ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

A Survey on Secure Cloud Computing Using Blockchain

Preeti Zirwal[1], Nimisha Battise[1], Bhavana Khandare[1], Snehal Tayade[1], Deepika Thakare[2]

Diploma Student, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India[1]

Guide, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India[2]

ABSTRACT:Here, Blockchain means various blocks which are interconnected with each other. In this application blocks are used for storing data.It is important to secure data from attackers to prevent the software piracy and unauthorized access of our personal data. With cloud storage services, users can store their data to the cloud and realize the data sharing with others.The new encryption technique has been proposed to encrypt the data. To protect data security, this project makes the first attempt to formally address the problem. Different from traditional security systems, the differential privileges of users are further considered in security check besides the data itself. We also present several new security constructions. We use SHA algorithm which is cryptographic hash function which takes an input and produce a 160 bit (20 byte) hash value and also used to give a key to check the integrity of data, known as message digest. Because of this, if anyone try to edit our data it will detect to the user.

KEYWORDS: Encryption, Decryption, Cloud Computing, Splitting, Cryptography, integrity.

I. INTRODUCTION

As we use BLOCKCHAIN for security instead of uploading data to a cloud server or storing it in a single location, Blockchain breaks everything into small parts and distributes them across the various cloud. If any one or two nodes going down will not result in any data loss. Everything that occurs on the blockchain is firstly encrypted and then it's possible to prove that data has not been altered. If someone does change any record, then the signature is rendered invalid.Each file uploaded to the cloud is also bounded to specify which kind of users is allowed to access the files.

II. LITERATURE SURVEY

1. Server-Aided Encryption for Reduplicated Storage:Server aided encryption for reduplicated storage for cloud storage service provider like Mozy, Dropbox, and others perform reduplication to save space by only storing one copy of every file uploaded to the different location of the cloud .Message lock encryption is used to resolve the problem of clients encrypt their file however the saving are lock. This is used to provide secure reduplicated storage as well as storage resisting brute-force attacks. Clients encrypt under message-based keys obtained from a key-server via an oblivious PRF protocol in this server. It allow clients to store encrypted data with an existing service, have the service occurs reduplication on their on the part, and yet achieves strong confidentiality guarantees. It show that encryption for reduplicated storage can successfully reach desired performance and space savings close to that of using the storage service with plaintext data.

2. Proofs of Ownership in Remote Storage Systems: It stores only the single copy of the data. Client-side tries to identify the chance already at the client and save the bandwidth of uploading copies of existing files to the server.
a client efficiently prove to a server that that the client keep a file, rather than just some short information about it present solutions based on specific encodings, and analyse their security.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

3. A Secure data with Efficient and Reliable Convergent Key Management: Data securing technique is a used for giving security to data, and has been widely applied in cloud storage to reduce not only storage space but also upload bandwidth.Promising as it is, an appearing challenge is to accomplish secure reduplication in cloud storage. Although convergent encryption has been extensively acquired for secure data, an uncertain issue of making convergent encryption practical is to efficiently and reliably manage a huge number of convergent keys.

4. Private Data Protocols in Cloud Storage: Most important issue in the cloud storage is utilization of the storage capacity. In this paper, there is a key which generate during the process of encryption. The proposed scheme in this paper not only reduces the cloud storage capacity, but also improves the speed of data. Furthermore, the key is computed for every uploaded file for verifying the integrity of files.

III. EXISTING SYSTEM

There are many any other systems are secure cloud storage are available. Like Qualys, White Hat security, Okta. But in our system the file is divided into different parts. If the user want to use that file they can download that particular file.
In qualys , this application, if some malware already happen, it will only give you the steps to fix the problem but in our system you will get a proper notification about that problem.

IV. PROPOSED SYSTEM

It is a DESKTOP APPLICATION. It is related to the personal key which is used in encryption. An attacker carries out various attempts to access a user's computer in order to hack the data. Hackers can break into traditional networks and find all the data and corrupt it, the blockchain makes this thing hard. The data is Encrypted and re-checked by the whole network. Once a record is spitted into various parts it's almost impossible to later or remove without it being noticed. To hack the blockchain you would have to hack most of the nodes simultaneously. Which is very tough.

V. MAJOR CONSTRAINTS

1. File Size: To evaluate the effect of file size to the time spent on different steps, we upload 100 unique files of particular file size and record the time break down. Using the unique or new files enables us to evaluate the worst-case scenario where we have to upload all file data. The time spent on encryption, upload increases linearly with the file size, since these operations involve the actual file data and incur file I/O with the whole file.

2. Privilege set size: To evaluate the effect of privilege set size, we upload 10MB unique files with different size of data owner and target share privilege set size. While the number of keys increases 100 times from 1000 to 10000the total time spent only increase to 3.81 times and it is noted that the file size of the experiment is small level(10MB), the effect would become less significant in case of larger file.

VI. WORKING

1. **Create an account:**
   Firstly, we have to create an account for uploading the file to server in this application. In sign up process you will get a token key for your account. After sign up process you will get your actual account.

2. **Selection of file:**
   After sign up or sign in process you have to select a file to upload. You can select that file for further processing.

3. **Encryption:**
   After selecting a file it is efficient to encrypt that particular file. That file will be encrypted using AES (Advanced Encryption Standard) algorithm. This algorithm is used in our program for encryption method.

4. **Generating a key:**
   After encrypting, a key will be generated for that particular file. This key will be generated automatically by our system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

5. **Splitting of file:**
The file is spitted into 3 or 4 parts. Because of this if attacker tries to hack data or attempt to edit it or delete it he only get the one part of that data as our data is divided into 4 different parts so the only 1 part is not sufficient to hack to the hacker.

6. **Uploading a file:**
After this process the file is ready to upload to the cloud. The 3 or 4 parts of that file is successfully uploaded to the various cloud locations.

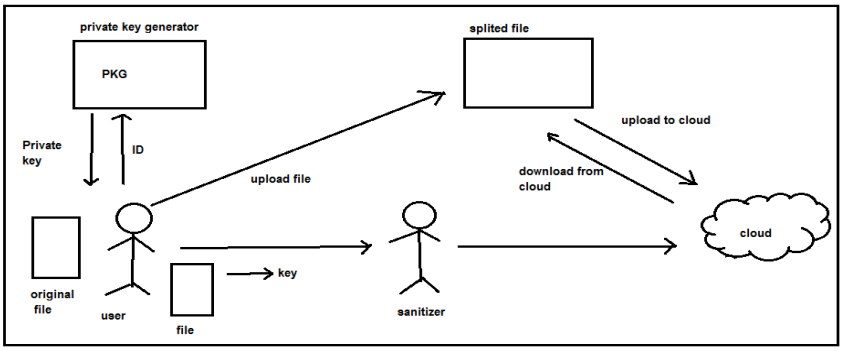
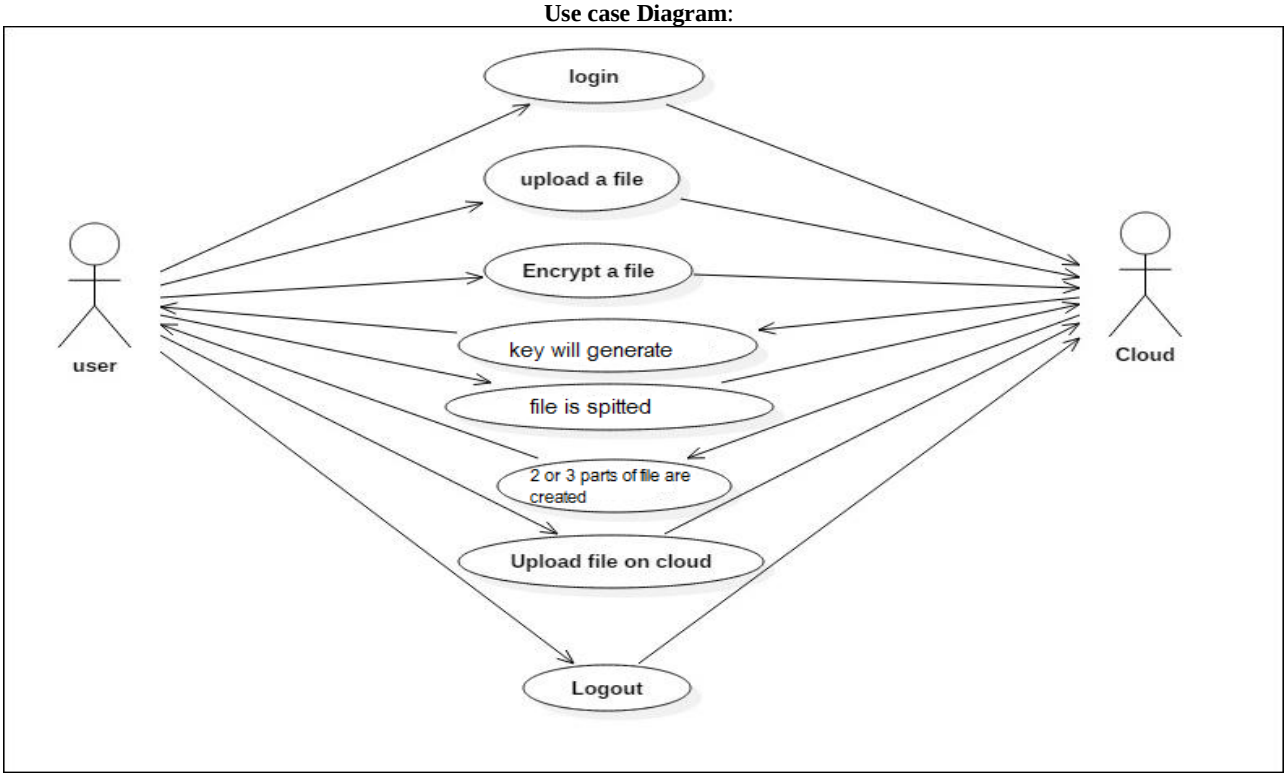


Fig. Block diagram of proposed system

Use case Diagram:



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

VII. ADVANTAGES

- **Cost efficiency –** The main reason behind shifting to cloud computing is that it takes considerably lesser cost than an on-premise technology. Now the companies need not store the data in disks, as the Cloud offers enormous space available for saving money and resources of the companies.

- **High Speed –**Cloud computing lets you use the service quickly in fewer clicks. This quick deployment lets you to get the resources required for your system within fewer minutes.

- **Good accessibility –** Storing the information in cloud allows you to access it anywhere, anytime at any place regardless of the machine making it highly accessible and flexible of present times.

- **Back-up and restore data –** Once the data is stored in Cloud, it is easier to get the back-up and recovery of that, which is quite a time taking process on-premise.

VIII. DISADVANTAGES

- **Security issues –** At the time of storing data in cloud may pose serious challenge of information theft in front of the company. Though advanced security measures are deployed on cloud, still storing a confidential data in cloud can be a risky affair.
- **Low bandwidth –** The bandwidth is low as many users are accessing cloud at the same time which causes its bandwidth to go down. With the less speed the benefits of cloud computing cannot be realized.
- **Flexibility issues –** The cloud services run on various servers which make it hard for the companies to have control over software and hardware. The services at some times do not run the way it should.
- **Incompatibility –** Since the whole infrastructure gets virtualized, increased, Incompatibility issues may be arise at some times that they may pose serious challenges to the smooth or actually running of services. When large number people used this at a same time or may be do the same work then also the incompatibility issues occur.

IX. CONCLUSION

In this project, we proposed an application for securing cloud storage, which sports data sharing with sensitive information hiding. In our scheme, the file will be stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Also the confidentiality and integrity maintained. Because of the blockchain, it is possible to make the cloud storage protected and robust against hacking. We show that our proposed scheme incurs minimal overhead compared to normal operations.

REFERENCES

[1] "What is cloud computing". Amazon Web Services.2013-03-19. Retrieved 2013-03-20.
[2] BaburajanRajani(2011-08-24). "The Rising Cloud Storage Market Opportunity Strengthens Vendors" It.imcnet.com. Retrieved 2011-12-02.
[3] Oestreich, Ken, (2010-11-15). "Converged Infrastucture". CTO Forum. Thectoforum.com. Archived from the original on 2012-01-13.Retrieved 2011-11-03.
[4] "Where is The Rub: Cloud Computing's Hidden Costs". 2014-02-27. Retrieved 2014-07-14.
[5] "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03.
[6] "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.
[7] Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.
[8] Jump up to "Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta". Amazon.com. 24 August 2006. Retrieved 31 May 2014.
[9] Antonio Regalado (31 October 2011). "Who Coined 'Cloud Computing'?". Technology Review. MIT. Retrieved 31 July 2013.
[10] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. chneider. Twin clouds: An architecture for secure cloud Computing. In Workshop on

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Cryptography and Security in Clouds (WCSC 2011), 2011.

[11] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. Re-claiming space from duplicate files in a serverless distributed file system. In ICDCS, pages 617624, 2002.

[12] He, Sijin; L. Guo; Y. Guo; C. Wu; M. Ghanem; R. Han (March 2012). Elastic Application Container: A Lightweight Approach for Cloud Resource Provisioning. 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA). pp. 15–22. doi:10.1109/AINA.2012.74. ISBN 978-1-4673-0714-7.

[13] Marston, Sean; Li, Zhi; Bandyopadhyay, Subhajyoti; Zhang, Juheng; Ghalsasi, Anand (2011-04-01). "Cloud computing – The business perspective". Decision Support Systems. **51** (1): 176–189. doi: 10.1016/j.dss.2010.12.006.