International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Educational Assistance for Document Sharing Using Secure Cloud Through HMAC Algorithm

Harshada Mandlik[1],Bhagyashree Pawar[2],Neha Maid[3],Monika Waghchaure[4]

[1,2,3,4] UG Students,Departments of Computer Science,

Gokhale Education Societry's R.H. Sapat College of Engineering ,Nashik-05,Maharastra,India

---

Abstract - There are most of the students are unaware of things related to academics and college like important notices, documents and notes.so we are found the solution on this problem to aware students about their academic and college curriculum by uploading and retrieving the data which is stored on the cloud which access by the authorized user anytime, anywhere. The Notification of uploading and retrieving data is showing on the Timeline and communication for the data shearing with authorized user using chat bot. We are going to use RSA, AES and .HMAC algorithm for Cryptography. Cloud Computing is a growing field in the computing history. It is a way to maximize the capacity and capabilities. We propose a Method that allows user to store and access the data securely from the cloud storage anytime and anywhere. Only authenticated user can access the data. Even cloud storage provider cannot access the data. This method ensures the security and privacy of data stored on cloud. A further advantage of this method is that if there is security breach at the cloud provider, the user's data will continue to be secure since all data is encrypted. Users also need not to worry about cloud providers gaining access to their data illegally.

Key Words: **Web Portal, Cloud Computing, Client/Server, Cloud Security, Android, cloud Storage, Data uploading/retrieving**

1. INTRODUCTION

In the modern world, security has become one of the main concerns about the Digital data. It is necessary in each organization, college, company, and even military to have good data security that enables them to manage and monitor their data. Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security. Also we use chat bot to interactive communication. Chat bot is computer program which conducts a conversation via auditory or textual methods. Some chatter bots use sophisticated NLP systems, but many simpler system scan for keywords within the input. If there lack of security any one can access data and misuse.to prevent such situation we are using some cloud security algorithm name as HMAC(Hash-based message authentication code), RSA(Rivest, Adi Shamir and Leonard Adleman).

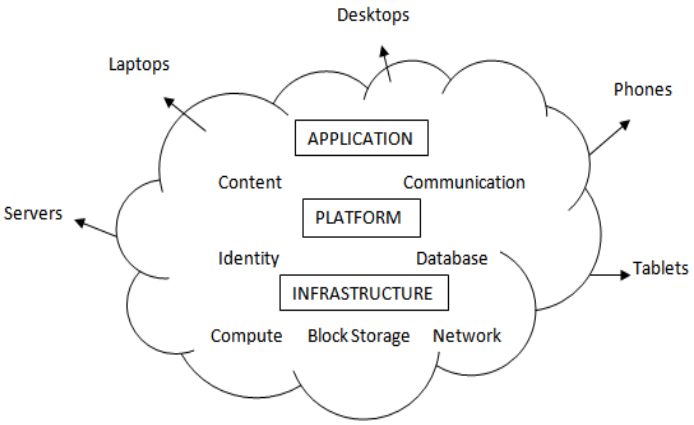

Fig. 1. A view of cloud

By uploading and retrieving the data which is stored on the cloud which access by the authorized user anytime, anywhere. The Notification of uploading and retrieving data is showing on the Timeline and communication for the data sharing with authorized user using chat bot. A chat bot is a computer program which used to communicate between machine and human via textual methods. We are going to use RSA and HMAC algorithm used for security purpose (Cryptography).

1.1 HMAC (Hash-based message authentication code)

HMAC is a hashed message authentication code which is used as a cryptographic checksum in this framework. It is used to detect errors in the data during transmission. Whenever data is transmitted the value of checksum is calculated using the HMAC Algorithm. During file retrieval, the checksum is used to find out whether the data is error free or not. However, it cannot correct the error. It can only detect the error.

HMAC (K, m)=H (K' XOR o pad) OR H((K' XOR I pad) OR m)

Where,

H is a cryptographic hash function,

K is the secret key,

m is the message to be authenticated,

K' is another secret key, derived from the original key K (by padding K to the right with extra zeroes to the input block size of the hash function, or by hashing K if it is longer than that block size), o pad is the outer padding (0x5c5c5c5c5c, one-block-long hexadecimal constant), and I pad is the inner padding (0x3636363636, one-block-long hexadecimal constant)

1.2 RSA (Rivest, Adi Shamir and Leonard Adleman)

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that including the factors of an integer is hard (the factoring problem). RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

2. Online Notes Sharing

In proposed system we are building a website for notes sharing. For data security we gone store our notes on cloud. By uploading and retrieving the notes which is stored on the cloud which access by the authorized user anytime, anywhere. The Notification of uploading and retrieving data is showing on the Timeline. And for communication purpose we are using chat bot. We are going to use RSA and HMAC algorithm for Cryptography. Flow of the proposed system are shown in following figure:

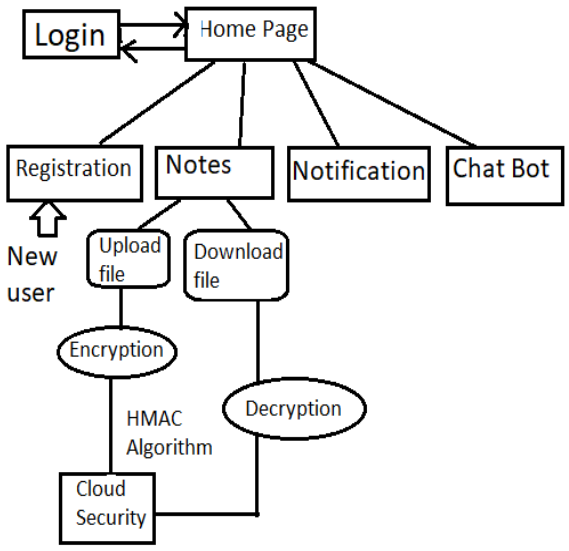

Fig -1: State Transition diagram.

A chat bot is a computer program which conducts a conversation via textual methods. In this paper we are using Chat bot for downloading notes from cloud. While downloading notes which is already encrypted, decryption process is done.

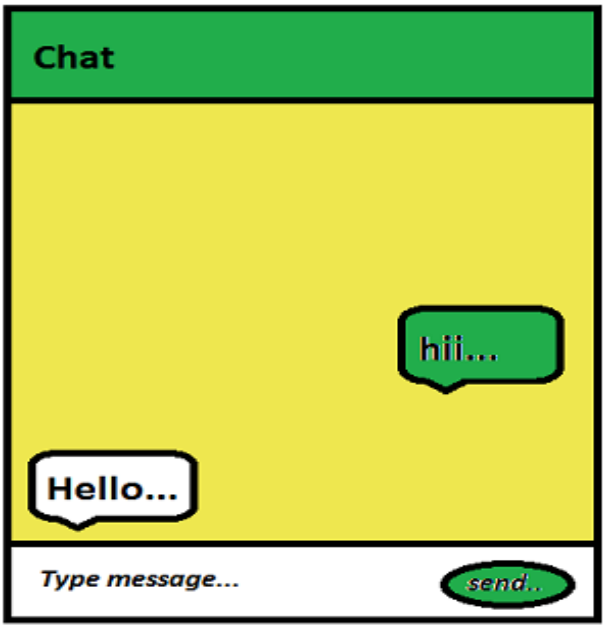

Fig-2 : Demo image of chat bot.

3. CONCLUSIONS

Security at the entrance of an organization will be the first line of defense. Any data are vulnerable to illegal access by outsiders. Security can be enhanced if the organization supports security physically, electronically and procedurally. systems with cloud security are become important nowadays.

REFERENCES

[1] G. L. Prakash, M. Prateek and I. Singh, 'Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal Of Engineering And Computer Science vol. 3, issue 4, pp. 5215-5223, April 2014.

[2] Prof. M.B. Vaidya Computer Department, A.V.C.O.E. Sangamner, India 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015

[3] Arora, Rachna, Anshu Parashar, 'Secure user data in cloud computing using encryption algorithms', International Journal of Engineering Research and Applications Vol. 3, pp.1922-1926, 2015.

[4] Akshita Bhandari "Department of CSE NIIT University Alwar," India 301705, Dec. 2016.