SECURITY ON PUBLIC CLOUD FOR FILE STORING

Jyoti Pawar[1], Sariya Damanwala[2], Tushar Kesare[3], Khalil Pinjari[4]

[1-4]*Department of Computer Engineering, Theem College of Engineering*

---***---

Abstract: *Cloud computing refers to a computing model in which a large number of systems are linked together in private or public networks to provide dynamically scalable infrastructure for application, data, and file storage. It is a modern type of computing in which dynamically scalable and often virtualized resources are made available as services over the Internet. The user will upload the ad to the cloud storage. However, since users no longer have physical control of the outsourced data, maintaining data integrity security in cloud computing is a difficult task, especially for users with limited computing resources. Furthermore, the consumer should not be concerned about the data's integrity and should instead use cloud storage. The customer employs a Third-Party Auditor (TPA), who verifies the data's accuracy. The user employs the services of a Third-Party Auditor (TPA), who verifies the data's accuracy and provides the results to the user upon request. The user can access the data without having to go through the hassle of checking it online, and they can use it without fear. The TPA's trustworthiness is checked, so the cloud user doesn't have to worry about sending a request to an untrustworthy individual. Furthermore, the error's localization is defined so that the misbehaving server can be detected and the user can easily change the data for future use if necessary.*

Keywords: *Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats.*

1. INTRODUCTION

This project focuses on creating a Java-based application that allows the user to perform various cryptographic operations in a GUI (Graphical User Interface) mode. The developed application is a desktop application that, when given various cryptographic keys, generates a report. The user's requests will be processed and executed as required. To make it a standalone application, all of the digital features of Public Key Infrastructure, such as key generation, certificates, message digest, encryption, and signatures, have been combined with the application itself. With large-scale cloud computing in use, the issue of whether computation can be delegated to servers in a safe manner is both a practical and theoretical concern. Another intriguing question is whether we can construct efficient schemes in which the server has no idea what function we want to compute but still computes it for us and returns a response that we can decode to get our desired output. Another intriguing question is if we can devise efficient schemes in which the server has no idea what function we want to compute but yet computes it for us and returns a response that we can decode to obtain our desired performance. A Completely Homomorphic Encryption (FHE) scheme is a protocol (encryption scheme) that allows us to encrypt inputs a, b in such a way that We have Eval (Enc(a), Enc(b)) = Enc(Eval(a, b)) for all functions Eval on inputs, where Enc(a) represents the encryption of input a using our scheme. Only the meaning of FHE is conveyed by this concept. Since we use randomness in our schemes to make them semantically stable, the actual correctness requirement for FHE is slightly different.

2. RELATED WORK

In 2016, Ahmad Albugmi, Robert Walter Published an Research paper name Data security in cloud computing: This paper discusses the safety of knowledge in cloud computing. it's a study of data within the cloud and aspects regarding it concerning security. The paper will enter to details of knowledge protection strategies and approaches used throughout the world to confirm most knowledge protection by reducing risks and threats. Availability of knowledge within the cloud is useful for several applications however it poses risks by exposing knowledge to applications which could have already got security loopholes in them. Similarly, use of virtualization for cloud computing may risk knowledge once a guest OS is run over a hypervisor while not knowing the reliability of the guest OS which could have a security loophole in it. The paper also will offer Associate in Nursing insight on knowledge security aspects for Data-in-Transit and Data-at-Rest. The study relies on all the degree of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

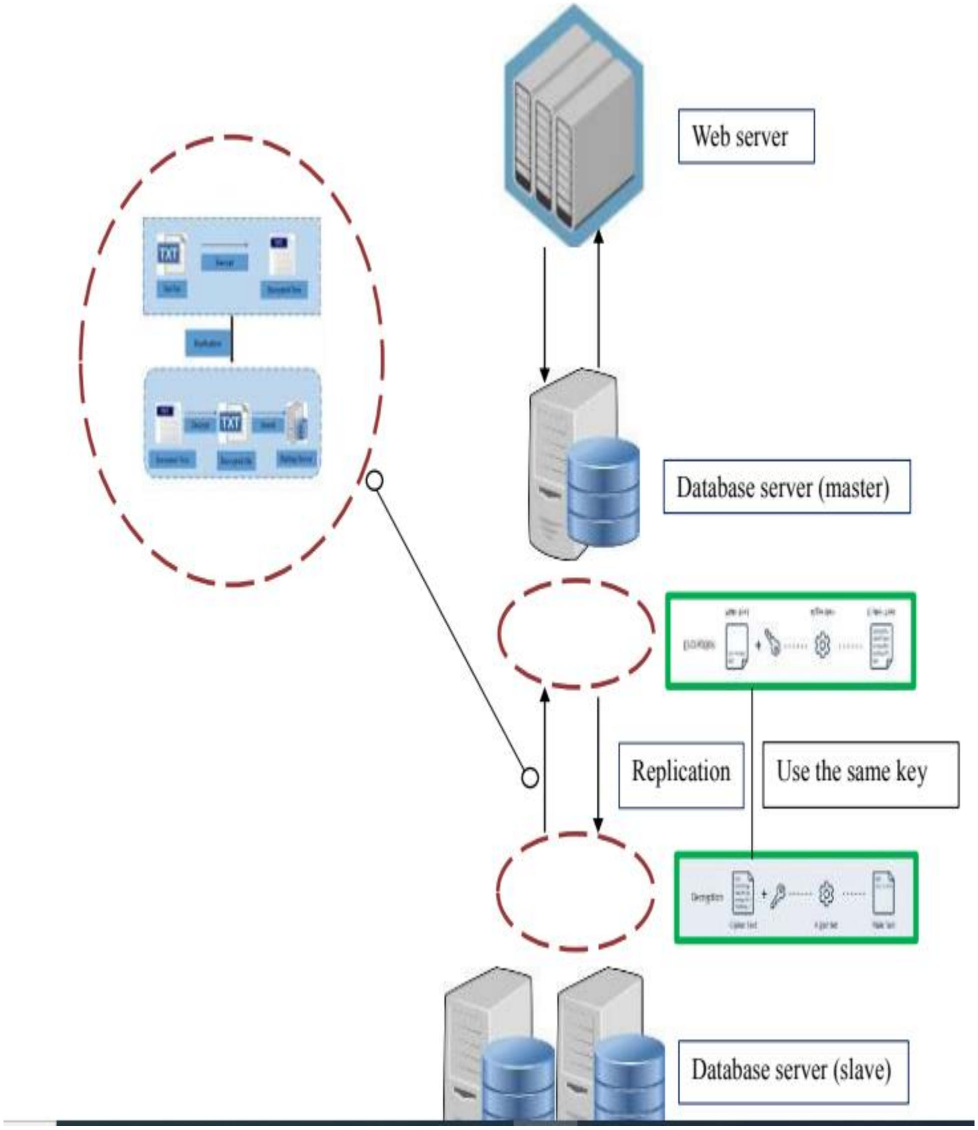
In 2018, Yue Shi Published a Research paper name Data Security and Privacy Protection in Public Cloud: This paper discusses approximately the challenges, benefits and shortcomings of present answers in records protection and privateness in public cloud computing. As in cloud computing, oceans of records could be saved. Data saved in public cloud might face each out of doors assaults and internal assaults on account that public cloud issuer themselves are untrusted. Conventional encryption may be used for storage, but maximum records in cloud desires similarly computation. Decryption earlier than computation will reason big overheads for records operation and plenty of inconvenience. Thus, green strategies to shield records protection as properly as privateness for big quantity of records in cloud are necessary. In the paper, extraordinary mechanisms to shield records protection and privateness in public cloud are discussed. A records protection and privateness enabled multi-cloud structure is proposed.

In 2014, Kirti A. Dongre, Roshan Singh Thakur and Allan Abraham Published a Research paper name Secure Cloud Storage of Data: Cloud computing is one in every of the approaching technologies that may upgrade generation of Internet. the info stored within the good phones is multiplied as a lot of applications are deployed and executed. If the phone is broken or lost then the data hold on in it gets lost. If the cloud storage is integrated for normal information backup of a mobile user in order that the danger of knowledge lost is minimized. The user will store data within the server and retrieve them at anytime from anywhere. the info would possibly be uncovered by attack throughout the retrieval or transmission of knowledge victimisation wireless cloud storage while not correct authentication and protection. So, to avoid this during this paper we tend to style a mechanism that has a security requirement for information storage of mobile phones.

In 2012, Wentao Liu Published a Research paper name cloud computing security problem and strategy: The cloud computing could be a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and different laptop technologies and it's additional advantage characters similar to massive scale computation and information storage, virtualization, high expansibility, high reliableness and low worth service. the safety downside of cloud computing is incredibly necessary and it will prevent the fast development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security downside and its strategy in keeping with the cloud computing ideas and characters. the information privacy and repair handiness in cloud computing are the key security problem. Single security methodology cannot solve the cloud computing security problem and lots of ancient and new technologies and techniques should be used together for safeguarding the entire cloud computing system.

3. METHODOLOGY

In figure shows that a general process of encryption of data replication. Its involves two databases which are master sever and slave server and base server has original copy data information while slave database server act backup server because they contain replicated copy of data information. For this project, employee data information will be used as a collection data. After that it stored the data in database server (master). Generally, authorize user access the web server and make a change to data input whether to add, delete, update about the data information. The data might be in semi-structured or unstructured condition. So, it needs to be in sorted first and stored in database server. For the first step, we have to select text file that saved on database server (master) because we want to encrypt it and replicated to another database which is slave database. The reason why text file needs to be encrypted because to ensure That data selected is secured during the process occur. Next, the encrypted text files need to replicate to backup server. So, the process of replication occur start from database server (master) to backup server (slave). This is can increase data availability, performance and enhances data access. Besides, the response time also will be faster. For example, if sudden damage happens to the server the other server already has that backup. So, the time taken to wait for maintenance to process it again is shorter.


Web server
TXT
Database server (master)
Replication
Use the same key
Database server (slave)

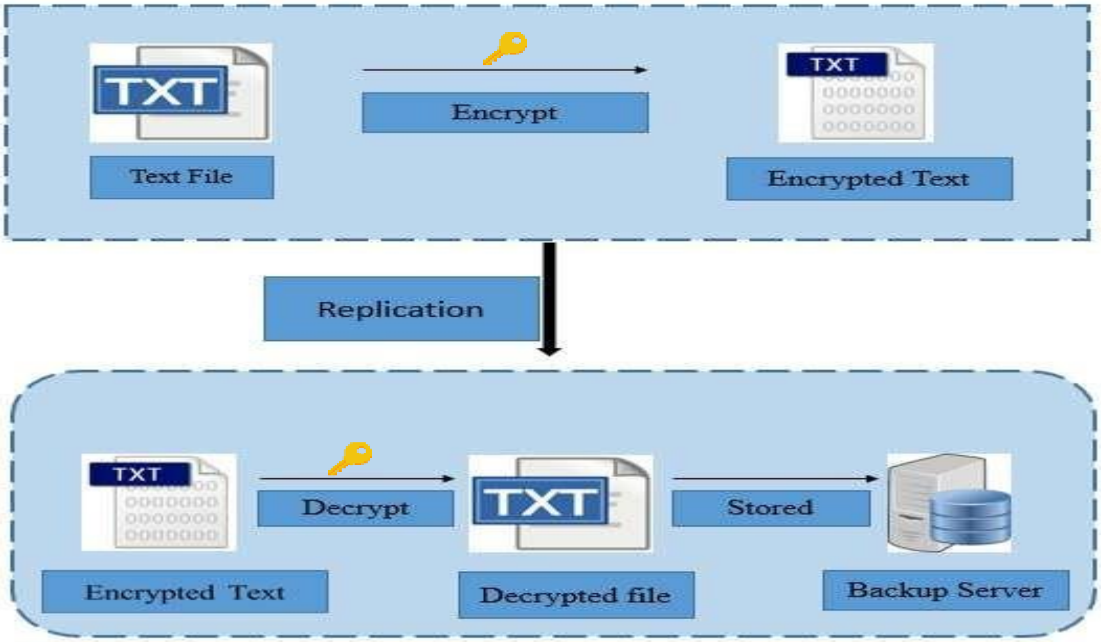


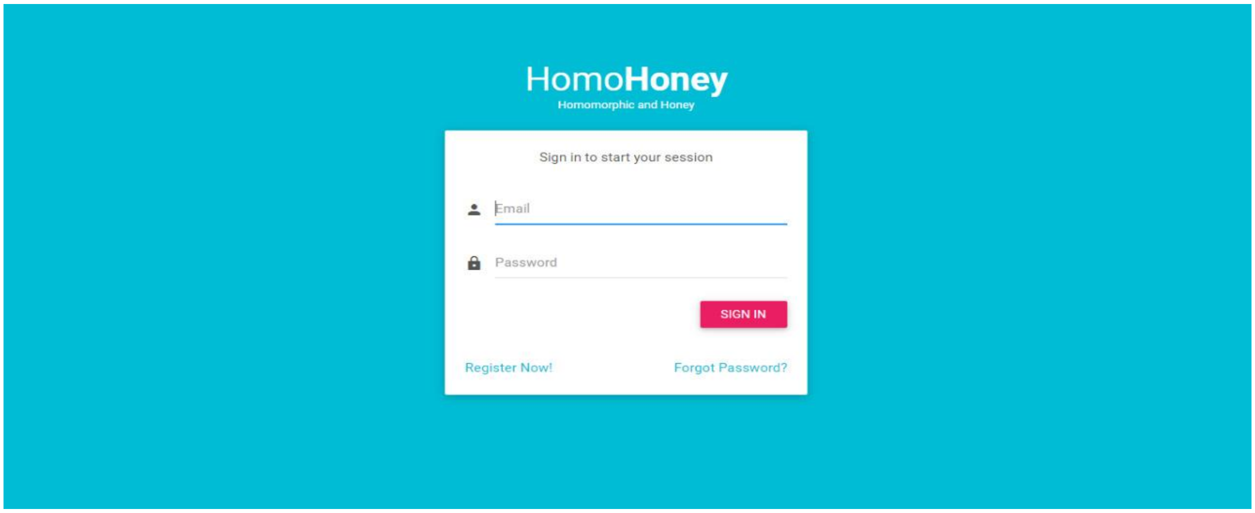
Figure 3.2.2

In figure 3.2.2, show that employee data which are located at database table in database server need to encrypt. After that, send the encrypt data to the database server (slave) which is also known as backup server. Data encryption must change to decrypt first. This is because decryption of data is a one way to make the data information as human-readable. Thus, they can be read and people will be understanding the data all about. The process of encryption and decryption of data replication are using the same key.

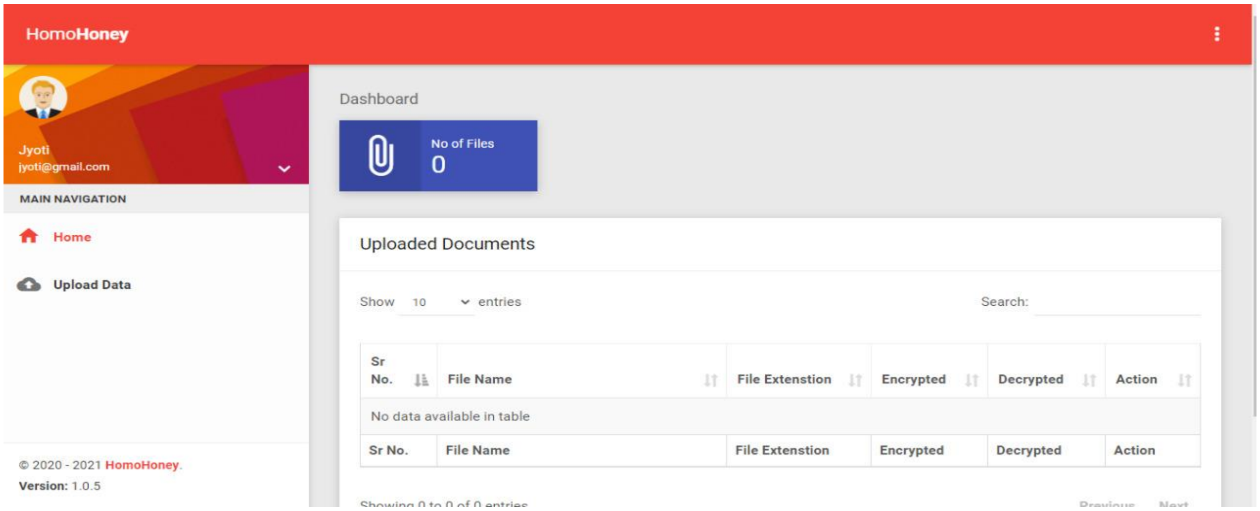
```
1.  Start
2.      Select text file from database
3.      Encrypt text file (for first 9 round)
4.              Perform XOR operation with sub key for encryption
5.              Divide input bit into 4 parts
6.                      Byte substitution
7.              Shifting rows is a simple byte transposition
8.              Mix the data with a column of static key
9.              Perform XOR operation with sub key
10.     At last round mix column will not involved
11.     Data send to the slave server (backup)
```

implementation of algorithm in this data replication is AES algorithm. AES is a symmetric block cipher which used same key for encryption and decryption process. Most of the AES encryption use same block bits which 128 bits. But, it depends of us to use other key length like 192 bits and 256 bits. It is important to use AES encryption in both software and hardware. Form figure 3.2.2 shows the algorithm used in this project which is AES encryption

4. RESULT



Sign in to start your session



Uploaded Documents

Sr No.	File Name	File Extenstion	Encrypted	Decrypted	Action
No data available in table					
Sr No.	File Name	File Extenstion	Encrypted	Decrypted	Action

Showing 0 to 0 of 0 entries

© 2020 - 2021 HomoHoney.
Version: 1.0.5

5. CONCLUSION

As a conclusion, hopefully that this project can be upgraded using the suggestion method or other suitable method that can increase the availability of the data. Besides, this project can be improved with the solution to the situation and focus more on big data. This is because the real world now requires the replicating of data in financing or banking. The cryptographic algorithm, Advance Encryption Standard (AES) had been proposed and used in this project. Data replication is more secured by using AES as AES provides a strong level of security. To prevent the data sent through the unsecured channel, data encryption is very useful. Encryption turns the readable data into unreadable form. Data becomes useless since people do not understand. To retrieve the encrypted data, user must have the key to perform decryption.

6. REFERENCES

[1] William Stallings, Principles and Practice of Cryptography and Network Security, seventh edition, 2017.

[2] Beg, A.H., Noraziah, A.A.Abdulla, A.N., and Rabbi, K.F., Framework of Resistance layer synchronous replication to increase data availability in a heterogeneous system, international journal of computer theory and engineering, 5(4), 611, 2013.

[3] Nidhi Singhal and J.P.S.Raina, Comparative analysis AES and RC4 for better Utilization, International Journal of Computer Trends and Technology, July to Aug Issue 2011.

[4] M.Pitchaiah, Philemon Daniel and Praveen, Implementation of Advanced Encryption Standard (AES) Algorithm, International Journal of Scientific & Engineering Research Volume 3, Issue 3, March, 2012.

[5] Nishtha Mathura and Rajesh Bansodeb, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, 7th International Conference on Communication, Computing and Virtualization, 2016.

[6] Manju Suresh and Neema M, 4 Hardware implementation of Blowfish algorithm for the secure data Transmission in Internet of Things, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, RAEREST, 2016.

[7] S.Suganya and R.Kalaiselvan, An Optimization and Security of Data Replication in Cloud Using Advanced Encryption algorithm, International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 5 Issues, 6 June 2016.

[8] Amandeep Kaur and Sarpreet Singh, Improved Storage Security Scheme using RSA & Twofish algorithm at Window Azure Cloud, International Journal of Computer Trends and Technology (IJCTT), volume 4 Issue, July 2013.

[9] Sumalatha Potteti and Namita Parati, Secured Data Transfer for Cloud Using Blowfish algorithm, International Journal of Soft Computing and Artificial Intelligence, ISSN: 2321-404X, Volume-3, Issue-2, and November, 2015.