ENHANCED ENCRYPTION APPROACH FOR DATA SECURITY AND USER VALIDATION USING AES AND BLOWFISH ALGORITHM IN CLOUD ENVIRONMENT

[1]RAJNI KUMARI, [2]ANUPAMA GUPTA, [3]KAUR BALDIP

[1]Computer Science and Engineering Department CT Group of Institutions, Shahpur Campus, Punjab,India
[2]Computer Science and Engineering GZSCCET, Punjab,India
[3]Computer Science and Engineering Department LLRIET, MOGA,Punjab,India
E-mail: [1]rjni786@gmail.com, [3]baldip20@gmail.com

Abstract - Cloud computing is a process that enables its users to access numerous services which are Saas, Paas and Iaas. Many of the individuals who use the framework to offer their services to different users usually try to manipulate and manage their data. One of the challenges in cloud computing is that the data that has been accessed with the aid of different resources need the access of the user on the access control model purposely for the integrated management. The issue of security has been of major concern in cloud computing and due to this, many researchers have decided to pursue the topic in detail. Numerous security issues come up as a result of outlining the importance of cloud computing.

Keywords - Cloud Computing, Security, OTP, Saas, Paas, Iaas.

I. INTRODUCTION

Cloud computing is primarily used to offer many services and also act as a platform for computer applications. The services that are provided by cloud computing has been used in several fields such as personal and business purposes. In many times the individuals who are using the cloud computing do not have the knowledge of where the software is located as well as its properties. In our case, the data that is used has been stored in a form that can be processed through the internet. Cloud computing examples include; web mails, social network sites, online business application and many cloud storage applications. The amount of information from each work area or from various gadgets is normally put aside in distributed computing because the information cannot be found on the web. The use of cloud computing does not put into consideration the handling that has been made for the end user level that all is in line with the happenings that the utilization information of the applications for mainly customer loyalty and developing of associations.

1.1 Deployment of cloud services

Many of the cloud services that can be used arise from different cloud practices. The services are beneficial from the private cloud, community cloud, public cloud, and hybrid cloud. The communication, email services and the online media storage services which are some of the cloud providers operate and provide services through the public cloud. Different services which can be found on enterprises can be utilized by the public cloud. Some of the cloud deployment models include:

1.1.1 Public Cloud: This type of cloud is mainly used by different services by use of various resources which can be found in different locations. The services have been offered by the third-party providers that are rated by checking their quality and the number of individuals using them.

1.1.2 Community Cloud: This is a type of cloud that is used by different organizations that need a framework which is the same. They normally use it in putting in order their products. The model requires the companies to develop a strategy that allows them to share their resources. Even though community cloud is expensive than public cloud, it provides high security, better services and privacy for the individuals who use it.

1.1.3 Hybrid Cloud: The cloud involves the use of services that have been provided by two different clouds but for the purpose of serving a single company. Hybrid cloud involves the combination of two cloud to perform the required services. There is the bringing together of both the public and the private could form a single cloud that can be used to render better services. The cloud is primarily used so as the virtual cloud services can be deployed on the physical hardware units.

1.1.4 Private Cloud: This type of cloud is mainly used by large firms that need high security and data storage for the different applications of the firm. The cloud is mainly custom made to fit the requirements of the company that is using it. The software and the hardware of the cloud can be upgraded or degraded to fit the demands of the organization.

1.2 Challenges in Cloud Computing: The performance of cloud computing can be affected by numerous challenges. Some of the challenges are:

a. availability
b. data security and integrity
c. complexity

d. authentication and Validation

1.3 Major Risks of cloud computing security:

Cloud computing is a large network that is used in carrying out various cloud services. There are different users who use the cloud services. Cloud computing has different security problems such as application security, data availability and integrity authentication and validation and data encryption. Since cloud computing can be accessed remotely by use of the internet, security issues arise that put in danger the cloud resources up to the extent that the integrity and authentication are questioned. The issue of security in cloud computing is something that is new and due to this, a lot of research can be done so as to provide the best security for the framework. The following are cloud computing issues in security;

i. Data Integrity
ii. Proper usage metering
iii. Abusing the cloud's resources
iv. Security attacks
v. Cloud Services Availability
vi. Legal and Regulatory Risks
vii. Data Leakage and data security

1.4 Important Security Issues in the Cloud:

The development in technology has made it easier for many service providers to attract more customers by use of various resources making them to easily get their information from anywhere by use of the internet. Cloud computing is the best place where users can find the best services. Due to the high-security risks that are associated with cloud service, many users fear using the platform. Some of the security issues that are linked with cloud data include;

Integrity: one of the major factors that play an important role in data storage in the cloud service is integrity. The main purpose of the integrity in cloud service is to ensure that data which is sent from the cloud storage is not corrupted in any manner. This means that no alterations have been made on the data by an individual who has not been authorized. Since there can be a system failure, the data that has been worked on can be stored in a portable gadget which makes its retrieval easy.

Availability: the main role of availability is to make sure that any resources that have been used in cloud computing can be utilized for the services and ensures that there are not attacks. This means that when an individual who uses the system tries to get any information from the cloud server, it must be available for it to be accessed.

Confidentiality: the main role of confidentiality is to make sure that data is not accessed by unauthorized individuals. In situations where unauthorized people can have access to information then confidentiality would have been lost. This can manifest itself either electronically or physically. Social engineering is the main way through which physical confidentiality can occur. In circumstances where the customers and any other users do not encrypt their communications, electronic confidentiality occurs.

II. REVIEW LITERATURE

2.1. Jongo Mun et al,[1] "An Improvement of User Authentication Framework for Cloud Computing" one of the most recent innovation give the various administrations to the customers by use of the internet is cloud computing. The users have the ability to store and even access their data from any location in the world through the internet. This study tries to show an approach that can be used to give security to cloud services by use of customer confirmation model. User authentication has been given by taking into consideration the cryptography model that involves different mathematical formulas with an aim of ensuring that the information of the person using the software cannot be accessed easily. According to the author of the paper, user authentication gives a high security.

2.2.Ahmed Dheyaa Basha et al [2] "Mobile Applications as Cloud Computing: Implementation and Challenge" since cloud computing and other versatile application have been linked with each other, various administrations that are related to cloud condition can be used by use of the portable application. There are many portable applications that are used mainly for cloud security. The paper outlines the administrations in detail. Also, various types of challenges have been dealt with in this paper.

2.3 Uma Somani et al. [3] The author shows how the individuals who use cloud computing have the validity of using different cloud computing services which can be found in the cloud environment. The main aim of this is to ensure that cloud services are utilized in the best manner. Some of the programming issues and those of different equipment have been solved by cloud computing. Also, the problem of pilling of stock in various organizations has been solved by cloud computing. This study outlines how the issue of information stockpiling has been handled by the use of the encryption model. This is done with the main aim of ensuring that the information that has been put away in the distributed location is done in a scrambled manner. Putting away of information through scrambling utilizes the computer signature calculations and mostly the Rivest, Adi Shamir (RSA) calculation. According to the calculations, utilization of hashing has been done with the aim of 0-changing the information by taking into consideration 128- piece key. Other 16-sub keys have been created from the 128-piece key which is used to change plain information to figure information. This creates an arrangement that offers

the best security for the information that has been moved from the cloud storage.

2.4 Ru Wei Huang et al. [4] "Design of Privacy-Preserving Cloud Storage Framework" proposed Privacy security is a key issue for distributed storage. Encryption is an entrenched innovation for ensuring delicate information. Be that as it may, it gives some new issues: how information proprietor and capacity specialist organization to work on encoded information? How to decrease information proprietor's outstanding task at hand of information administration and bolster information sharing in the meantime?

In the event that they can't be anything but difficult to settled, encryption will convey a great deal of inconveniences to individuals. In this paper, we structure a security safeguarding distributed storage system to tackle those issues. We plan a communication convention among members, receive key inference calculation to create and oversee keys, utilize the mix of symmetric and lopsided encryption to shroud the touchy information of clients, and apply Bloom channel to acknowledge figure content recovery.

A framework dependent on the structure is figured it out. The paper breaks down the achievability of the structure from the execution of Bloom channel, the running overhead of the framework and the protection security of the system.

2.5 Farzad Sabahi. Et al [6] "Research on Privacy-Preserving Cloud Storage Framework Supporting Cipher Text Retrieval" The author of this study tries to give more information on the problem of stockpiling mainly in the distributed computing stockpiling. Security plays an important role in cloud computing because of the capacity of information from all across the world. The author of this study shows various problems that have been experienced by clients who have decided to transform their businesses' information to cloud foundation. Some of the security problems that have been handled in this paper include; assaults, trustworthiness and accessibility. The writer of the paper outline various ways that can be used to deal with the identified security issues. According to the plan of handling the issues, information security has the ability to accommodate media that has been stored in cloud servers. .

III. RESEARCH METHODOLGY

In this section, cloud computing save channel has been utilized specifically for the user and data verification. There are numerous stages that have been developed to help in user registration in cloud computing. The hybrid credential is used in processing the personal information of users during the registration procedure. The credential has been stored in the system so that it can be processed later by use of the hybrid encryption model. Each user is given a confidential key to ensuring that the information is not accessed by unauthorized people.

The initialization of user login is completed after the registration process. Initialization of the user's login is done through the verification of the one-time key validation procedure. The login of the user's credentials has a secret key which is given to the user. The use of the key verifies the user and the one-time key is sent for verification. When the login process is over, the information that has been stored by the user on the distributed storage has been moved and the information has been encoded which is one way of encryption. The main aim of doing the entire process is to ensure that there is a high level of information privacy.

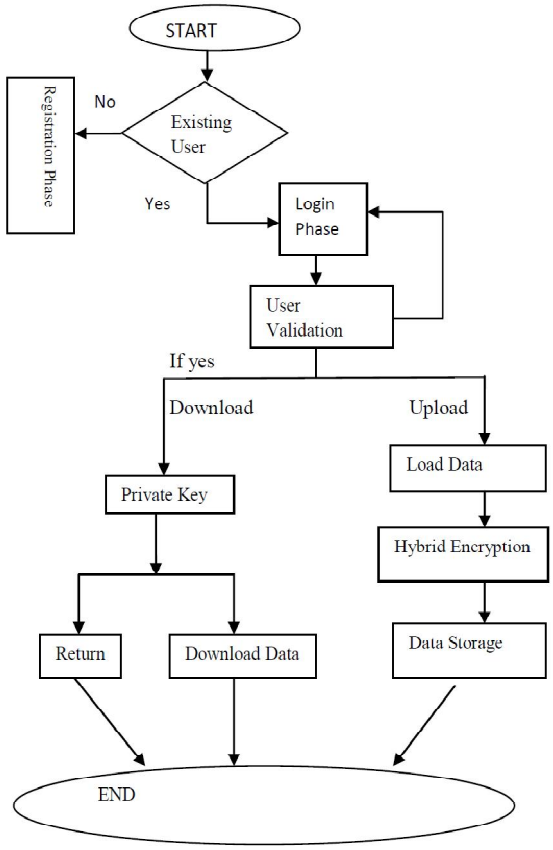


Fig3.1. Flowchart of Proposed Work

IV. RESULTS AND DISCUSSION

Table 1: Computation time for encryption of different size files.

Sr, No	Files (in bytes)	Fully Homomorphism	DES
	Time	(In ms)	
1	2681	132	118
2	3431	165	142
3	4386	285	256
4	5546	365	343
5	22588	606	555

The table below shows the value for computation duration pf various size files. Fully homomorphism and DES encryption models have been evaluated for the computation time for the intended job.

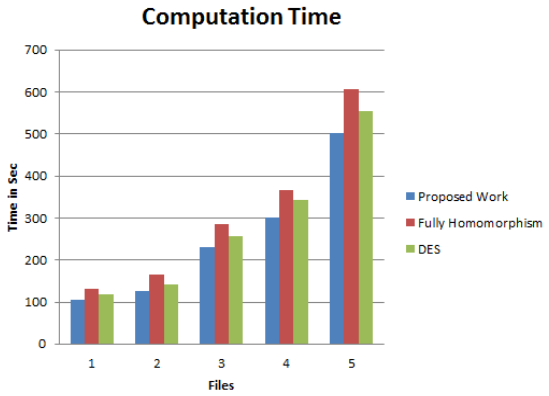


Fig.4.2.Compression graph for computation time for encryption

The above figure is a comparison graph for the computation time of the intended approach and fully homomorphism and DES model.

Table2: Compressed File Size after compression of data of various sizes

Sr, No.	Files (in bytes)	Proposed Work	Huffman Coding	RLE
		Compressed files size (In bytes)		
1	2681	1910	2346	2576
2	3431	2430	2995	3068
3	4386	3230	3964	4018
4	5546	4168	4864	5264
5	22588	14044	17048	19428

The table above is a representation of the value of the compressed files for the encryption of various size of files. The compressed values were evaluated mainly for work and fully homomorphism and DES encryption model.

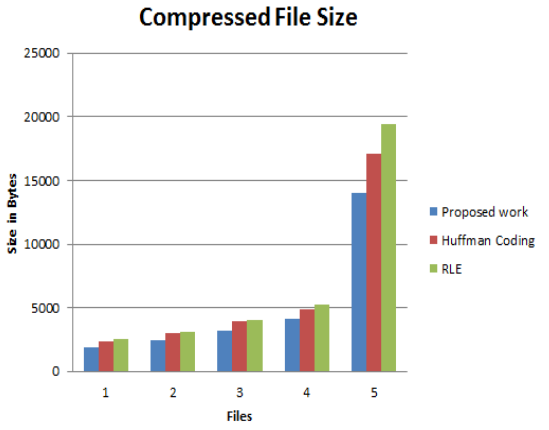


Fig 4.3 Comparison graph for compression file size after compression.

The figure above is a representation of the comparison graph for compressed file size by using proposed approach and Huffman coding and RLE compression model.

CONCLUSIONS

1. Data storage has been done on the cloud for the given work. Each user has been given a different name and different email ID for security purposes. The request by the user to access the system is transmitted to the cloud whereby the secret key is sent by the cloud to the individual using the system and if it is verified, then the user has the ability to access the account. After login, the user can use the hybrid encryption to securely store data in the cloud.
2. The hybrid encryption deployed is that of the arithmetic and logarithmic formula which is necessary for encryption/ description process of any data which is removed from the confidential information to the cipher text.
3. Security of data is ensured by these operations since they lack key operations which are moved to the individual using the system.
4. The detailed work makes it possible for the storage of data in the cloud. The work also has the ability to minimize the storage capacity of data. Performance evaluation has been made possible by purposed work, encryption size and the time of computation.
5. The proposed project uses fully homomorphism and DES approach to provide 15% efficiency compared to the work that has been done before.

FUTURE WORK

This can be made possible by implementing encryption and future reference for the best security of data in the cloud. This project which is to be done by efficiently utilizing the cloud environment.

REFERENCES

[1] Jongho Mun, Jiye Kim, Dongho Won “An Improvement of User Authentication Framework for Cloud Computing”, Journal of Computers, December 15, 2015, pp 446-454.

[2] Ahmed Dheyaa Basha, Irfan Naufal Umar, and Merza Abbas, Member, IACSIT “Mobile Applications as Cloud Computing: Implementation and Challenge”, pp. 7865-7564, IEEE, 2013.

[3] Uma Somani, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[4] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, “Research on Privacy-Preserving Cloud Storage Framework Supporting Cipher text Retrieval" 2011 Ninth International Conference on Grid and Cloud Computing.

[5] Farzad Sabahi, “Cloud Computing Security Threats and Responses," IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp. 670 { 684, 2002.}

[6] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.
[7] Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth "A Layered Security Approach for Cloud Computing Infrastructure" 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. © 2009 IEEE.
[8] Jianfeng Yang, Zhibin Chen "Cloud Computing Research and Security Issues" Vol. 978-1-4244-5392-4/10/$26.00 ©2010 IEEE
[9] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh "Personal Cloud Computing Security Framework" 2010 IEEE Asia-Pacific Services Computing Conference.
[10] Mohammed Achemlal, Sa ıd Gharoutand Chrystel Gaber "Trusted Platform Module as an Enabler for Security in Cloud Computing", Vol 978-1-4577-0737-7/11/$26.00 ©2011 IEEE.
[11] Yong Pan "Research on dependability of cloud computing systems" IEEE Conf. on Reliability, Maintainability and Safety (ICRMS), 2014 ,pp. 435 – 439.
[12] Idris, A.S. "The readiness of Cloud Computing: A case study in Politeknik Sultan Salahuddin Abdul Aziz Shah, Shah Alam" IEEE Conf. on Computational Science and Technology (ICCST), 2014, pp. 1 – 5.
[13] Shaikh, F.B. "Security threats in cloud computing" IEEE Conf. on Internet Technology and Secured Transactions (ICITST), 2011, pp. 214 – 219.
[14] Almorsy, M. "Collaboration-Based Cloud Computing Security Management Framework" IEEE Conf. on Cloud Computing (CLOUD), 2011, pp. 364 – 371.

★★★