks," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 2, pp. 688–695. 2018, doi: 10.11591/ijeecs.v11.i2.pp688-695.

[19] Md Hussain Ahmad and M. Madhava Tripathi, "Development of Encryption and Decryption Technique To Secure the Confidential Data." *Int. J Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 60–63,2018, doi:10.26483/ijarcs.v9i0.6138