IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN EFFICIENT FRAMEWORK FOR SECURED DATA MIGRATION IN HYBRID CLOUD COMPUTING ENVIRONMENT

MARIA KIRAN L[1], ***PREETHI S***[2]

PG Scholar[1], Associate Professor[2]
Dept. of Computer Science and Engineering[1],
Dept. of Information Science and Engineering[2],
Cambridge Institute of Technology, Bangalore, India

ABSTRACT

Cloud computing is a new paradigm that combines several computing concepts and technologies of the Internet creating a platform for more agile and cost-effective business applications and IT infrastructure. This is advantageous in several applications. One of the most popular services of cloud computing is data outsourcing, which is constantly carried out to hybrid or public cloud. For reasons of cost and convenience, as many large enterprises such as personal health records, emails, income tax and financial reports move their business-critical data and applications to the cloud and enjoy the benefits of remote storage and management. But the confidentiality and security of data is being the major concern. In this paper, we provide a data security analysis and solution for privacy protection framework during data migration. A Secure Socket Layer (SSL) is established with the AWS cloud services and a migration ticket with minimum privilege is introduced. Further, data encryption is done using Prediction Based Encryption (PBE) where the ticket holds the ID and the password for encryption process and the password should match for the decryption process to retrieve the source file from cloud environment.

Keywords **- AWS (Amazon Web Service), SSL (Secure Shell Layer), PBE (Password Based Encryption), SNS (Simple Notification Service) SES (Simple Email Service), GUI (Graphical User-Interface).**

I. INTRODUCTION

Cloud computing services such as Amazon EC2 and Windows Azure are becoming more and more popular but it seems many people are still unclear as to what exactly the buzzword “Cloud computing” actually means. In its simplest form, the principle of Cloud computing is the provision of computing resources via a network. Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. There are many benefits stated of Cloud Computed by different researchers which make it more preferable to be adopted by enterprises. Cloud Computing infrastructure allows enterprises to achieve more efficient use of their IT hardware and software investments. This is achieved by breaking down the physical barrier inherent in isolated systems, automating the management of the group of the systems as a single entity. Cloud Computing can also be described as ultimately virtualized system and a natural evolution for data centres which offer automated systems management [1]. Enterprises need to consider the benefits, drawbacks and the effects of Cloud Computing on their organizations and usage practices, to make decision about the adoption and use. In the enterprise, the "adoption of Cloud Computing is as much dependent on the maturity of organizational and cultural (including legislative) processes as the technology, per se" [2] Due to its huge success lot of people trying their hands-on cloud computing. There are a lot of players out there who are providing cloud services are-- Google Cloud platform, Amazon web service, Microsoft Azure, IBM Cloud, VMWARE, Digital Ocean and many more.

There are three service architectures of cloud:

1. Iaas (Infrastructure as a service): providers of IaaS offer computers—physical or (more often) virtual machines—and other resources. IaaS refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc.

2. Paas (Platform as a service): PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform including operating system, programminglanguage execution environment, database, and web server.

3. Saas (Software as a service): In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs.

A. Why Data Migration is required?

The object of an organization can be moved from the cloud to cloud or data from one cloud to another. However, this is a very challenging task for migrating data and includes various key security issues such as data integrity, security, portability, data privacy, data accuracy, etc. to achieve an automatic data migration; a programmatic data migration approach is required to get rid of the tedious tasks of a human organization.

B. Need for migrating data into the cloud

For integrating data under the various projects of the enterprise, data migration plays a key role in the field of cloud computing technology. Since business demands are growing rapidly so more and more applications are required to support these demands and for this purpose, the cost involved for running and managing the databases for applications are affecting badly due to the emerging demands. Therefore, in order to gain the benefits of cloud computing and to meet the growing demands by resolving the cost issues for integrating data for any organization, there is much need for bringing the concept of data migration into the cloud. And for this reason, cloud computing has brought its new service model as the data migration as a service (DMaaS) model.

In the simplified form, the need for migrating data into the cloud arises if merging of the computer systems is performed or is the old computer system is to be replaced by the new computer system or is upgraded to new system by the organizations. All above reasons supporting the need for data migration in the cloud are summarized below:

- If a company wants to transfer its data to another company in a thought to get better support for their requirements by another CSP.
- To gain the benefits of emerging cloud computing paradigm for meeting growing business demands.
- When the systems or accounts are to be merged by an organization after acquisition.

C. Advantages of Data Migration to Cloud

There are numerous benefits associated with data migration to the cloud. Moreover, there several organizations that are already availing the advantages of the data migration to the cloud. Some of the pros are explained in the section given below:

- Save Huge Data Storage Costs
- Flexible Scalability and Increased Collaboration
- Reliable Backup Facility
- Pay-per-user Billing
- Superior Disaster Recovery

D. Disadvantages of Data Migration to Cloud

Cloud data management has numerous advantages associated with it. Still, there are many organizations that face various cloud migration issues while moving their data to the cloud. This is due to the challenges that occur Due the data migration process. Some of the major cons of data migration are explained in the section given below

- Business Downtime
- Unexpected Initial Migration Issues
- Data Security can be Compromised
- Cloud Apps Cloud be Inflexible at Times
- Platform Dependency

E. Security Issues in Hybrid Clouds

A hybrid cloud environment consisting of multiple internal and/or external providers is a possible deployment for organizations. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud [3]. Providing security in a private cloud and a public cloud is easier, comparing with a hybrid cloud since commonly a private cloud or a public cloud only has one service provider in the cloud. Providing security in a hybrid cloud consisting of multiple service providers is much more difficult especially for key distribution and mutual authentication. Also for users to access the services in a cloud, a user digital identity is needed for the servers of the cloud to manage the access control. While in the whole cloud, there are many different kinds of clouds and each of them has its own identity management system. Thus a user who wants to access services from different clouds needs to have multiple digital identities from different clouds, which will lead to inconvenience for users. Using federated identity management, each user will have his unique digital identity and with this identity, he/she can access different services from different clouds [4]

II. LITERATURE REVIEW

In this chapter we present the result of a systematic literature review we conducted on existing research in the searchable encryption area. A systematic review is important for research activities since it summarizes existing techniques concerning a research interest and identifies further research directions. The purpose of the review described in this chapter is to compare current searchable encryption solutions and identify their limitations through a systematic evaluation.

Tamanna Narula et. Al [6], proposed framework for analysing and testing cloud based application. In this paper they proposed that software testing is the main processing of accessing functionality and correctness off a program through analysis. In software engineering related projects testing has become the challenge, especially for the major system. Because testing can be such a difficult and costly and more manpower required process.

Rashmi Rao et. Al [7], proposed improving security for data migration in cloud computing using encryption randomized technique. In this paper they proposed that with the development of the cloud computing the security of the data is becoming major concern of user. In the cloud move the data from one to another target cloud which may be a public, private and hybrid cloud. It also require to maintain the need of organization with different models of Database as a service. In this process it face some issues like integrity, security, privacy, accuracy and others. In their proposed work they created an encryption algorithm which provides security to data.

Nirav Shah Et. al [8], proposed secure data migration in cloud providing integrity and confidentiality. Cloud computing is a new feature which adds many features and application together on a platform over internet for better IT infrastructure and cost effective organization. The security has been become major issue n term of moving data of user from one machine or a server to another in the development of cloud computing. In their proposed work they created an encryption algorithm to secure the data in cloud which gives better performance and better results more than the already existing algorithm like PBE and IBE. And they conclude that cloud computing is increasing the business with high usage of data and it is helpful for the companies and other who are using the cloud services. By providing the encryption, confidentiality, integrity data can be more secure and security of data is the priority of everyone.

Dhrumil Parikh et. al [9] have proposed migrating algorithm for data security in cloud computing. In this paper they described IT firms are converted their self into the cloud based infrastructure through internet resources. And security is becoming the major concern of the companies. Transmission of data called migration which can be online or offline. Cloud computing is defined as set of resources and offered service. It conveys everything as a service over the internet based on demand of user.

Shyamli Dewan et. Al [10], proposed that cloud computing has become a future generation infrastructure for computing. Normally cloud computing is defined as a bunch of computing resources access by internet. Basically user stores their data in the cloud with firewall and other security to keep the data safe from third party or some intruders. In the cloud computing resources there are many service providers who provide the services to the user and it’s their duty to keep the data safe of the user or protect the data from unwanted access or the user can take the help from the Third party auditor to keep their data safe from the unwanted access and provide the security to their data in cloud over the internet.

Suganya .N et. al [11] proposed implementing RSA algorithm to get the data security in cloud computing. Cloud computing is an internet based technology where a good amount of resources which is shared as a services. It is a payment based model where user pay money for the cloud services. Many organizations are afraid to store their data over the internet due to negative effects of cloud. With the help of cloud computing user can access the data and application from anywhere in the world with user authentication. And many user can access the same data in cloud system. In their related work they mostly works in security of users data. In third party auditor and auditing mechanism are proposed.

Shyamli Dewan et. Al [12] proposed secure data migration across cloud system using TPA. Cloud computing is acquiring as future generation architecture of computing. Basically cloud computing is defined as a bunching of computing resources which is easily accessible via internet. Accordingly the user store their data in cloud with firewall and other security protection to make save their data from unwanted access and intruders to access the data.

Gowri et. al [13], proposed cloud computing application and their testing methodology. In this paper they proposed cloud computing provides new security to the user. These new technology create a platform for the user of the opportunity and activate the internal operation of the cloud to the user. For provide the better quality of service it representing security testing and assure the better quality and accuracy for whatever user design.

III. PROPOSED SYSTEM

The proposed methodology is shown above in figure 3.1. Before conducting the migration process, it is essential to perform a thorough examination on the access rights and user accounts. This ensures that there is no insecure access protocol or out-dated credentials. The entire system security can be made vulnerable with a single stray user account. Hence this step is the essential and foremost in secure data migration.

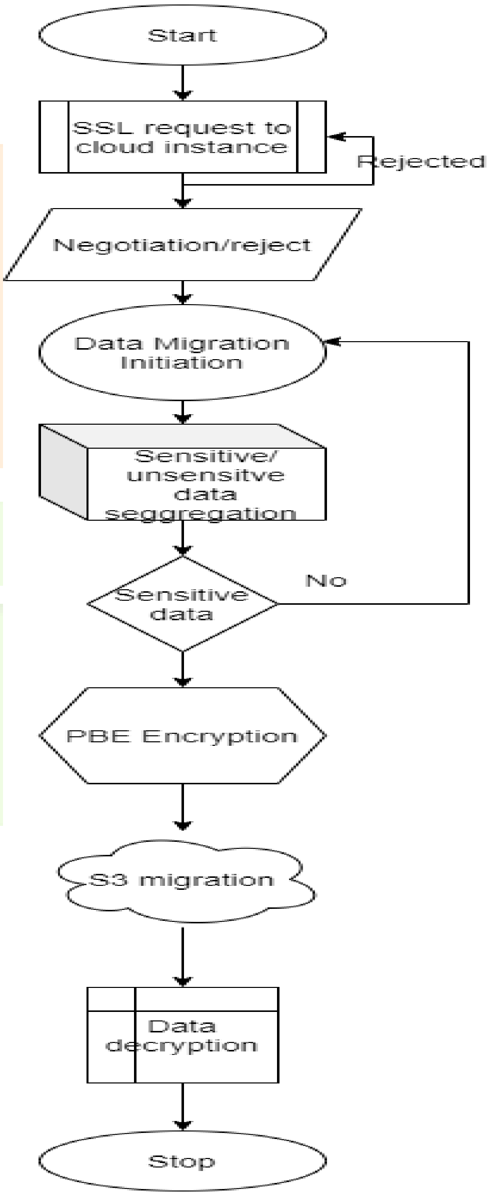
Start
SSL request to cloud instance
Rejected
Negotiation/reject
Data Migration Initiation
Sensitive/ unsensitve data seggregation
Sensitive data
No
PBE Encryption
S3 migration
Data decryption
Stop

Fig. 3.1 Flow diagram of Proposed System

The first step involves establishing a secure socket layer between the sender and receiver nodes. Secondly, the data migration ticket is initiated with minimum privilege. The data on the sender node is encrypted using Prediction Based Encryption with keys.

A. Security Socket Layer (SSL) establishment

Before beginning the migration process, the SSL protocol is used by the source and destination nodes and a secure channel is established. This security channel acts as a foundation for migration related security parameters. Data encryption key, random key, message authentication code and so on are temporarily used in this security channel. SSL creation and negotiation as shown in the fig 4.1 is not done manually instead it is readily available AWS services.

B. Migration ticket with minimum privilege

In order to verify the identity of a subject and appropriate permissions, tickets are used. In the source cluster from which the transmission is initiated, the data nodes hold the tickets. The destination node accepts the ticket when the SSL connection is established. Before beginning the migration process, the SSL protocol is used by the source and destination nodes and a secure channel is established. This security channel acts as a foundation for migration related security parameters. Data encryption key, random key, message authentication code and so on are temporarily used in this security channel.

The main purpose of the ticket is to authenticate the data transmission at source node and to reduce the use of unauthorised tickets by reducing the permission granted to the tickets. In case of multiple migrations happening simultaneously, it is easy to identify as the ticket carries the identity of the data node. This enables single usage of the ticket. Once the ticket is used, it will be destroyed automatically.

C. Amazon Web Service (AWS)

AWS is a cloud platform of Amazon that offers computing power, database storage, content delivery, and any other functionality that a basic cloud platform offers a platform where Amazon offers its cloud services like a database, servers, computing machines, file storage, etc., where you can rent them and pay for them according to your usage.

Servers are rented out so that Amazon takes care of the security and maintenance of the servers and helps the business. It also offers migration, networking, development tools and management to its clients. It is used by many companies, and its revenue is higher than any other large company. More than 100 cloud computing products make up AWS. Together, they provide storage, servers, networking, mobile development, email, and security. AWS is comprised of two main products: EC2 and S3. EC2 is a virtual machine service, while S3 is a storage system. Many popular websites such as Instagram and Netflix make up the AWS customer base. AWS data centres are located around the world in various regions. This provides greater disaster recovery. If one data centre fails, another region can pick it up quickly. According to various sources, Amazon Web Services is a secure cloud services platform offering computing power, database storage, content delivery, and other functionality to help businesses scale and grow.

IV. IMPLEMENTATION

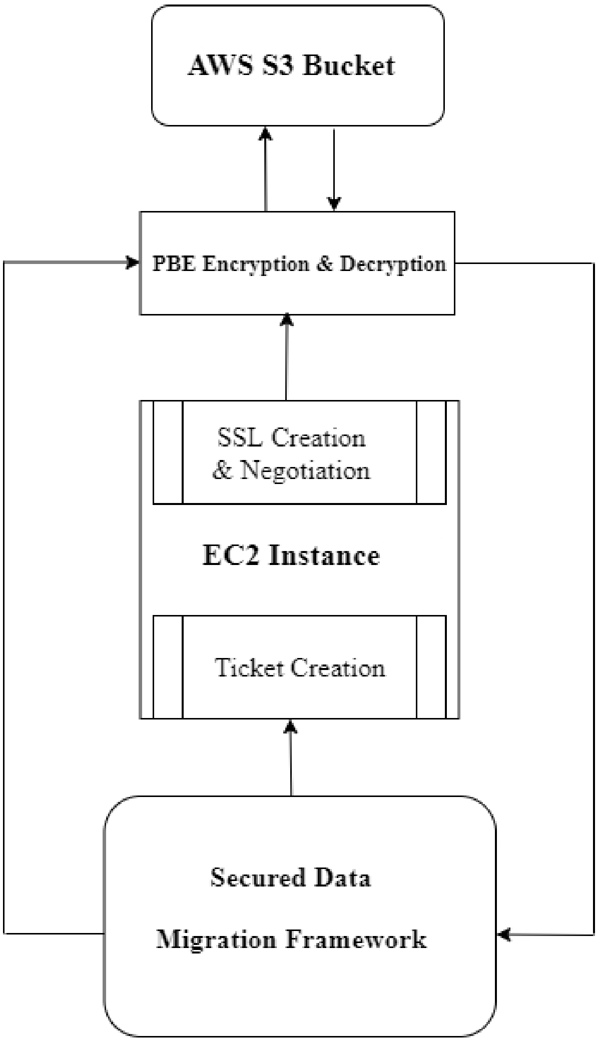
AWS S3 Bucket
PBE Encryption & Decryption
SSL Creation & Negotiation
EC2 Instance
Ticket Creation
Secured Data Migration Framework

Fig 4.1 System Architecture

The system architecture of the proposed methodology. Before conducting the migration process, it is essential to perform a thorough examination on the access rights and user accounts. This ensures that there is no insecure access protocol or outdated credentials. The entire system security can be made vulnerable with a single stray user account. Hence this step is the essential and foremost in secure data migration. Before beginning the migration process, the SSL protocol is used by the source and destination nodes and a secure channel is established. This security channel acts as a foundation for migration related security parameters. The services and method used for the paper implementation of the paper are described below in detail:

A. AWS Services

Amazon web service is an on-demand cloud computing platform that offers flexible, reliable, scalable, managed and easy-to-use, cost-effective cloud computing solution these all services are comes with a different level of abstraction like (IaaS) Infrastructure as a Service, (PaaS) Platform as a Service, and (SaaS) packaged software as a service and all of the service can be used on a pay-as-you-go basic means you will only be paying for what you are using and while it's using computing resources. The list of Services offered by AWS are—Analytics, Storage, Compute, Block chain, Database, Developer Tool, Networking and Content Delivery, Security, Identity and Compliance, Machine Learning. But we are using EC2 Instance, S3 Bucket, SNS and SES.

Amazon S3 or Amazon Simple Storage Service is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements.

AWS EC2 or Elastic Compute Cloud is a primary offering from Amazon web services that are useful for creating virtual machines on the cloud with several operating systems and configuration options. The EC2 instances are easy to set up and provision for use. AWS EC2 is secure and scalable. AWS supports various types of EC2 instances based upon the business need and cost plans. These can be fully controlled by the AWS account user for starting, accessing, stopping or depleting the EC2 Instances.EC2 Instances are associated with IP for remote access to the EC2 instances; the IP is known as elastic IP Address. AWS EC2 is associated with Storage options like EBS for volume data storage.

Amazon SNS or Amazon Simple Notification Service is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel. Clients can subscribe to the SNS topic and receive published messages using a supported endpoint type, such as, Amazon SQS, HTTP, email, mobile push notifications, and mobile text messages (SMS).

Amazon SES or Amazon Simple Email Service is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains. For example, you can send marketing emails such as special offers, transactional emails such as order confirmations, and other types of correspondence such as newsletters. When you use Amazon SES to receive mail, you can develop software solutions such as email auto responders, email unsubscribe systems, and applications that generate customer support tickets from incoming emails.

B. Using Virtual EC2 Instance

The instance is the virtual cloud environment which is provided by AWS. The connection from EC2 can be directly done by logging in to AWS web page and connect or by SSH the connection can be done using putty configuration for using the virtual computer on the local computer.

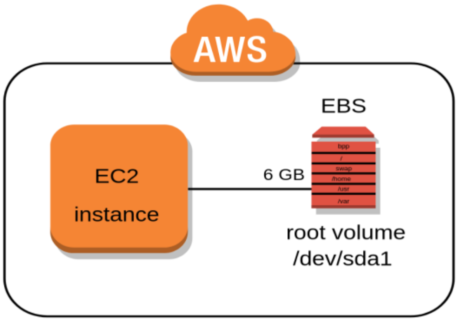

Fig. 4.2 AWS EC2 instance

The virtual instance by AWS is made the job easier to use it directly. SSM and Lambda services are implicitly running in the background. SSM for data login as a backend for SSH and Lambda behind IAM service. SSH is the method typically used to access a remote machine and run commands, retrieve files or upload files. Paramiko is a library that makes a connection with a remote device through SSH and it helps to transfer file from a virtual computer, only with this SSH client creation is done.

To access AWS EC2 authentication is required so the 'aws cli' commands is used to initialise it and start the EC2 instance and get the IP address and the encryption and decryption process is completed successfully and the acknowlegment is given to the user

C. Data Encryption and Decryption using PBE

Encryption is a process done to convert an undamaged message (plaintext) into an unreadable form (cipher-text), decryption is a process done to convert an unreadable message into a readable and understandable form. The encryption and decryption process is governed by one or more cryptographic keys. Cryptosystem is a facility to convert plaintext to cipher-text and vice versa. Based on the keys used for encryption and decryption, cryptography can be divided into symmetric key cryptography (Symmetric-key Cryptography) and asymmetric key cryptography (Asymmetric-key Cryptography). Encryption and decryption process as shown in below figure 4.2.

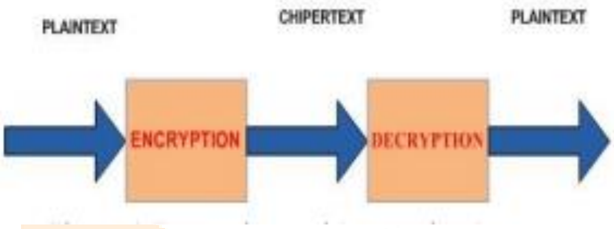

Fig 4.3 Encryption and Decryption Process

Hashing**:** This method is used in assigning dates to a document where by using hash functions, each person can assign date to the document without showing the contents of the document during the date allocation process. Cryptographic hash function is a hash function that has some additional security properties that can be used for data security purposes. A hash function is a function that efficiently converts a finite input string to an output string with a fixed length called a hash value. The best known examples of hash functions are MD2, MD5 and SHA. Perhaps a common use of hash cryptography is the creation of digital signatures. Since hash functions are generally faster than other digital signature algorithms. In this we are using the MD5 hash function.

The salt is a value that can thwart dictionary attacks or pre-computation attacks. The salt needs to be generated using a pseudo random number generator (PRNG). It is also strongly recommended not to reuse the same salt value for multiple instances of encryption. Note that the salt is not a secret value. So, it can be transmitted along with the cipher-text to the receiver or via out-of-band transmission methods. Ideally the length of the salt should be same as the output of the hash function being used.

Password Based Encryption (PBE) is a symmetric cryptographic method that uses a password-like key to perform the encryption process and uses the same key to perform the decryption process so that it will generate the same data as the original plain-text data. Plain-text data that has been encrypted will produce a cipher-text that cannot be read by others. Cipher-text is what will be sent to a second party so will have a reliable confidentiality. The resulting cipher-text data will be changed according to the password data input provided. PBE cryptography is based on the hashing mechanism. A password and salt will be combined so that it will generate random data through the application function process and will be processed by the iteration count so that when the mixing process has finished it will produce the data in the form of cipher-text.

A PBE algorithm generates a secret key based on a password, which will be provided by the end user. Currently there are two standards (PKCS #5 and #12) that define how a password can be used to generate a symmetric key. A good PBE algorithm will also mix in a random number called the salt along with the password to create the key. Without a salt, the hacker can perform a brute force search for the key-space with relative ease. PBE is typically used in systems such as local file encryption tools, which are used to ensure data confidentiality.

D. GUI Development to Single Window Access

The user interface used for this paper implementation is Tkinter. Tkinter is a Python binding to the Tk GUI toolkit. It is the standard Python interface to the Tk GUI toolkit, and is Python's de facto standard GUI. It is a backend support module in python. This simple GUI module is been working based on tkinter. The GUI gives the commands for it to connect to EC2 instance and migrate the files. The sample portal window is shown below in fig. 5.3.

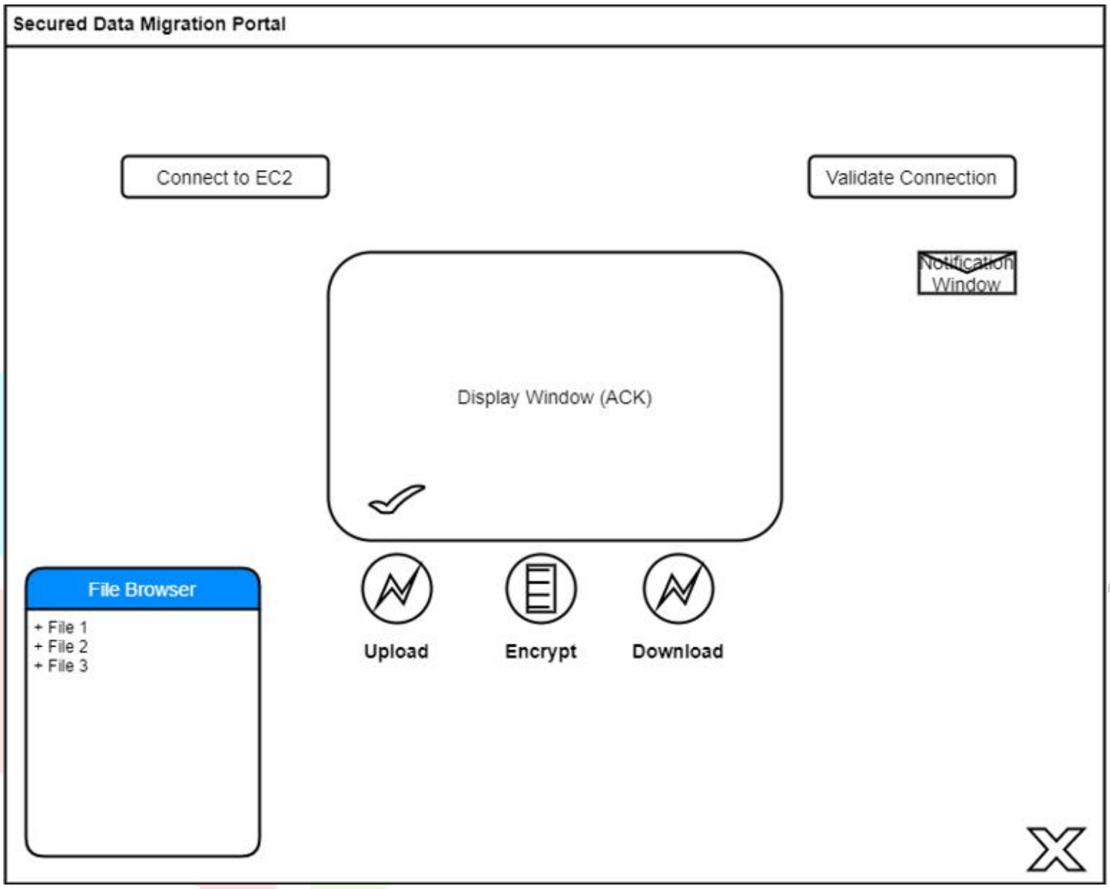

Fig. 4.4 GUI Portal Window

E. Notification Service

The notification services are user friendly options to display the acknowledgement message on the screen to understand whether the specific action is been occurred or failed. Say, if the user as to check the encryption process is complete and the file is ready to be uploaded to the S3 bucket and download the encrypted file to decrypt it and get back the source file acknowledgment is a must to keep a track with the help of SES and SNS services provided by AWS. The popup notification in the local computer as well as a mail will be sent to the verified mail id with the file name with the single window access, while the respective action is performed by clicking on Connect to EC2, Validate EC2, Browse the file, Encrypt, Upload, Download, Decrypt buttons.

V. RESULTS

When we simulated the traditional uploads and downloads time with 1.024Mbps bandwidth, the time taken to transfer increased as the size of the data increased. As the bandwidth increases the transfer time decreases. Now, when we simulate our proposed framework which is useful in transferring data from one cloud to another cloud, we find that the time taken to transfer from one cloud to another cloud is lesser than the time taken in traditional method of transferring data. When we simulated the traditional uploads and downloads time with 500Mbps bandwidth, the time taken to transfer increased as the size of the data increased. As the bandwidth increases the transfer time decreases Now, when we simulate our proposed framework which is useful in transferring data from one cloud to another cloud, we find that the time taken to transfer from one cloud to another cloud is lesser than the time taken in traditional method of transferring data. When we simulated the traditional uploads and downloads time with 1Gbps bandwidth, the time taken to transfer increased as the size of the data increased. As the bandwidth increases the transfer time decreases Now, when we simulate our proposed framework which is useful in transferring data from one cloud to another cloud, we find that the time taken to transfer from one cloud to another cloud is lesser than the time taken in traditional method of transferring data. The time complexity depends on the user usage speed.

VI. CONCLUSION AND FUTURE WORK

Cloud migration involves moving data, applications or other business essentials into a cloud computing environment. There are three types of cloud migrations namely from data centre to public cloud, from one cloud to another, from cloud back to data centre. This paper work provides an optimal solution for secure data transfer in cloud computing environment with three steps. The first step involves establishing a secure socket layer. Secondly, the data migration ticket is initiated with minimum privilege both done using the AWS services. The data to be migrated is encrypted using PBE technique for the data to be secured. The retrieval of data can be done by decryption process.

With the increase in the levels of encryption, the time taken for the encryption, transfer and decryption of data increases. Future work involves reduction of time cost required for encryption and transfer of data. Also, the data blocks can be split into smaller units to improve the speed and security during transfer and the password key management system after encryption process. This framework can be adopted by all cloud storage systems.

REFERENCES

[1] Security Guidance for Critical Areas of Focus in Cloud Computing, Version 2.1; Cloud Security Alliance: Palo Alto, CA, USA, 2009.

[2] Rittinghouse, J.W.; Ransome, J.F. Cloud Computing Implementation, Management, and Security; CRC Press: Boca Raton, FL, USA, 2010.

[3] Mather, T.; Kumaraswamy, S.; Latif, S. Cloud Security and Privacy; O'Reilly Media: Cambridge, MA, USA, 2009.

[4] Wilson, P. Positive perspectives on cloud security. Inf. Secur. Tech.Rep. 2011, 16, 97–101.

[5] Piao, Jing Tai, and Jun Yan. "A network-aware virtual machine placement and migration approach in cloud computing." In 2010 Ninth International Conference on Grid and Cloud Computing, pp. 87-92. IEEE, 2010.

[6] Er. Tamanna Narula, Er. Geetika Sharma, "Framework for Analyzing and Testing Cloud based Applications", semantic scholar, 2014.

[7] Rashmi Rao, Pawan Prakash, "Improving securityfor data migration in cloud computing using randomized encryption technique", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 11, Issue 6 (May. -Jun. 2013), PP 39-42.

[8] Nirav Shah, Sandip Chauhan, "SECURE DATA MIGRATION IN CLOUD PROVIDING INTEGRITY AND CONFIDENTIALITY", IJIRT | Volume 1 Issue 12 | ISSN: 2349-6002, 2015.

[9] Parikh Dhrumil Pareshkumar ,M S Deora, "Migration Algorithm for Data Security in Cloud Computing", IJSRDV2I1123, Page(s): 140-143, 2014.

[10] Shyamli Dewan, D. Kumar, Sandeep Gonnade, N. Verma, "A Survey on Data Migration Techniques Across the Cloud Storage Systems", Semantic Scholar, 2015.

[11] Suganya .N, N.Boopal M.E , Naveena .M, "Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing", International Journal of Innovative Research in Science, Engineering and Technology, 4, 18954- 18957, 2015.

[12] Shyamli Dewan,Devendra Kumar,Sandeep Gonnade, "Secure Data Migration across Cloud System Using Third Party Auditor (TPA)", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June2015.

[13] G. Gowri,M. Amutha, "Cloud Computing Applications andtheirTesting Methodology", International Journal of Innovative Research in Computerand Communication Engineering, Vol. 2, Issue 2, February2014.

[14] Kazim, Muhammad, and Shao Ying Zhu. "A survey on top security threats in cloud computing." in 2015.

[15] F. Wang, J. Liu, M. Chen and H. Wang, "Migration towards cloud-assisted live media streaming", IEEE/ACM Transactions on Networking, pp. 1-11, 2015

[16] X. Qiu, H. Li, C. Wu, Z. Li and F. Lau, "Cost-minimizing dynamic migration of content distribution services into hybrid clouds", IEEE Transactions on Parallel and Distributed Systems, vol. 26, pp. 3330-3345, 2015,

[17] M. Menzel, L. Wang, S. U. Khan and J. Chen, “Cloudgenius: a hybrid decision support method for automating the migration of web application clusters to public clouds”, IEEE Transactions on Computers,vol. 64, pp. 1336-1348, 2015.

[18] Y. Zhu, D. Huang, C. Hu and X. Wang, “From Rbac To Abac: Constructing flexible data access”. IEEE Transactions on Services Computing, vol. 8, pp. 601-616, 2015.

[19] M. Ali, S. Malik and S. Khan, “Data security for cloud environment with semi-trusted third party”, IEEE Transactions On Cloud Computing, pp.1-14, 2016.

[20] Y. Alsalhi, “An accurate and high-efficient qubits steganography scheme based on hybrid neural networks”, Multimedia Tools and Applications, pp. 1-17, 2019.