

Location Based Secure Cloud Data Storage Using Biometric Authentication

Ayush Singh, Sandhya Tarar
Post Graduate Student, Assistant Professor
School of ICT
Gautam Buddha University, Greater Noida, India

Abstract : Cloud computing is a set of information technology services such as network, software system, storage, hardware, software and resources. Federated cloud computing is a type where various users data is stored across both private and public clouds. Federated cloud has certain rules set by the federation which its users need to follow strictly. Since the federated cloud has data stored across private as well as public clouds, there is constant threat to data. This paper describes a simple data security system implemented using fingerprint biometric technology to ensure data security of the federated cloud system. The data is made more secure by encrypting it before storing it to the cloud. Desired location is also taken into consideration i.e. the location where the user wants his data to be decrypted. Data storage is demonstrated by a prototype consisting of components namely hardware and software. The hardware component is inclusive of fingerprint sensors as an application server. A software program is developed to verify and record the fingerprint data on the remote server. To lower the implementation cost all system components are connected to the cloud.

Index Terms - Data Security, Security Issue, Cloud Computing, Encryption, Decryption

1. INTRODUCTION

Cloud computing is the usage of services such as servers, databases, storage and various other computing services over the internet. The basic concept of cloud computing is using computing resources located at some other part of the world via internet. The network where these computing resources are available is known as cloud. There are namely two types of cloud - private and public clouds.

Private cloud refers to the cloud computing and resources set up by a private organization in order to fulfil its computing needs with its organization. The cloud servers in case of private clouds are run within the organization's own data centers. Some of the public clouds are Dell EMC, Red Hat, VMWare, IBM etc.

Public cloud is defined as "allocation of cloud services based on user needs that can only be accessed by the authorized user". Public clouds and its resources are provided to users or organization depending upon their need. Some common examples of private clouds are AMAZON AWS, Microsoft and Google Cloud Platform.

2. Federated Cloud

Federated cloud refers to the group of clouds inclusive of both public and private clouds. This group or association of clouds falls under a federation which sets certain rules and regulations that are must to be followed by the cloud members. The main motive behind using both public and private clouds is to mitigate the lack of storage for data and also using the utilizing the unused storage of various private and public clouds. But along with the use of public and private clouds accompanies the threat of unauthorized access to the data on the cloud. This paper therefore focuses on a system implemented to secure data across federated clouds.

3. Cloud Data Security

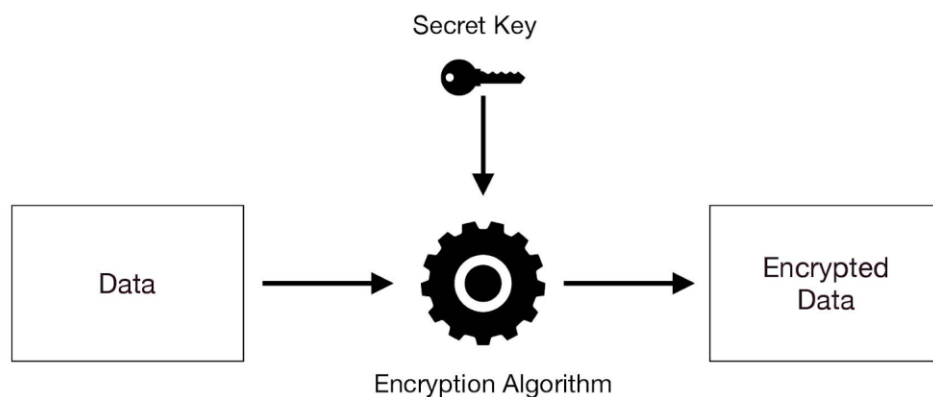
Nowadays both private and government organizations are moving towards cloud computing for their data storage and other computing services. All of this data whether be government or private needs to be secured. Some organizations still keep themselves away from the cloud services because of the safety concerns of the data over the cloud. Security of cloud data is of utmost importance and therefore needs proper concern and attention. Attackers constantly try to get access of the data over both private and public clouds. One possible and efficient solution to this security issue is cryptography .Cryptography includes two basic functions encryption and decryption.

4. Encryption

In cryptography encryption is hiding the data or converting it in such a form that prevents the original data to be accessed by unauthorized users. In other terms encryption is the process of converting the original data into a non-standard format which is of no use to anyone without decrypting it.

There are various methods for encrypting the data. Some of these are - DES, BLOWFISH, AES, Twofish, IDEA etc. In this paper we use Blowfish algorithm for encrypting the data. Blowfish is used against other like AES, DES since it is fast and supports variable key length while others don't.

Figure 1.1 Encryption



Decryption

Decryption is the reverse process of encryption i.e. getting the original data from the encoded data using the secret applied to the data while encrypting it. Decryption cannot be done without the secret key supplied to the data while encrypting it. Blowfish algorithm that is used in this paper, supports variable key length from 32 Bits to 448 Bits while others like AES, DES take fixed key length.

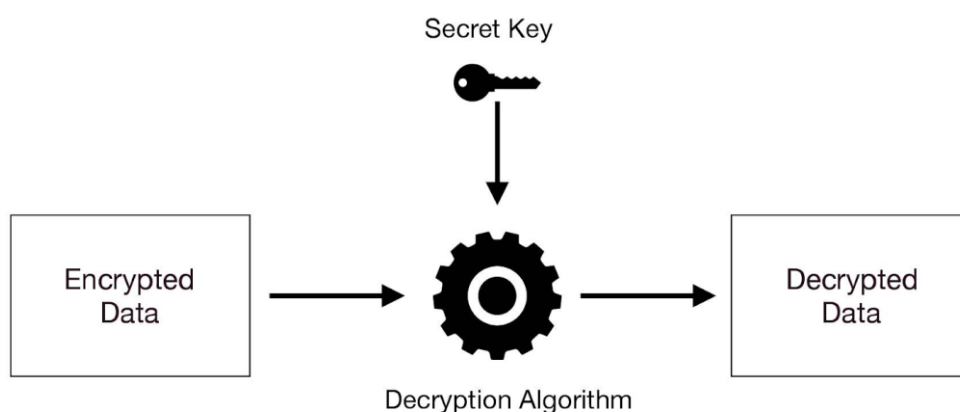


Figure 1.2 Decryption

Biometric Verification

Biometric authentication or verification can be defined as authenticating a person based on his biological traits. Biometric verification might be any of the following - hand geometry, fingerprints, earlobe geometry, voice waves, DNA, signatures, retina and iris patterns. Fingerprint verification stands to be the oldest form of biometric verification. The new or say recent ones include iris/retina scan. The retina scan has been implemented at some places like banks lockers, automated teller machine. One more amongst the new ones is voice recognition which is used in research facilities for accessing proprietary data banks. Facial recognition is the most recent and trending one which is also being used in various smartphones. Apple was the first company to launch facial recognition in its smartphones accompanied by various other companies. It does not depend upon which biometric verification process is being used, it is almost same for all process i.e. a person's unique characteristic is stored in the database which is later on used for verification.

II. TOOLS USED

A. Biometric Scanner

In the system developed fingerprint scanner has been used. Fingerprint scanner is a device which captures fingerprint of an individual which is later used to verify him against the details stored in the database. Fingerprint biometric is one of the earliest types of biometric verification process which is highly accurate and reliable. Fingerprint verification is now a days is available in many smartphones as well. It is very cost-effective way of biometric verification for the authenticity of a user.

B. Glassfish Server

Glassfish server is an Oracle sponsored open source application server which was started by ‘Sun Microsystems’ for the Java EE platform. This server provides an http server where the system developed is run. The best thing about Glassfish server is that being an application server, it can also be used as a Web Server (Http Server). Since it is web server it can be used from any of the browsers like chrome, apache etc. In this system implemented we run a jsp application but this server can handle EJBs as well.

III. ARCHITECTURAL FLOW

A. Authentication

Authentication checks and authenticates the person requesting access to the information is the one he claims to be. It is a process of proof of identity. This is a very crucial and an important security measure for providers and users of cloud computing services.

Developer has provided many securities to access the file like fingerprint security after the login to the system via username and password within the required location. Login to the cloud interface has been given by Google Login which ensures the user to be an authenticated one as google users are most of the time authenticated ones.

B. Access Control

After authenticating and making sure the user is the one claiming to be, the next step is access control. This restricts the user to accessing all information and accessing only material that the user has access to. The more efficient way is to assigning rights when compared to assigning permissions to a specific users. In this system if any user want to access the file has send the request of user who is uploaded the resources by specific user. If user gives access to the file then received OTP as file password and within the location which is specified by the user to decrypt the file and must be register with the same cloud.

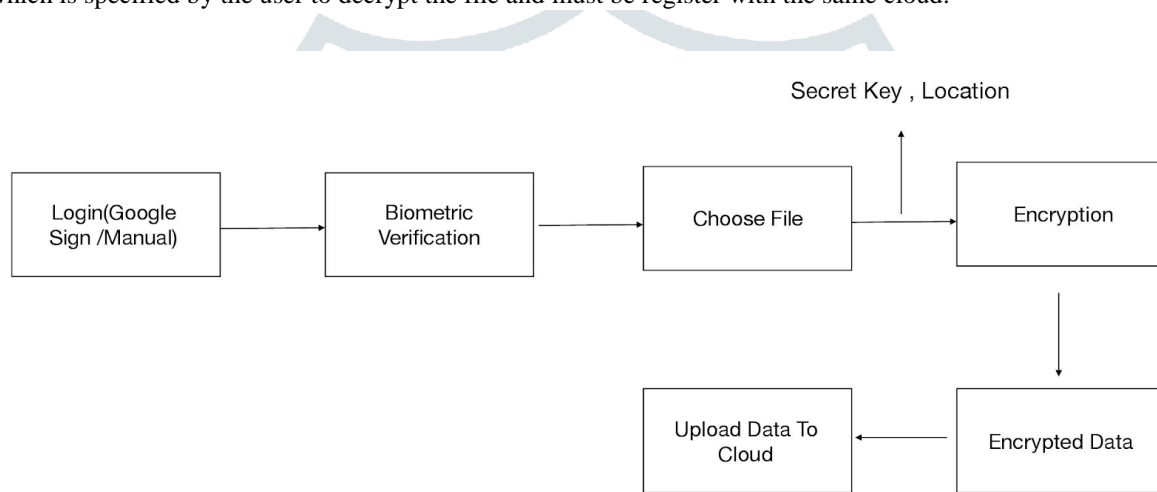


Figure 3.1 Encryption Flow for the System

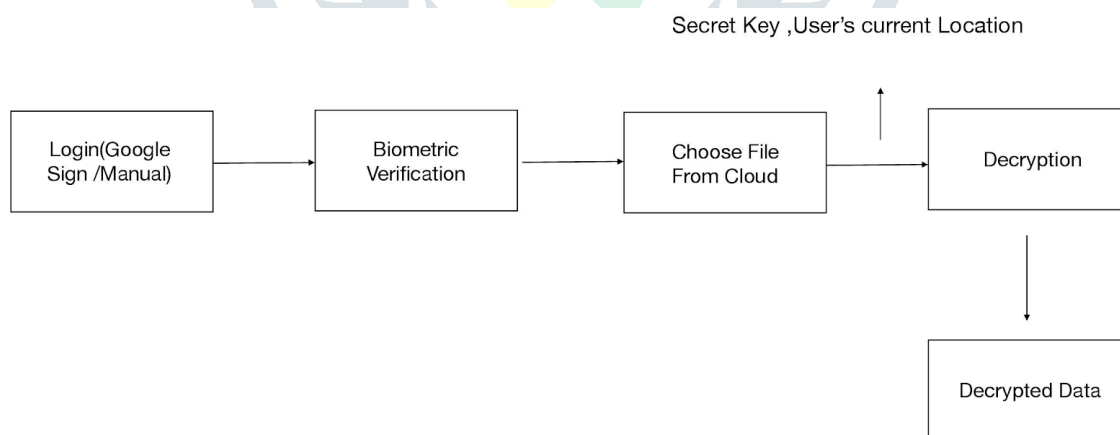


Figure 3.2 Decryption Flow for the System

C. AUDIT

Third and last part of data security is auditing. Information security configurations should be reviewed to ensure the existing access controls.

In this system auditing is done using fingerprint security to ensure that the user is register with the same cloud.

Biometric authentication techniques like fingerprint biometric authentication used in the cloud access control platform, should be used to create an indisputable audit trail.

IV.ALGORITHM USED

A. Blowfish Algorithm

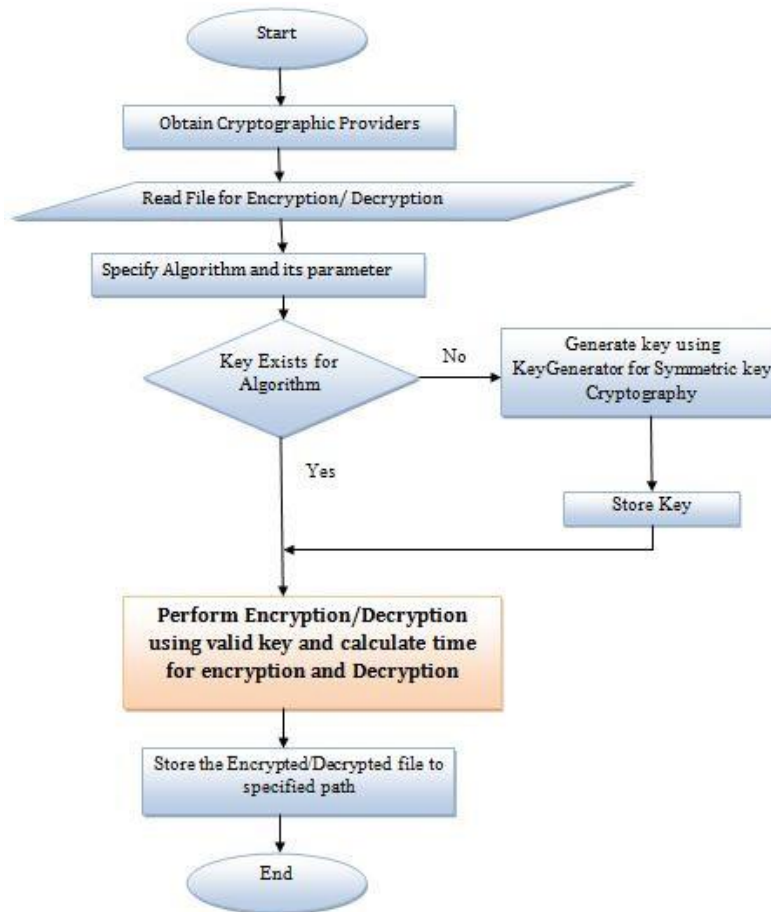


Figure 4.1 Flowchart depicting Blowfish Algorithm

Blowfish Algorithm is variable key encryption algorithm that can be used as a replacement for DES, 3DES and IDEA algorithms. The best thing about Blowfish is that it uses a variable length encryption key i.e. from 32 to 448 bits which makes it suitable for exportable as well as domestic use.

Pseudo Code

```

Line
1  Key Expansion(byte key[4*NK], word k [Ni+1,Nc], Nc, Nk, Ni)
2  begin
3    i =0
4    while (i<Nk)
5      k[i] = word [key[4*i+3],key[4*i+2],key[4*i+1],key[4*i]]
6      i = i+1
7    end while
8    i = Nk
9    while(1<Nc*(Nr+1))
10     word temp = k[i-1]
11     if(i mod Nk = 0)
12       temp = (SubByte(RootWord(temp))xor
13         Rcon[i/Nk]))
14     end if
15     k[i] = k[i-Nk] xor temp
16     if(i mod Nk =3)
17       //Apply the new approach "ShiftRow" transformation
18       word temp1 [4][4]
19       for (c = 3; c>=0;c-1)
20         temp1 [c][r] = k[Nk+c]
21       ShiftRow (temp1);
22     end if
23     i = i+1
24   end while
25   end

```

V.PROPOSED SYSTEM

Federated clouds incorporate both private and public clouds to minimize the issue of data storage. But by the use of private and clouds together, a threat occurs to the data. Unauthorized access to the data on clouds is major problem in federated cloud. In this paper we try to prevent unauthorized access to the data by implementing a system to secure the data by encrypting it using Blowfish algorithm.

In the system user is validated at almost each step. First while logging into the system user has two options - Login via Google or Login via entering manual credentials. In case of Google login the user is already authenticated by google but still he is verified by his fingerprint biometric before providing him access to the application. In case of manual credentials also the user is verified by his fingerprint biometric. At the data encryption phase user is asked for the desired location where his data can be decrypted which makes the data more secure. At the time of decryption the user is asked for the secret key and also his fingerprint biometric is verified and the most important part is that the user needs to be within a range set at the time of encryption. At each and every stage of the system developed, data is tried is keep away from unauthorized users. If by any means they get access to the encrypted data, still they won't be able to get the original as decryption process includes fingerprint biometric phase which they won't be able to pass.

VI.IMPLEMENTATION


A. Authentication/Authorization

This is entry point to the app where user needs to verify himself as the one he claims to be before he can encrypt or decrypt his files or use them. Two options are given to the user:

- 1. Google Login:** With the help of google login we generally get authenticated users as google does a lot checks for its users validity. OAuth 2.0 protocol is used by google in order to authenticate and authorize the user. This approach is also better as it takes less time than the manual entry of credentials.
- 2. Using Credentials:** This is the normal method where the user inputs his credentials i.e. unique id or email and password associated. This process checks for the users' entered credentials and verifies it with the details in the system's database. If the credentials entered match with any of the database records, access is granted to the user.

[Home](#) | [Register](#) | [Login](#)

Login



Email ID:

Password:

[Login](#)

Figure 6.1 Login

B. Data Encryption

Encryption refers to the process where data is converted into such a form that is of no use to the unauthorized parties. In this phase we are using **Blowfish** algorithm to encrypt the data. The key thing about this encryption is that we store the desired location (latitude + longitude) where the user wants his data to be decrypted. This location is verified against users' active location at the time of data decryption.

Encrypt File

File Password:

[Get Location](#)

Latitude: Longitude:

File Name:

Upload File: No file chosen

[Submit](#)
[Reset](#)

Figure 6.2 Encryption

C. Data Decryption

Decryption is the reverse process of encryption where we decode the encrypted data that is in a secret format to the normal original format. Here before decrypting the data we check users' authenticity by fingerprint biometric and also check his location that has to match the location stored while encrypting the data. At last if first checks are passed by the user then he is asked for the password required to decrypt the data.

Decrypt Files

S.No	File Name	Adding Date	Download	Delete	Share
1.	report1	2018-12-16.	Download	Delete	Share
2.	test	2018-12-17.	Download	Delete	Share
3.	test2	2018-12-17.	Download	Delete	Share

Figure 6.3 Decryption

D. Data Sharing

Data sharing means sending and receiving data amongst various users that may or may not belong to a group or community. Here in case if federated cloud data can shared amongst users who are associated with the clouds that are a part of the cloud federation. Data cannot be shared to any party or user who is not a part of the cloud federation.

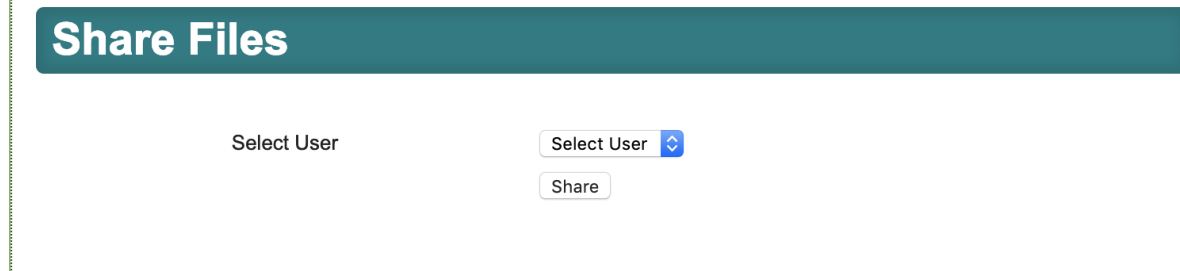


Figure 6.4 Data Sharing

VII.RESULT ANALYSIS

Federated cloud solves a lot of problems as it incorporates both private and public clouds for data storage. But along with this solution follows threat to data that is stored across these private and public clouds.

The primary concern of this system developed here is to secure the data over the private and public clouds. As public clouds are involved, so the data is can be accessed by any user of the cloud. But our primary aim is to make the data secure enough so that it can be accessed only by the authorized users.

File	Extension	Size(prior encryption in mb)	Size(post encryption in mb)
File1	pdf	48.8	48.8
File2	jpg	20	20
File3	jpeg	10.5	10.5
File4	doc	1.2	1.2
File5	zip	6.4	6.4
File6	tar	2.3	2.3
File7	xlsx	0.9	0.9
File8	mp3	150	150
File9	exe	250	250
File10	rar	22	22

Above table illustrates list of files along with their type and size (prior and post encryption) that were tested against the system developed. First amongst some major concerns that we have for the developed system is the time taken for the entire encryption process i.e. normal encryption vs encryption along with location and other additional parameters. Second one is the file size before and after the encryption process.

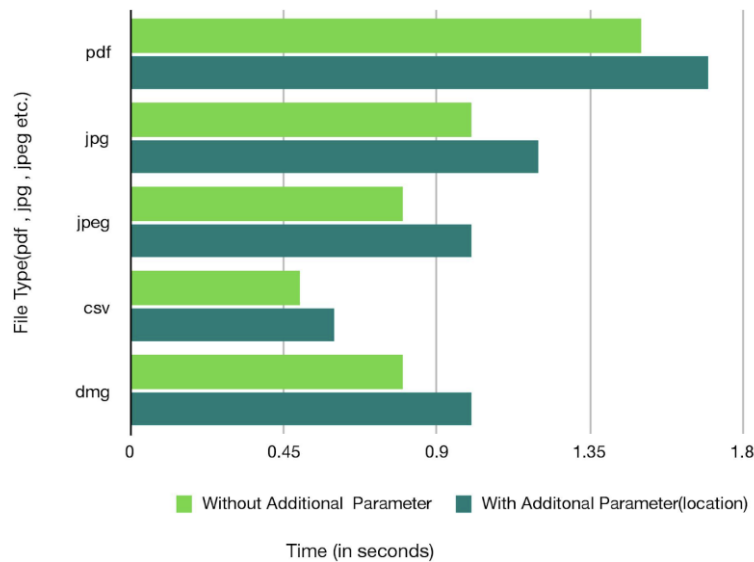


Figure 7.1 Time Comparison for encryption with and without additional parameters (location)

The above graph shows a comparison of the time taken for encryption with and without additional parameters like location for various types of data.

From the above graph it is clear that the time taken for encryption with and without additional is almost the same. There is a minute difference in the two times and also on the other hand the data is now more secure. Some seconds can be neglected when it comes to the security and authenticity of data.

So it is clear from the results above that the system implemented has passed the time constraint factor.

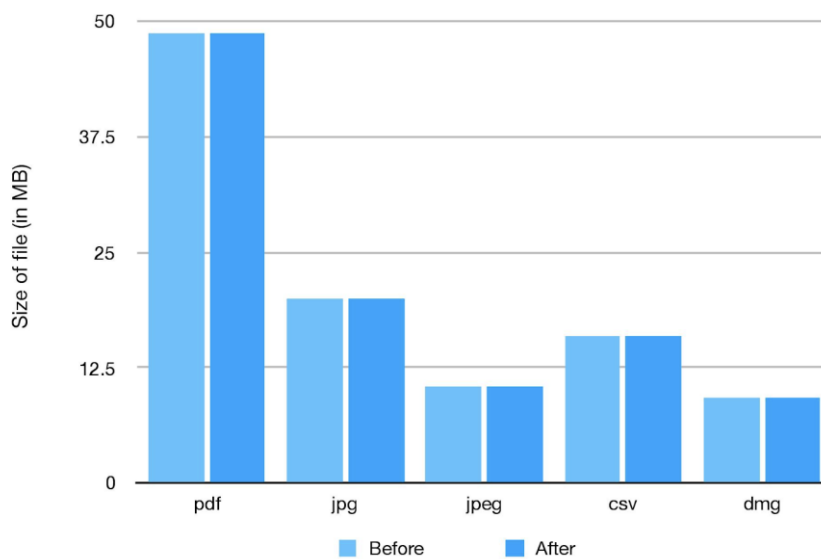


Figure 7.2 File size before and after encryption

The second important factor that comes to mind regarding the implementation of this system is the data size before and after the encryption process. As per the system, size of the data should not change before and after the encryption process and that is exactly what we get from the results.

Above two important results show that the system implemented at no point interferes with the data and also does not tamper it, instead it makes it more secure where authorized users constantly try to get access of secret and sensitive data.

The system implemented supports files of almost all type like pdf, jpg, jpeg, xlsx, mp3, mp4, text etc. for encryption or decryption and also its security. The purpose of this paper is minimize any possible unauthorized access of any data across the private and public clouds that are part of the cloud federation, and this motive has been fulfilled.

VII.CONCLUSION

Cloud services lay bases for various industrial and research works. Hence, organization's data security is an area of primary interest. The proposed approaches can help secure cloud environments for complex business operations. This research paper therefore focuses on cloud computing data security through fingerprint authentication and **Blowfish** algorithm and all data security information in cloud computing.

Using a wireless network biometric fingerprint, can be an alternative to data security. This process can be more reliable and more convenient. The components used in this project are relatively cheap and are used widely in the market. Fingerprints over a wireless network are expected to provide the best data security in the cloud for storage and access to the data.

In future more improvements can be done to this system. Possible improvements can be securing the channel through the data is uploaded to cloud, using more reliable and secure data encryption algorithm. Using steganography instead of cryptography can also be a possible improvement to increase the security of data.

REFERENCES

- [1] Christian Esposito, Aniello Castiglione and Kim -Kwang Raymond Choo, "Encryption Based Solution For Data Sovereignty in Federated Clouds", 2016
- [2] "Hype Cycle for Emerging Technologies", Gartner, 2012;www.gartner.com/DisplayDocument?doccd =233931
- [3] Robert Gellman and World Privacy Forum , "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", February 23, 2009
- [4] Amazon.com, "Amazon Web Services (AWS)," Online at <http://aws.amazon.com>, Version 2019
- [5] P. Mell, T. Grance, "Draft NIST working definition of cloud computing"
- [6] A. Konwinski, D. A. Patterson,G. Lee, A. Rabkin, M. Zaharia,I. Stoica, "Above the clouds: A Berkeley view of cloud computing," University of California, Berkeley, Tech. Rep, 2009
- [7] Panagiotis Kalagiakos, Panagiotis Karampelas, Cloud Computing Learning, Application Of Information and Communication Technology (AICT), 2011 '5th International Conference'
- [8] Alkhatib, Ghazi I. (ed. 2010), "Web Engineering Advancements and Trends: Building New Dimension of Information Technology", Available at: <https://books.google.co.in/books?isbn=160566720X>
- [9] Alfred C. Weaver, "Biometric Authentication", 2006 Tayseer S. ATIA, "Development Of A New Algorithm For Key And S-Box Generation In Blowfish Algorithm", 'Journal Of Engineering Science And Technology Vol.9 No 4 (2014)'

