IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 5 (May. 2019), ||S (XV) || PP 68-71

Implementing Data Storage Security in Cloud Computing

Nayana Bnasod[1], Mr. Pranjal Dhore[2], Ms. Nisha Balani[3]
Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India
Email: nainabansod4495@gmail.com, pranjal.dhore@gmail.com, n.balani@jit.org.in

Abstract: *Anti Crime branch maintain huge data related to criminals and crimes done. They use manual system to maintain individual file. They need a space to maintain these files digitally. So cloud is best solution for it and that too be maintained with security. Cloud computing provides on demand services to its clients. Data storage is among one of the primary services provided by cloud computing. The goal of cloud computing is to allow users to take benefit from all these technologies[5]. Many organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere. Cloud service provider hosts the data of data owner on their server and user can accessthei data fromthese servers. As data, owners and servers are differentidentities, the paradigm of data storage brings up many security challenges. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper, we will discuss the different techniques that are used for secure data storage on cloud. We will use cryptography to maintain data in encrypted format and we will use two way security to authenticate users of this anticrime branch data[9].*

Keywords: *Cloud computing, Data storage, Cloud storage server, Cryptography, TwoWay Security.*

I. Introduction

Anticrime data hubs are where files are maintained related to criminals and crimes done in India. They need to maintain data digitally and in secured manner, so that data can be accessed in readable manner with high security. Manual System of handling such data is time consuming and rigorous. We can define cloud storage as storage of the data online in the cloud. A cloud storage system is considered as a distributed data centers, which typically use cloud-computing technologies and offers some kind of interface for storing and accessing data. When storing data on cloud, it appears as if the data is stored in a particular place with specific name[2]. Data breaching is possible in cloud environment, since data from various users and business organizations lie together in cloud. By sending the data to the cloud, the data owners transfer the control of their data to a third person that may raise security problems. Sometimes the Cloud Service Provider(CSP) itself will use/corrupt the data illegally.

Security and privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. A simple solution is to encrypt the data before uploading it onto the cloud. This approach ensures that the data are not visible to external users. In this paper, we discuss the security flaws in data storage and the mechanisms to overcome it. We will discuss the different techniques that are used for secure data storage on cloud[11]. We will use cryptography to maintain data in encrypted format and we will use two way security to authenticate users of this anticrime branch data.

II. Related Work

In order to complete this researchsuccessfully, we have gone through following research papers to get ideas
1) Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers. This study identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data[1].

2) Cloud Computing is a huge scale distributed computing prototype that is manage by economies of scale, in which services are provided on demand over the internet for customers. Central remote servers and Internet are used to maintain application and data in cloud computing. It allows using application without access and installation their personal files on computer with internet access because of which data storage, bandwidth and processing became more efficient[7].

3) Multiple issues with cloud computing that impairs security and privacy of data, as well as presents on threat that impacts data residing in the cloud. In addition to this, various mitigating approaches for countering these

threats are presented here as well as multiple open issues are noted for further studies for providing a secure cloud computing environment[5].

4) The security of cloud computing plays a vital role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. The main issue of cloud storage is to secure the data. Many of the security algorithms are available in the cloud computing environment. This proposed algorithm is also to ensure the data key generation very important[4]. In this proposed method ANENC table is used to generate key and perform several versatile operation used to secure the data in cloud computing.

III. Current Implementation

After studying the literature, we proposed a system which works on the following modules.

a. Administration

a. Administrator will be authenticated with static key.
b. He/She can upload, view and change file contents of criminals or crimes done all over India.
c. He can design users and their roles to use cloud data.
d. He can view how many users accessed cloud and can maintain log.
e. He can terminate or blacklist any user or staff and restrict to use cloud files.

b. **Staff**

a. Staff will be provided ID to use for uploading criminals files over cloud
b. They can upload files related to crimes done onto cloud.
c. They need permission to view and change files.

c. **Cloud**

a. We will use windows azure to maintain and store files related to criminals, crimes done.
b. We will use SQL Azure to store and manage database related to implement this paper in encrypted mode.

d. **Cryptography**

a. Cryptography is process to encrypt and decrypt data.
b. We will encrypt data uploaded by staff in encrypted manner.
c. This data will be decrypted for study and maintenance purpose by cloud users by verifying their security.

e. Two Way Security

a. First security will be set by user itself by setting username and password while registering himself.
b. After successful authentication, user will redirected to email link. Once this link verified and he/she can use cloud according to roles set by admin.

f. Users

a. User must be law and anticrime student who need to study over files of criminals and anticrime.
b. User will register himself by submitting degrees
c. Admin will go through degrees, If he find it convenient then he will issue and set roles for user to use cloud data.

System Flow Diagram

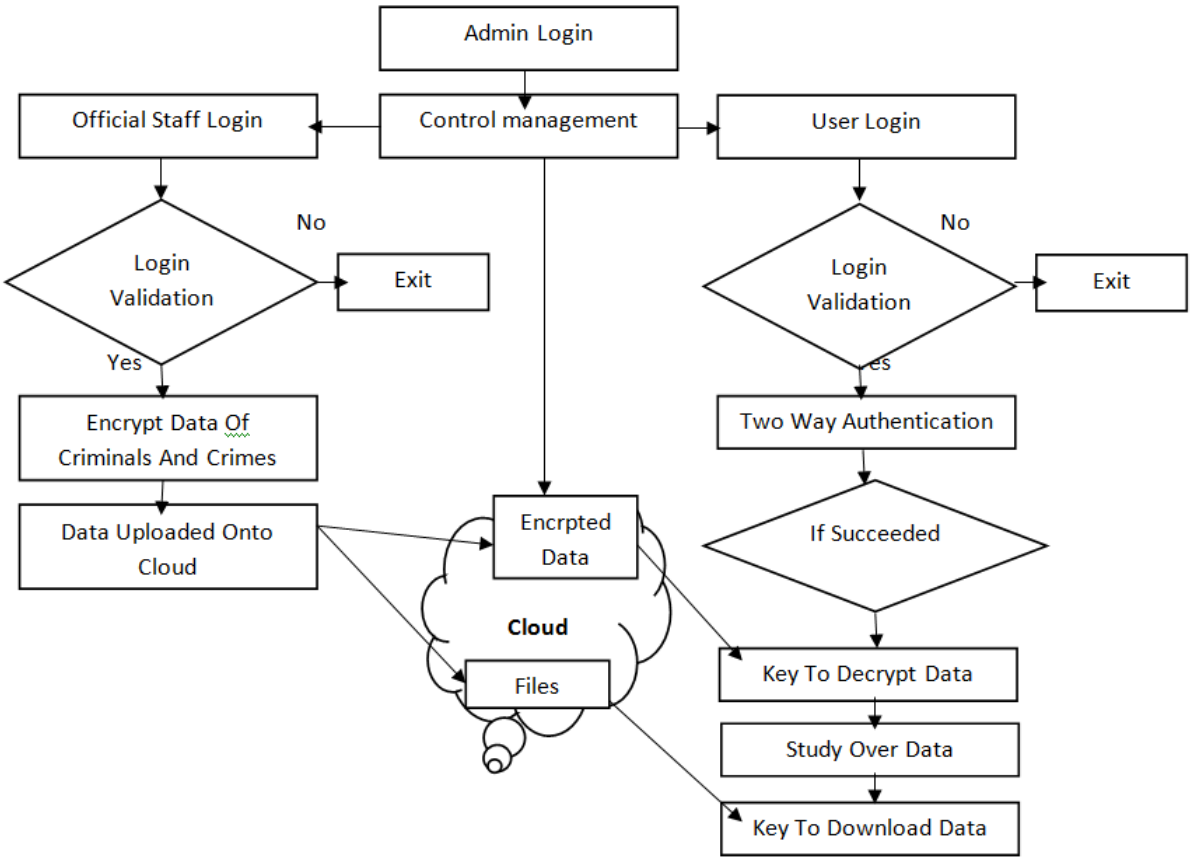

Figure 1: Architecture of project flow diagram

IV. Conclusion

Henceitisconcludedthatwe are developingAnti Crime portal wheretheywillupload data in encrypted mode onto cloud. The users can use and study over this data by decryptingitonlyaftertwowayauthenticationissuccessfullyproceded. Anti Crime branchmaintainhuge data related to criminals and crimes done. They use manual system to maintainindividual file. Theyneed a space to maintainthese files digitally. So cloud is best solution for it and thattoobemaintainedwithsecurity. Cloud computingprovides on demand services to its clients. Data storageisamong one of the primary services provided by cloud computing. Manyorganizations are movinginto cloud becauseitallows the users to store their data on clouds and can access at anytime from any where. In thispaper, wediscussed the different techniques like cryptographythat are used for secure data storage on cloud. Wewill use cryptography to maintain data in encrypted format and wewill use two way security to authenticateusers of this anticrime branch data.

References

[1]. Naresh Vurukonda, B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing",2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016).
[2]. Monjur Ahmed and Mohammad Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.
[3]. V.S. Varnika, "Cloud Computing Advantage and Challenges for Developing Nations", International Journal of Scientific Research in Computer Science and Engineering Vol.6, Issue.3, pp.51-55 , June (2018).
[4]. Dr. Ramalingam Sugumar, K.Raja, "A Study on Enhancing Data Security in Cloud Computing Environment", Dr. Ramalingam Sugumar *et al*, International Journal of Computer Science and Mobile Applications, Vol.6 Issue. 3, March- 2018, pg. 44-49.
[5]. Eesa Alsolami, "Security threats and legal issues related to Cloud based solutions", IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.5, May 2018.
[6]. Varsha, Amit Wadhwa, Swati Gupta, "Study of Security Issues in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 230-234.
[7]. Prof. Syed Neha Samreen, Prof. Neha Khatri-Valmik, Prof. Supriya Madhukar Salve, Mr. Pathan Nouman Khan,"Introduction to Cloud Computing", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 02 | Feb-2018.

[8]. M.B. Jayalekshmi and S.H. Krishnaveni, "A Study of Data Storage Security Issues in Cloud Computing", Indian Journal of Science and Techonology, Vol 8(24), DOI:10.17485/ijst/2015/v8i24/84229, September 2015.
[9]. Everaldo Aguiar, Yihua Zhang, and Marina Blanton," An Overview of Issues and Recent Developments in Cloud Computing and Storage Security".
[10]. Ilango Sriram, Ali Khajeh-Hosseini, "Research Agenda in Cloud Technologies".
[11]. John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security".