Cloud Computing Security Solution Based On Fully Homomorphic Encryption.

Jadhav Aishwarya [1] , Ilhe Nikita [2] , Gagare Leena [3] , Bhalerao Rahul [4] , Prof. Sachin Thanekar [5]

[1]B.E. Comp, Savitribai phule pune university, AVCOE, Sangamner, India
[2]B.E. Comp, Savitribai phule pune university, AVCOE, Sangamner, India
[3]B.E. Comp, Savitribai phule pune university, AVCOE, Sangamner, India
[4]B.E. Comp, Savitribai phule pune university, AVCOE, Sangamner, India
[5]Asst . Prof. M.E Comp, Savitribai phule pune university, AVCOE, Sangamner, India

ABSTRACT

Computing is an emerging trend in the modern world of computing. Because of its rapid development its become more popular. Due to its popularity number of users deposit their data, their applications on the cloud that means rate of accessing cloud services is greater. But its popularity, its uses improvement is hindered by the security issue. Cloud doesn't provide more security for its services and storage purpose. So there is a need to develop such a techniques which increases the security level of cloud. The encryption of data which is stored in remotely fill the security gap between this. To solve the problems of data security in cloud computing system, by introducing fully homomorphism encryption algorithm in the cloud computing data security for encryption purpose. The proposed homomorphic encryption system helps to store the data on cloud computing. And in the cloud storage their data is still safe also check for the users privileges . All cloud operations should be done according to the rights provided by the cloud admin. In proposed system on cloud computing perform encryption on data which take as an inputs and processing is done without knowing their contents and this data is retrieved by performing decryption only for authorized users by checking their privilege. In our system, we establish security precautions in worm containment and intrusion detection against virus, worm, and distributed DoS (DDoS) attacks. We also deploy mechanisms to prevent online piracy and copyright violations of digital contents.

Keyword- *Cloud Computing ,Homomorphic Encryption, Security Issues*

1.INTRODUCTION

Cloud Computing is the new era in the world of development . For delivering IT services Cloud is a broad solution. Cloud computing is a technology based on an internet that uses the internet & central remote servers to support both stored data and applications. It allows consumers and businesses to approach their personal files at any computer with internet access and use without its installation. Cloud computing also provided shared resources like electricity which is distributed on the electrical grid. Before implementation of cloud computing, websites and server based applications were executed on a particular specified system. The main function of cloud computing is its flexibility. Flexibility is a function of cloud computing, the allocation of resources on authority's request, and it also provide the act of uniting. A cloud is a pattern of parallel and distributed computing system, which make combination of both a collection of interconnected and virtualized computers that stipulate dynamically and presented as different computing resources built on service level agreements found amongst negotiation between the service supplier and consumer. By using different resources it uses remote services through a network. It is basically meant to give maximum resources with the minimum resources.

User end using the maximum capability of computing even though having the minimum hardware requirements. This is achieved only through this technology which requires and utilizes its resources in the better way. The cloud computing is closely related with this services such as Information as a service (IaaS), Platform as a

service (PaaS), Software as service (SaaS) all of which means a service-oriented architecture. There are different benefits of cloud computing i.e. it minimize the cost of hardware which is used at user end. As therefore there is no need to store data at user's end because it is already stored at different location. So there is no need to buy the whole infrastructure required to implement the processes or execute services, instead of only pay for those what you need, according to your requirement. Same idea is applied for all cloud networks.

In Cloud Computing there are two actors, cloud provider and cloud user. Cloud provider is an enterprise vendoring cloud services. A cloud user can vary from one to another that is from organisations, educational institutes to individuals for utilizing the services of a cloud. There is a need for security, confidentiality and visibility with respect to the current cloud providers. For only Providing services such as Infrastructure as Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) is not sufficient if the cloud Provider doesn't give any assurity for a better security and confidentiality of customer data. Cloud providers such as: IBM, Google and Amazon use the technique of virtualization in their cloud platform, and in the same machine can coexist the storage space for their data and treatment virtualized which belong to the same enterprises. The fact of security and confidentiality must intervene in order to protect the data from each of the enterprises.

2. SECURITY ISSUES

Cloud is categorized into two i.e. in Public Cloud and Private Cloud. In Public Cloud services is accessible for all users who is authorized where as in Private Cloud services are accessible only for those users whose having their privileges. The security ensures to encrypt the data stored. Also its become very easy to perform secure transmission from a local machine to a cloud data store. The encryption is then performed on data which is stored on cloud and the channel of data transmission well secured with exchange of keys. For performing computations on that stored data in the cloud requires decryption first; this makes critical data available to the cloud provider. Data Mining and Data Analysis onto the Database which is encrypted is a far different things to get by using available encryption standards. The proposal is perform encryption on data before sending to the cloud providers. For enabling a cloud computing vendor in order to perform computations on clients' data at their request, such as analyzing sales patterns, without exposing the original data. To achieve this it is also necessary to hold the cryptosystems which is based on Homomorphic Encryption either a Fully Homomorphic Encryption (FHE) or Somewhat Homomorphic Encryption (SHE).

2.1 Security Issue

The cloud service provider for cloud makes sure that the user does not face any problem such as data loss or data theft. There is also a possibility where a malicious user can penetrate the cloud, there by infecting the whole infrastructure of cloud. This affects on number of users who are accessing the services and sharing the resources of the infected cloud. There are five different types of issues are form at the issue of security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues

2.2 Homomorphic Encryption

In the cloud computing their is need of security for data. The data which we stored on cloud is not fully secure and that data can be getting hack by the hackers very easily. Hence we provide our own security mechanism for that data. Homomorphic encryption is technique which is used for security purpose. In homomorphic encryption different operations are performed on the encrypted data to make it more secure.

The operations are carried out without knowing the private key. Client is the only holder of the secrete key. Homomorphic encryption is a technique of encryption that allows computations to be carried out on ciphertext, hence that generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

There are two type of homomorphic encryption techniques.

1.Partially Homomorphic encryption.
2.Fully Homomorphic encryption.

Also there are several partially homomorphic encryption methods and also a number of fully homomorphic encryption methods.

1. ***Partially homomorphic encryption :***
In partially homomorphic technique, operations are performed on the encrypted data. These operations either additive or multiplicative operation, but not both operation can be carried out at a same time.
RSA - multiplicative homomorphism
ElGamal- multiplicative homomorphism
Paillier - additive homomorphism

2. ***Fully Homomorphic encryption***
In this case, both operations can be carried out at same time. Due to this security mechanism for encrypted data is improved.
The first (and currently only) such system is a lattice-based encrypted system developed by Craig Gentry in 2009. Fully homomorphic encryption (FHE) and is more powerful technique.

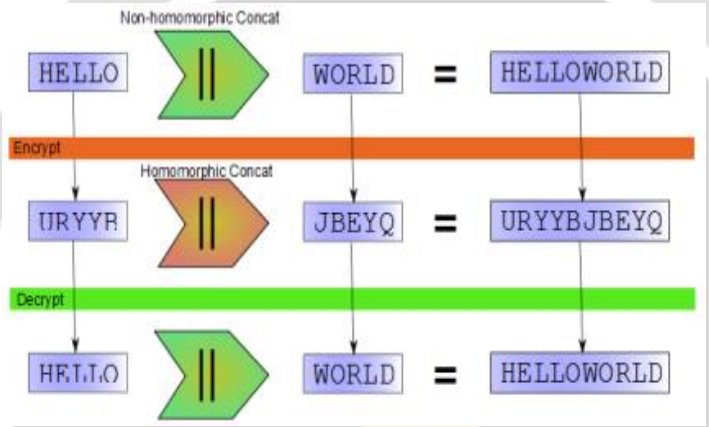


Fig 1. Homomorphic Encryption – rot-13

The popular cipher scheme is ”rot-13” in the homomorphic encryption technique. Replace each english letter with one 13 placed forward or back along with alphabet. Here the ”Secret key” will be 13. Major advantage of rot-13 over rot(N) is ,it is self inverse,so that same code can be use for encoding decoding. Finally decrypt the data.

var c1=Encrypt(13,”HELLO”); //c1=URYYB

var c2=Encrypt(13,”WORLD”); //c1=JBEYQ

var c3=Concat(c1,c2); //c1=URYYBJBEYQ

var p=Decrypt(13,13); //p=HELLOWORLD

In order to protect data which is available or stored on cloud different security mechanisms are invented, An Encryption is one of them. Encryption is a well known technology which is applied on cloud to increase the security level for data stored on cloud. Encryption is achieved by implementing different algorithms like: DES algorithm, RSA algorithm etc.

3. EXISTING SYSTEM

In order to protect data which is available or stored on cloud different security mechanisms are invented, An Encryption is one of them. Encryption is a well known technology which is applied on cloud to increase the security level for data stored on cloud. Encryption is achieved by implementing different algorithms like : DES algorithm, RSA algorithm etc.

3.1 Implementing RSA algorithm for data security

P. Kalpana, S. Singaraju have designed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm use to encrypt the data to provide security so that only the authorized user can access it. The purpose of securing data, unauthorized users does not allow. User data encryption is first perform and then it is stored in the Cloud. When required, user sent a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of both keys, Public-Key and Private-Key. In the proposed Cloud environment, Pubic-Key is known to all, whereas Private Key is known only to the user who is data owner.

Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only. These both algorithms provide security as much more level but although there is a necessity to increase the security level for whole infrastructure on Cloud. At the user level, one needs to perform trust negotiation and reputation aggregation over all users. At the application end, we need to establish security precautions in worm containment and intrusion detection against virus, worm, and distributed DoS (DDoS) attacks. We also need to deploy mechanisms to prevent online piracy and copyright violations of digital content. So to solve such problems a new encryption technique is design to maintain security and for protection of data from different malicious users.

3.2 Implementing AES algorithm for data security

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The block and key can in fact be chosen independently from 128,160,192,224,256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys-128,192,256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is not structure.

The four stages of the AES algorithm are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

4. PROPOSED SYSTEM

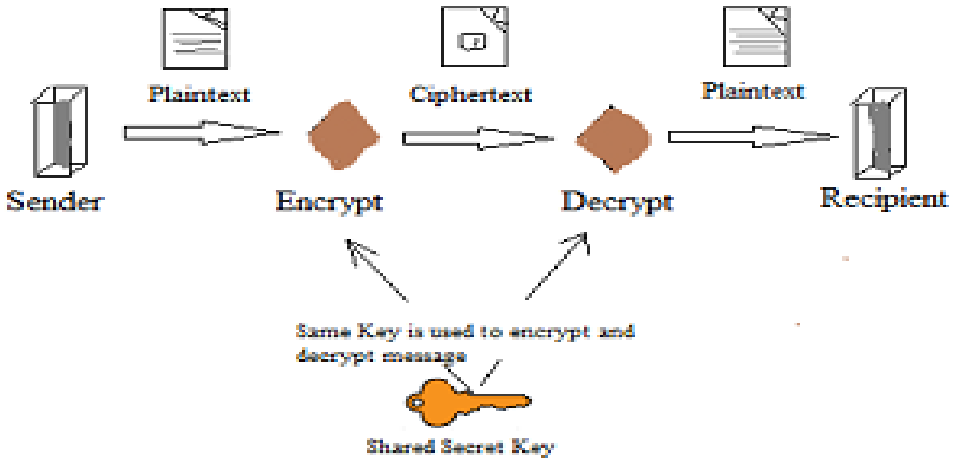


Fig.2. Flow Of Proposed System

Encryption is one of the a well known technology for protecting sensitive data present in a cloud. Due to encryption data is convert in such a form where any one user can not easily access it until taking its permission. For performing encryption different keys are used. By using the combination of both Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval for the purpose of maintaining security on cloud.

Implementing Homomorphic Algorithm in Cloud for Data Security

Maha TEBAA have proposed an application to execute operations on encrypted data without decrypting them which will provide the same results after calculations that means worked directly on the raw data. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption) the client is the only holder of the secret key. When the author decrypts the result of any operation, it is the same as if they had carried out the calculation on the raw data.

In this system Homomorphic encryption which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of confidentiality of data. The proposed work is based on the application of fully homomorphic encryption to the cloud computing security considering the analyse and the improvement of the existing crypto systems to allow servers to perform various operations requested by the client. The improvement of the complexity of the homomorphic encryption algorithms and compare the response time of the requests to the length of the public key.

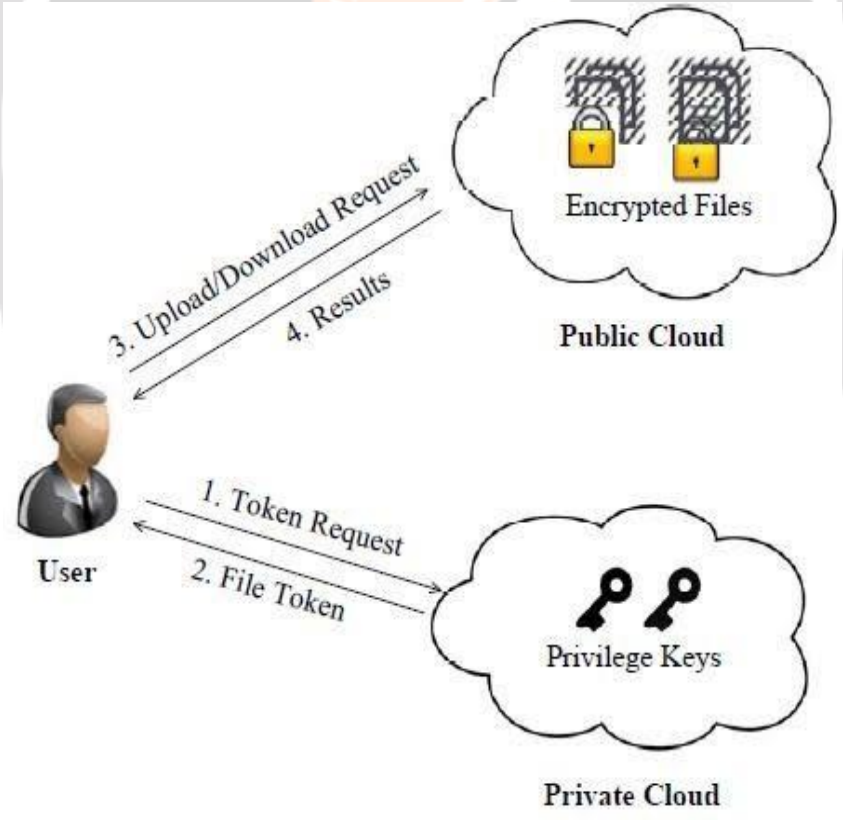
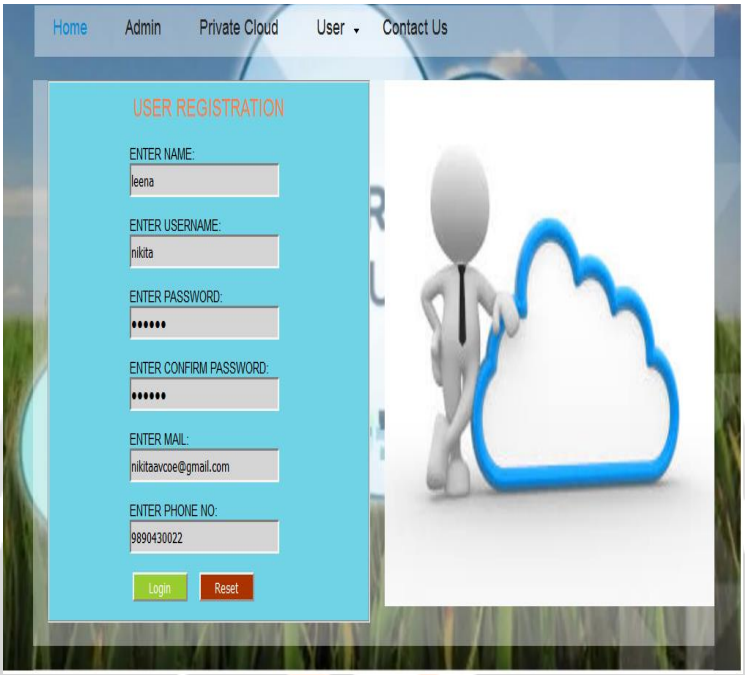
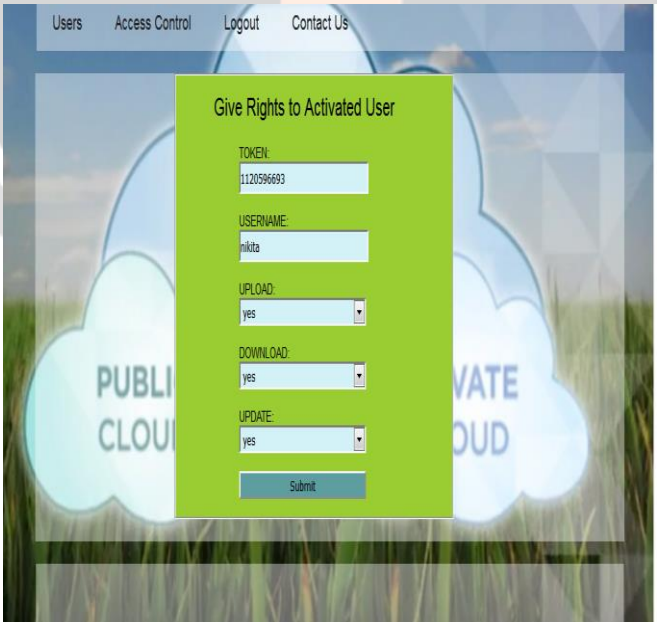


Fig 3. System Architecture

5. IMPLEMENTATION





6. CONCLUSIONS

In cloud computing Security is a major concern. For protecting data on cloud we proposed a system which aims is to increase the security level on cloud. The cloud computing security based on fully homomorphic encryption, is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. Our work is based on the application of fully homomorphic encryption to the security of cloud computing. Based on the cloud data security problem faced, this system introduced the homomorphic encryption mechanism, proposes a cloud computing data security scheme. The scheme ensures the transmission data between the cloud and the user safety. And in the cloud storage their data is still safe. It is convenient for users and the third party agency to search date to dispose. At present, fully homomorphic encryption scheme has high computation problem needs further study.Criticism kept us working to make this project in a much better way. Working under him was an extremely knowledgeable experience for us.

7. REFERENCES

[1] Dan Boneh et al. "Evaluating 2-DNF formulas on ciphertexts. In Theory of Cryptography," Conference,TCC'2005, volume 3378 of Lecture Notes in Computer Science,pages 325-341. Springer, 2005.
[2] Furht,B., and Escalante, A. "Handbook of Cloud Computing,"http://search cloudcomputing.techtarget.com/definition /private-cloud, Springer, 2006.
[3] Kevin Hamlen, et al., International Journal of Information Security and Privacy, 4(2), p.p(39-51), April-June 2010.
[4] C.N. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl (2011) .
[5] VAMSEE KRISHNA YARLAGADDA and SRIRAM RAMANUJAM, "Data Security in Cloud Computing", Vol.2 (1), p.p (15-23) (2011).
[6] F.A.Alvi, B.S.Choudary, N.Jaferry, "Review on cloud computing security issues & challenges", iaesjournal.com, vol (2) (2012).
[7] Priyanka Arora, et al. ,"Evaluation and Comparison of Security Issues on Cloud Computing Environment", (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, p.p (179-183), 2012.
[8] Prince jain, "security issues and their solution in cloud computing ", International journal of computing & business research, ISSN (online):2229-6166.
[9] Rohit Bhadauria, et al.," A Survey on Security Issues in Cloud Computing". IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
[10] Sara Qaisar and Kausar Fiaz Khawaja," CLOUD COMPUTING:NETWORK/SECURITY THREATS AND COUNTERMEASURES", ijcrb, JANUARY 2012 VOL 3, NO 9.
[11] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.
[12] Vic (J.R.) Winkler, "Securing the Cloud, Cloud Computer Security,Techniques and Tactics", Elsevier, 2011.

8. BIOGRAPHI

SR.No	Authors's Photo	Author's Profile
1		Aishwarya Jadhav received the B.E. degree in computer Engineering from Amrutvahini college of Engineering , Sangamner(MS) ,Savitribai Phule Pune University,India in the year 2016.Her current research interest include cloud computing and its Security.
2		Nikita Ilhe received the B.E. degree in computer Engineering from Amrutvahini college of Engineering , Sangamner(MS), Savitribai Phule Pune University, India in the year 2016. Her current research interest include cloud computing and its Security.
3		Leena Gagare received the B.E. degree in computer Engineering from Amrutvahini college of Engineering , Sangamner(MS),Savitribai Phule Pune University, India in the year 2016.Her current research interest include cloud computing and Encryption Schema.
4		Rahul Bhalerao received the B.E. degree in computer Engineering from Amrutvahini college of Engineering , Sangamner(MS), Savitribai Phule Pune University, India in the year 2016.He mainly engaged in cloud computing. He has completed his diploma in Computer Technology in Mumbai University, India.