Cloud Based Security & Adaptive Data Compression with AES Algorithm

Poonam Kale[1] Snehal Deshmukh[2] Varsha Patake[3] Rashmi Kadu[4] Prof. A. B. Pahurkar[5]
[1,2,3,4,5]Department of Computer Science Engineering
[1,2,3,4,5]PRMIT&R, Badnera, India

Abstract— This paper proposes an overview of desktop application which uses cloud service and provides a network to user for securing data over cloud by storing it in encrypted format and even compressing file to certain extent. This data could only be retrieved with the help of key which is provided by the application to the user. The main aspect of cloud computing is how one can Secure, Protect and Process the data. Cloud computing is a technology that is recently developed for complex systems with large-scale services sharing among multiple users. Therefore, authentication, integration & confidentiality of data of users and services are a significant issue for the trust and security. Cloud computing is essentially the management and provision of applications, information and data as a service. Using key based Cryptography technique we have proposed and implement a new algorithmic approach for cloud security in this paper. The efficiency of the algorithm can be improved by integrating multiple cryptography algorithms. To ensure the data security, we proposed a method by implementing AES algorithm and with data compression through lossless algorithm.

Key words: Cloud Computing, Authentication, Integration, Cryptography, Data Security, AES Algorithm, Lossless Algorithm

I. INTRODUCTION

Cloud computing is a resource delivery and usage model. It means to obtain resource where by shared software, hardware, and other information are provided to computers and other devices as a metered service via network. Cloud computing model is very exciting model especially for business peoples. Many business peoples are getting attracted towards cloud computing model because of the features easy to manage, device independent, location independent. But this cloud models comes with many security issues [4]. A business person keeps crucial information on cloud, so security of data is crucial issue as probability of hacking and unauthorised access is there. Also availability is a major concern on cloud. In order to reduce threats, vulnerability, risk in cloud environment, consumers can use cryptographic methods to protect the data, information and sharing of resources in the cloud computing. [3]

A. User Interface:

As per the project is for security it will have a very basic GUI. It will only allow the authenticated use to login and for new user there is an available option of registration on the main page .The new user has to register by providing a valid information's about him/her. The registration will make a new entry in the user detail database and the person will now be an authenticated person to use the software. The GUI is being developed in the .NET. We are being using the SQL database as our background storage of user information.

B. Objective:

Cloud computing is emerging technology that says renting is better than buying as its application need not to be installed on user computer and can be accessed from different places just by paying the rent. Security is also important when you perform any work on cloud server like storage of data, running application *etc*. for that purpose we have to send the data in cryptographic manner [6].

The general objective of this project is to contribute to the development of these cloud systems as well as to study the technical impacts of a state-of- the-art prototype. More specifically, a secured storage on cloud will be developed, which will take advantage of recent advances in the areas of cloud computing and development, data storage and security, parallel and distributed software engineering and networking techniques. This prototype will be tailored to the specific needs of cloud exploration; furthermore, it will be particularly suitable for areas such as education, training, business, electronic commerce. Thus, the overall objective of this project is to develop a system that stores user data on cloud in a secured manner. In other words, the general aim of the project is to offer a concrete contribution to the creation (and evaluation of its impact) of the Information Society in the Cloud computing region.

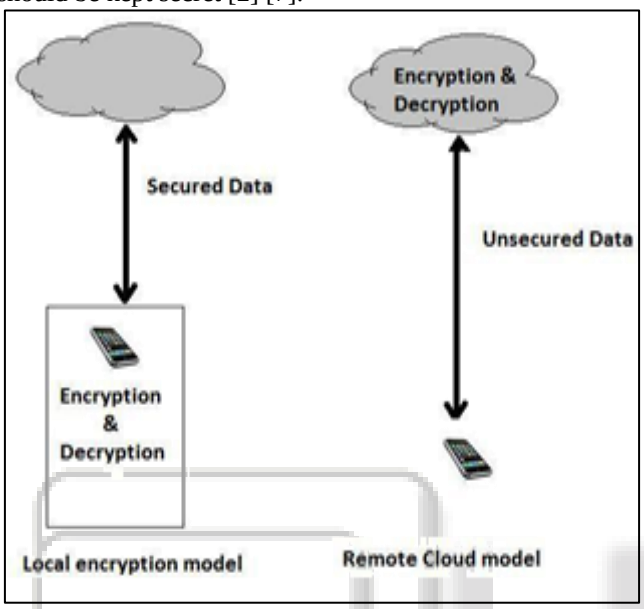
This general objective can be broken down to three more specific objectives that would together achieve the overall goal of the project as follows:

- Store Data in cloud based storage; main aspect of cloud computing is how one can secure, protect and process the data.
- Develop cryptography AES Security, protect client data from unauthorized access disclosure, modification and monitoring
- Compress data, to save data storage capacity, speed of file transfer and decrease cost for storage and network bandwidth.

C. Cryptographic Approach:

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data Related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. We propose a suitable method that cryptographic algorithms with different key lengths are used in various environments. End users can access easily to cloud computing environment though these user friendly software, we define that such software is one of specific services of cloud computing and its service which is added a cloud computing service[1][3]. According

to key characteristics, modern cryptosystem can be classified into symmetric cryptosystem, asymmetric cryptosystem and digital signature. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), AES (Advanced Encryption Standard). For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret [2] [7].



D. Compression:

Lossless compression reduces a file's size with no loss of quality. This seemingly magical method of reducing file sizes can be applied to both image and audio files. While JPEG and MP3 uses lossy, instead of it we can use lossless algorithm for more sufficient use.

Lossless compression basically rewrites the data of the original file in a more efficient way. However, because no quality is lost, the resulting files are typically much larger than image and audio files compressed with lossy compression. For example, a file compressed using lossy compression may be one tenth the size of the original, while lossless compression is unlikely to produce a file smaller than half of the original size.

II. LITERATURE REVIEW

Cloud computing has grabbed the spotlight in the year 2013 at a conference in San Francisco, with vendors providing plenty of products and services that equip IT with controls to bring order to cloud chaos. Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lie. At an unusual pace, cloud computing has transformed business and government. And this created new security challenges. The development of the cloud service model provide business – supporting technology in a more efficient way than ever before .the shift from server to service based technology brought a drastic change in computing technology. However these developments have created new security vulnerabilities, including security issues whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and security solutions.

Some of the proposed methods have been discussed in the literature survey for handling security issues in cloud computing. Popovi and Hocenski, discussed about the security issues, requirements and challenges that are faced by cloud service providers during cloud engineering [4]. Behl explores the security issues related to the cloud environment. He also discussed about existing security approaches to secure the cloud infrastructure and applications and their drawbacks [5]. Sabahi discussed about the security issues, reliability and availability for cloud computing. He also proposed a feasible solution for few security issues [6]. Mohamed E.M et.al presented the data security model of cloud computing based on the study of cloud architecture. They also implemented software to enhance the work in Data Security model for cloud computing [7]. Wentao Liu introduced some cloud computing systems and analyzes cloud computing security problems and its strategy according to the cloud computing concepts [8]. Mathisen, E discussed about some of the key security issues that cloud computing are bound to be confronted with, as well as current implementations that provide a solutions to these vulnerabilities [9].

In March 2014, Emerging Security Issues and Challenges in Cloud Computing S C Rachana , Dr. H S Guruprasad stated that ,Cloud computing is an Internet-based computing solution which provides the resources in an effective manner. A very serious issue in cloud computing is security which is a major obstacle for the adoption of cloud. The most important threats of cloud computing are identified and understood in this survey. This paper covers the information about the threats such as- Multitenancy, Availability, Loss of control, Loss of Data, outside attacks, DOS attacks, malicious insiders, etc. The solutions to overcome some of these threats have also been highlighted in this paper. [2]

III. SYSTEM ARCHITECTURE

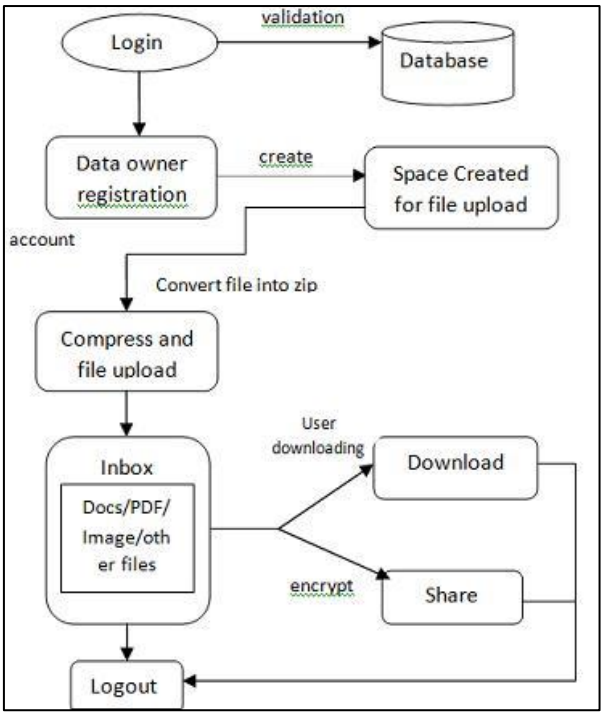
As per the project is for security it will have a very basic GUI. It will only allow the authenticated use to login and for new user there is an available option of registration on the main page. The new user has to register by providing a valid information's about him/her. The registration will make a new entry in the user detail database and the person will now be an authenticated person to use the software.

For secured sharing of data we have used AES algorithm.

Due to this only authenticated user will able to access data.

Following is system architecture of our project.

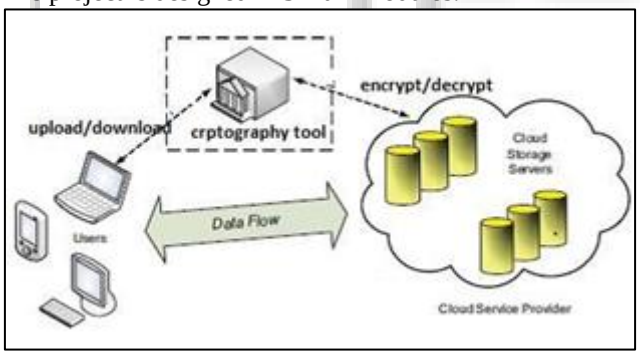
User need to login and the data that is being saved in database will validate whether user is authenticate. When user had created account, space will be allocated to the user to save/upload data. Data will be saved in compressed form and user can download the zip file or even can share file by inserting user name. While sharing the data key will be generated and will be send to authenticate user.



IV. SOFTWARE DESIGN

Security is also important when you perform any work on cloud server like storage of data, running application etc. For that purpose we have to send the data in cryptographic manner. The following figure illustrates the flow of project. Data flows from user to the cloud server and vice-versa. User can make use of cryptographic tool if he wishes.

Cryptographic tool encrypts data and stores it on server. If the user requests an encrypted file, the cryptographic tool decrypts the file and sends it to the user. This project is designed in 3 main modules:



A. Cloud document server:

A Server where a user can store documents. It will be a network application which will use xml based command request to perform operations. It will maintain user registry. It will also maintain storage space of all users Will Store user documents in user space [3].

B. Web application:

It will provide an interface between cloud server and end user who wants to store documents. It will provide interface to register new users with cloud server. Will send user registry request to server for registration. Will provide a login interface and will send login information to cloud server. It will provide an interface to upload and download documents.

C. Cryptography Tool:

It is a desktop application which will perform cryptographic operations. This tool can be downloaded from the web application for security. This tool will use AES algorithm for cryptography. It will generate a new AES key whenever requested. This key will be used to encrypt documents. These encrypted documents can be sending to the cloud server by using web interface [5] [8].

V. CONCLUSION & FUTURE SCOPE

A. Conclusion:

In the older techniques these cryptographic algorithms are implemented in the Single system environment and compression. Now due to availability of high performance computing techniques, similar test has been conducted in the single system Environment i.e. local environment and also in the Cloud environment. From the observed results, and based on the considered parameters, storing the data in cloud increases the efficiency. Also the results reveal that AES algorithm qualifies better than other algorithms in Mean processing time and Compression provide huge storage of data.

B. Future Scope

To save huge amount of data and in secured form, such software will be efficient for user. Here user will get security and compression of data, due to which large storage can be done.

REFERENCES

A. Basic format for books:

[1] Jaber, A.N.; Bin Zolkipli,,M.F. "Use of cryptography in cloud computing" Control System, Computing and Engineering (ICCSCE), 2013 IEEE International Conference on Year: 2013
[2] Emerging Security Issues and Challenges in Cloud Computing S C Rachana , Dr. H S Guruprasad, March 2014.
[3] Okubo, T.; Wataguchi, Y.; Kanaya, N."Threat and countermeasure patterns for cloud computing" Requirements Patterns (RePa), 2014 IEEE 4th International Workshop on Year: 2014
[4] Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.p.344-349.
[5] Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai, 2011.p.217-222.
[6] Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks (ICCSN), May 2011.p.245-249.
[7] Eman M.Mohamed, Hatem S Abdelkader, Sherif EI Etriby. Enhanced Data Security Model for Cloud Computing, in:8th International Conference on Informatics and Systems(INFOS), Cairo, May 2012.p.12-17.

[8] Wentao Liu. Research on Cloud Computing Security Problem and Strategy, in: 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), April 2012.p.1216-1219.
[9] Eystein Mathisen. Security Challenges and Solutions in Cloud Computing, in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.p.208-212.

