IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

Privacy Secure Data Authentication in Cloud Computing

Rakesh Prasad Sarang[1*], Anshu Chaturvedi[2], D.N. Goswami[3]

[1,3]SOS in Computer Science & Applications Jiwaji University, Gwalior (M.P.), 474001, India
[2]Dept. of Master of Computer Applications, M.I.T.S. Gwalior (M.P.), 474001, India

[*]*Corresponding Author:* sarang.snit@gmail.com, *Tel.: +91-9926646335*

Available online at: www.ijcseonline.org

Accepted:25/Sept/2018, Published: 30/Sept/2018

Abstract—Cloud computing is a new modern and broad concept of the world. Users store huge amount of data on cloud storage for future use. Now a day's privacy to the data stored in cloud is an aspect and security is a very major challenging mission in cloud computing. These challenges have huge effect in the development of secure data storage qualities of cloud system. The objective of this paper is to provide the privacy two factor authentication (2FA) techniques algorithm for the cloud environment with an attempt to bring solutions of such problems. The main aim of this paper is to design and propose Two-Factor Authentication (2FA) technology with One-Time Password (OTP) and finger print for providing strong security system to the data stored in cloud system. This paper, presents two modules, the first module deals with ensuring the storing security of data in encrypted format by using the (2FA) technique and the second module with digital signature algorithm (DSA). We have proposed framework which provides, verifies user authenticity using two-step verification, which is based on password, CSP level key establishment between the users and the cloud server.

Keywords—Cloud Computing, 2FA Secure Data Storage Cloud Server, DSA, Encryption and Decryption Algorithm Cloud Storage

I. INTRODUCTION

In the beginning of the 21st century, there is various types of exploring growth related to research in cloud computing. Cloud computing is a rapidly arising technological area with enormous and broad concept of the world. Now a days digital signature is used to verify the cloud server systems. Henceforth this technique expands the assurance that has been authorized to get to secure systems but helps to maintain the security code. Digital fingerprint can also be utilized as a technique for a unique identification number. The user is given the privacy to access and analysis only one key is used for encryption and other equivalent one key should be used for decryption. Thus,the 2F authentication technique is generally a process which is required to access the secure and confidential information. So that authentication user is required to establish three different factors such as smart card, Personal Identity Number and Biometric data, like a fingerprint or the face geometry or eye retina. The main advantage of this technique is to provide high level privacy to the data which is secured in the cloud server system. The performance of the proposed system is evaluated in terms of uploading data encryption time and decryption time [1, 2].

In the present paper, our objective is to simplify the preceding analysis by considering the privacy which is provided for each data by using the 2FA technique. Two factor authentication techniques are cleared then only authenticated user is allowed to access cloud service, because the data are stored in encrypted format [3]. Authenticity deals with correctly identified sender and receiver. Here we have seen that some problems on the basis of cloud which are design, access control methods and authentication techniques [4, 5]. In this section, an attempt has been made to design algorithms and how these problems can be resolved by proposed algorithms.

This paper is organized as follows: Section 1 presents introduction to cloud, digital signature and two factor authentications. Section 2 presents methodology used in encryption and decryption. The section 3 presents development of the new algorithm for 2FA. Section 4 presents digital signature procedure of two factor authentication (2FA) technique. Section 5 proposes privacy encryption algorithm for cloud storage. Section 6 proposes privacy decryption algorithm for data storage. In Section 7 we have presented experimental results and performance of both existing proposed techniques. We have described the working of our proposed cloud system in section 8. And finally section 9 presents conclusion.

II. METHODOLOGY USED IN ENCRYPTION AND DESCRIPTION

In this section, we have proposed methodology which works in steps where detailed description for the privacy method has been shown in cloud computing environment. The proposed method is based on advanced encryption standard algorithm. To provide confidentiality encoded record which keys are arranged one by one to the cloud framework. The main purpose of this work is to store the data securely in the cloud. Proposed method is classified in two categories- one is secure data storage in cloud digital signature algorithm and second is encryption/decryption search in cloud system. Typically, in 2FA a system: At first users register their systems. After registration, user's personal profile will be created for them and it will be stored in the cloud server database. There are several cryptographic encryption techniques available for privacy of cloud computing. The 2FA and digital signature algorithm are to preserve privacy in cloud computing for using standard data encryption privacy algorithms. A privacy algorithm is to propose for data encryption, which is used for secret key of the encrypted data. After encryption, the privacy will be preserved for each data stored in the cloud database [6,7,8]. Furthermore, the sensitive database is identified and design a secure two factor authentication cloud storage environment through encryption and decryption algorithm. The details description of the proposed algorithms framework uses two factor authentication is given in the following stages.

III. PROPOSED ALGORITHMS FOR 2FA

To achieve the confidentiality, digital signature and authentication issue of privacy of the information is most suited for multi-users communication in cloud computing environments. The development of the new algorithm, special unique keyword is taken for making algorithm feasible in real world research area. According to new research in proposed algorithm is new challenges the concept of using 2FA protection for support the data storage security in the cloud. The 2FA technique is also called the encryption and retrieved decryption algorithm. Digital signature algorithm and data encryption standard algorithms are to generate encrypted format only when users fetch the details in cloud server storage. Symmetric encryption standard algorithm is used to store data and secure sensitive information. It means that data encryption standard algorithm maintains the single key, used for encryption and decryption of the personal data encrypted. The decryption of data requires authentication user name, and password. To enhance privacy digital signature algorithm key will be encrypted using two factor authentication (2FA) and stored in a cloud server. Only authorized user can read files and retrieve data on it in the cloud system. Because it is the most popular algorithm to find all the cloud data in a secured system.

IV. DIGITAL SIGNATURE ALGORITHM (DSA)

To make algorithm show the procedure of two factor authentication (2FA) technique is very essiential in modern world to verify the senders identification. Two factor authentication is one of the broad algorithms based on a digital signature processing algorithm. A digital signature algorithm is presented as verification and authentification of data [9]. The digital signature algorithm process consists of an encryption and a secret key. This secret key value is an independent on the specific of the plaintext. The algorithm will produce a different output depending on the specific key being used at that time. The main objective of digital signature technique is to secure stored data by the cloud service provider (CSP) at the cloud server. Following steps in proposed algorithms are given below:

Step 1: User sends the request registration to the cloud.
Step 2: At first each user has to register with the cloud data storage.
Step 3: 2FA clears to get registered users through cloud services.
Step 4: User gets a unique name for each session.
Step 5: After registration, identifies user profile.
Step 6: Generates secret unique key for identification.
Step 7: Users upload encrypted file on cloud server system.
Step 8: During authentication process, verifies the username and password are correct or not.
Step 9: if it is correct the message "successful" login is generated by any application.
Step 10: CSP checks the authorization using 2FA and sends the acknowledgement back to the user.
Step 11: Registered user use thumb impression in digital finger print machine.
Step 12: Receives the message of fingerprint image.
Step 13: Upload and download the data file.
Step 14: Displays the declaration of view security database.
Step 15: else
it is not correct, the message "unsuccessful", again returns to login page.
End if

The general architecture of the proposed system is shown in Figure1, the secure data storage in cloud server. Firstly, the registration process is performed by creating the login system. After login, personal profile is generated for each cloud customer, who are already registered in their systems. The proposed work is used to handle client's name and secret key, thought to be stronger two factor authentication (2FA). Two factor authentications (2FA) are currently the most increasingly new technology which has been designed to secure the user's data.

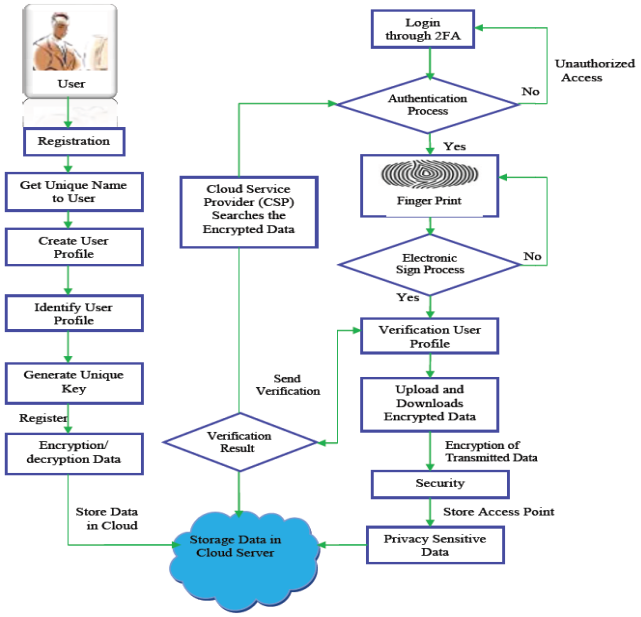

Figure 1: Two factor authentication (2FA) Cloud Server

In 2FA firstly, the user verifies its profile there is only one way to verify the user profile by identifying the fingerprint on the system admin and then the finger print data sends a message to local cloud server. After that CSP helps the user profile data to send it to data centre. If the user profile matches with the data sent to the data centre, it generates an OTP (numeric key) no. that is sent to the system admin. System admin logins the data to verify the entry, if the profile data does not match with the main data of the user, it sends a message to the head for the mismatch of data. Data of all the users are stored in local cloud and each data is collected then it is sent to main data centre, so that the data can be saved permanently and can be secured too. Hence by the use of two factor authentication (2FA) unauthorized user can not access anyone's data. During this research work, there are three types conformations in fingerprint verification process:

- Enrolment: in first step the biometric machine scans the finger image and then the other details of the user, like name and important information are added.
- Storage: after scanning all the details in the first step, they are translated into a unique code and stored in computer. Then all the characters of fingerprints are analyzed which are divided into two parts. Computer with the help of some software identifies the distance between the points and makes a pattern. This pattern helps to make a unique numeric code.
- Comparison: when biometric machine is used, it scans the fingerprints and matches with the data stored in the computer. If the code of fingerprint and the unique code of machine matches, your identification and your presence is observed quickly. If the code does not match, your presence is not observed. Here, the data is stored in the encrypted format by using the proposed two factor authentication algorithm. This technique generates the individual key for client and it stores the encrypted data in the cloud database.

V. ENCRYPTION ALGORITHM FOR PRIVACY DATA STORAGE

The basic motive of this algorithm is to design an encryption algorithm, the encrypted data is stored in the cloud storage server. The importance of this technique is to secure the privacy data of both the encryption and decryption algorithms. In this method, clients have to verify that they know the secret key without sending it to the cloud service provider. Following steps in proposed encryption algorithms are given below:

Step 1: Initialize: get the plaintext letter.
Step 2: Get the fixed key length from the range of numbers (0 to 256).
Step 3: Insert confidential key value from ASCII character.
Step 4: Assigned same fixed value length is considered as a key.
Step 5: Retrieve values of each character of plaintext.
Step 6: Get converted plain text which is equivalent to ASCII code.
Step 7: Encrypts the values using Hexadecimal and $\oplus$ XOR operation.
Step 8: Convert all the plaintext into equivalent ASCII code, and form of square matrix (S_1xS_1 grater then = Ep). Here, Ep is the No. of characters in message.
Step 9: Then ASCII code value for the plaintext applies and converted into Hexadecimal code from left to right in the matrix. i.e. the transpose matrix ($T=T^M$).
Step 10: After replacement the evaluated ciphertext would be ready to saved and sent.
Step 11: Store all the values of T^M in ascending order matrix.
Step 12: Thus we have considered the without space no. of character (Ep) in the message.
Plaintext message = "PRIVACYCLOUDCOMP"
Ep=16(Ep=No. of characters in the message)
Step 13: Then the plaintext obtained above is converted the plaintext into equivalent ASCII code.
So ASCII code value for the plaintext:
80 82 73 86 65 67 89 67 76 79 85 68 67 79 77 80
Step 14: ASCII code value for the plaintext is converted to its Hexadecimal code into character value, can be written in the form:
50 52 49 56 41 43 59 43 4C 4F 55 44 43 4F 4D 50 to form a square matrix 4x4 order.
Step 15: Whole string value will read through loop here only character evaluation has been shown down. Let's it be represent it in the form of a matrix size 4x4, assumes form as:

T =

50	52	49	56
41	43	59	43
4C	4F	55	44
43	4F	4D	50

Step 16: The Hexadecimal code value read the message row by row in transpose matrix T^M. Where T^M denotes transpose matrix 4x4>=16, this can be written in the form as:

T =

50	41	4C	43
52	43	4F	4F
49	59	55	4D
56	43	44	50

Step 17: Now let us give a circular rotation to the first column of the matrix, such that each elements moves one step up elements occupies the bottom most position.
Step 18: Applying the process stores the values from T[0] to T[15] matrix. Then the row assumes the form [T[0]=50, T[1]=41, T[2]=4C, T[3]=43]^M
The same operation performed on all the elements rows.
Step 19: Now, take the even column [2, 4] values rewrite the row wise and odd column [1, 3] values rewrite to the row wise.
Step 20: Encrypt even column [2, 4] values as
[(R_1=>2C_1, R_2=>4C_1, R_3=>1C_1, R_4=>3C_1) (R_1=>2C_1, R_2=>4C_1, R_3=>1C_1, R_4=>3C_1)]
Now also odd column [1, 3] values as
[(R_1=>2C_1, R_2=>4C_1, R_3=>1C_1, R_4=>3C_1) (R_1=>2C_1, R_2=>4C_1, R_3=>1C_1, R_4=>3C_1)]
Step 21: We now to encrypt the message use four different key's and $\oplus$ XOR operation for separately matrix with each row of the matrix.

2 4 1 3

T =

41	43	59	43
43	4F	4D	50
50	52	49	56
4C	4F	55	44

Step 22: Each matrix we are taking four different key's 56 - R_1, 65- R_2, 52 - R_3, and 25 - R_4 message in each row of matrix.

41	=	0100	0001
Key 56	=	0101	0110
		0001(1)	0111(7)
50	=	0101	0000
Key 52	=	0101	0010
		0000(0)	0010(2)

Step 23: Similarly, we apply the next encrypted value into the matrix in the same order. i.e. the same operation is performed on all the even column and odd column.
Step 24: Here, this matrix reads the message column by column. Using the four different key values (key values 4, 1, 2, 3).
Step 25: Now convert the ASCII code into character value as per the algorithm, the cipher text would be:

15	35	04	61
17	26	02	69
15	2A	00	6A
0F	28	1B	70

The plaintext message for "PRIVACYCLOUDCOMP" is:
To find encrypted cipher text is:
ETBNAKSINAK&*(5STXNULLESCEOTiJPa

17	15	0F	15
26	2A	28	35
02	00	1B	04
69	6A	70	61

ETB	NAK	SIN	AK	&	*	(	5	STX	NULL	ESC	EOT	i	J	P	a

VI DECRYPTION ALGORITHM FOR PRIVACY DATA STORAGE

In this section, we retrieve the data from cloud server, decryption algorithm is necessary to get actual data in the cloud. Decryption time is possible only with key values which are used for encryption. Therefore decryption is defined as the process of converting the encrypted into the original text [10]. Here in this section, the reverse process is applied for decryption when user wants to access the file. The importance of this method is that the advanced encryption standard functionality can be managed to provide strong security while storing the data into cloud. Following steps in proposed decryption algorithm are given below:

Step 1: Initialize: generate the ASCII character of the cipher text letter.
Step 2: Count the number of character in the decrypted text.
Step 3: Assigned the same fixed key (K) value used in decryption.
Step 4: The function of decryption is applied to the ASCII character value of the ciphertext character and key value.
Step 5: Came cipher text ASCII character value.
Step 6: Convert all the encrypted text into equivalent ASCII code values.
Step 7: Thus we have considered the without space no. of character (Ep) in the decrypted text and form a square matrix (S_1xS_1).
Step 8: Here, read the letter in reverse process order of the key value row by column.
Step 9: We now to decrypt the message use four different key's and ⊕XOR operation for separately matrix with each row of the matrix.
Step 10: Now, we rearrange into ascending order from T[0] to T[15] matrix.
Step 11: Then to find the transpose matrix $(T^M)^M = T$.
Step 12: Convert all the each character in the encrypted text into equivalent ASCII code values.
Encrypted text:
ETBNAKSINAK&*(5STXNULLESCEOTiJPa
Step 13: We have convert all in the ASCII code values.
15 35 04 61 17 26 02 69 15 2A 00 6A 0F 28 1B 70
Step 14: Now read the message from the in reverse process order of the matrix the key value row by column. The values of four matrix after decryption.

17	15	0F	15
26	2A	28	35
02	00	1B	04
69	6A	70	61

Step 15: Here, we are taking four different key's 56 - R_1, 65- R_2, 52 - R_3, 25 - R_4 message and ⊕ XOR operation for separately matrix with each row of the matrix.

17	=	0001	0111
Key 56	=	0101	0110
		0100(4)	0111(1)

0 2	=	0001	0010
Key 52	=	0101	0010
		0101(5)	0000(0)

Step 16: Similarly, we apply the next message value into the square matrix in the same order. i.e. the same operation is performed on all the matrix.

41	43	59	43
43	4F	4D	50
50	52	49	56
4C	4F	55	44

Now the message is:
50 52 49 56 41 43 59 43 4C 4F 55 44 43 4F 4D 50
Step 17: Then, we rearrange into ascending order from T[0] to T[15] column by column matrix.

50	41	4C	43
52	43	4F	4F
49	59	55	4D
56	43	44	50

Step 18: Now, read the message as row by row from left to right process of matrix.
Step 19: So to find the transpose of matrix $(T^M)^M = T$.

T =

50	52	49	56
41	43	59	43
4C	4F	55	44
43	4F	4D	50

Convert the Hexadecimal code into equivalent ASCII character code value. Then, determine decrypted result is: "PRIVACYCLOUDCOMP" So that, by end of every one of these steps in the decryption algorithm the original text retrieved by the client. Here "PRIVACYCLOUDCOMP" is a plaintext which will be changed to this "ETBNAKSINAK&*(5STXNULLESCEOTiJPa" as cipher text. Using this substitution encrypted data is changed to get a better description. The pair of the keys which includes encryption and decryption messages. Here, secret key is an encryption and decryption keys which verifiability in cloud server storage. These techniques, the same alphabets in the plaintext are rearranged. This technique alone can be satisfied for privacy data storage. If removed bits are equivalent and similar as secret key the succession will progress toward becoming ciphertext as original plaintext.

VII PERFORMANCE EVALUATION OF PROPOSED ALGORITHM

This section, presents the performance results of both existing and proposed techniques. To explore the proposed algorithm's performance, authentication accessing database encryption techniques are used and all the experiments have been performed on Pentium IV 2GHz Intel corei3 PC machine with 4GB RAM, organization MS Windows7. This algorithm is implemented in .Net C# and oracle based cloud. All the runtime reports include both CPU time and I/O time. To show the performance and analysis of time required to encryption and decryption for cloud systems in different input file size has been calculated. This section presents the results of both existing and proposed techniques. The data are stored in the dataset in the encrypted format. We are considering two cases to performe. These techniques are being evaluated and shown in below.

A. Analysis Uploaded Downloaded Files in Cloud Server

In this section, we present the analysis of uploaded and downloaded files in cloud server. We design the algorithms for encryption/decryption and two factor authentications (2FA). The proposed model is being implemented on the different file size of data ranging from 45 KB to 195 KB is shown in Figure 2. Here the experimental evaluation the file is first encrypted before uploading and decrypted in the season of downloading. Therefore some essential performance parameters are getting and running time of the data conversion on the cloud system. In this scheme, multiplicity of authentication technology is a secure cloud based storage where we can store our data in secure group is encrypted. But it cannot store our authentication information in his server. According to table1 graphical view of process time and file size of each and every second the graph is in increasing order. But in this case, if the file size increased from 45 KB to 5 MB then also uploading and downloading time graph is increased [11, 12]. In the following analysis, both the upload and download techniques have been implemented using several input file sizes: 45kb, 85kb, 105kb, 175kb, and 195kb. The table1 below is showing the required time for the process of uploading and downloading to the database.

Table 1: Analysis uploaded and downloaded process for different file size

File Size (in KB)	Cloud Storage	
	Uploading Time (Seconds)	Downloading Time (Seconds)
45	15	05
85	21	15
105	35	39
175	52	51
195	105	55

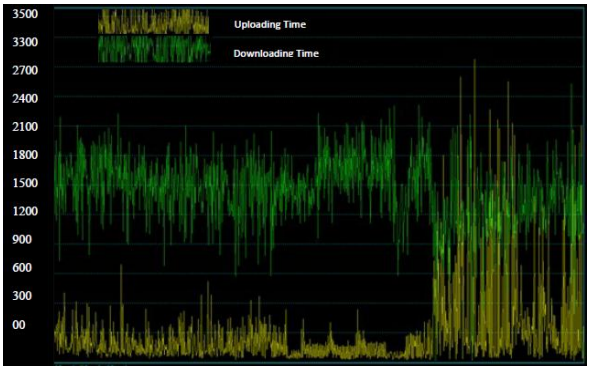

Figure 2 Analysis Uploaded and Downloaded Files in Online Cloud Server

B. Working of Encryption and Decryption Time

This section, presents the encryption and decryption time required, when the users need to protect their information to cloud server and get their information from the cloud server. Figure 3 shows that there is the execution processing time in encryption technique[13,14]. We see the read time increased rates by encryption. Our proposed algorithm takes minimum time for encryption. That is this algorithm compared to the encryption time for both existing system and proposed system. Experimental results are shown in Table 2 and Table 3 show the execution time corresponding to different input file sizes.

Table 2: Execution time in seconds for different input file size

Input File Size (in KB)	Encryption Time (Existing System)	Encryption Time (Proposed System)
45	291	261
85	341	306
105	351	315
175	352	316
195	355	319

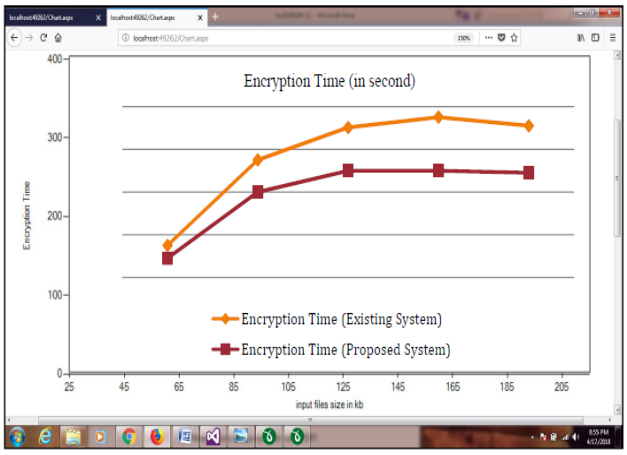

Figure 3 Execution Process of Encryption Time

Figure 4 shows that there is also an execution processing time in decryption with respect to different input file sizes. So that time consumption for converting cipher data back to the original data. The proposed algorithms are implemented in this real time, and performed on the machine requiring minimizing decryption time (ms). Finally, when results are compared and analyzed, we can see that proposed approach (proposed system) takes only minimum time in comparison to an existing system. Hence, we save approx 5 to 10 % time in the proposed system.

Table 3: Execution time in seconds for different input file size

Input File Size (in KB)	Decryption Time (Existing System)	Decryption Time (Proposed System)
45	278	250
85	331	297
105	338	304
175	338	304
195	341	306

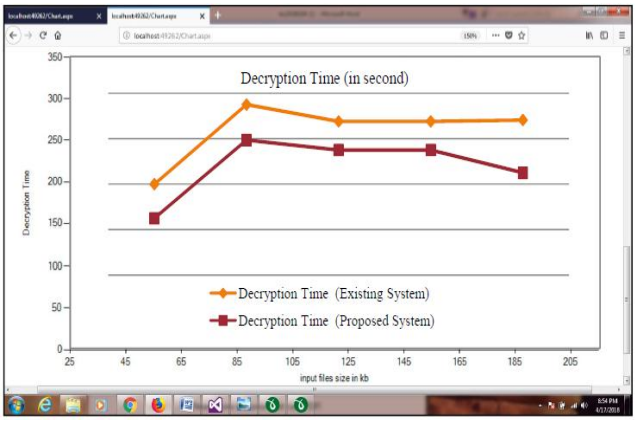

Figure 4 Execution Process of Decryption Time

The encryption time is defined as the process of converting the original data into an unknown format. Encryption technique is the total time required to encrypt format the given data [15]. By the completion of all these steps in the decryption algorithm, the original texts are retrieved by the user. This algorithm utilizes a similar key an incentive for encryption and decryption in before section. Everyone could know algorithm but that key should be known only to authorized user through secure the channel. Generally, on the whole proposed techniques perform better in comparison with other system technique.

VIII WORKING OF PROPOSED CLOUD SYSTEM

To make proposed system easy to work and recognize, this section is describing steps wise step execution of the cloud system.

First screen of the system known as snapshot presents brief preface of the system such as identify of privacy for cloud system copy right in organize.

Figure 5: Snapshot Login Window

Above mentioned snapshot Figure 5 shows the Login Window page through which user could request by assign a unique user Id and password for each authorized user in system. And the next windows shown in Figure 6 will appear, after receiving the user Id and password finger key.

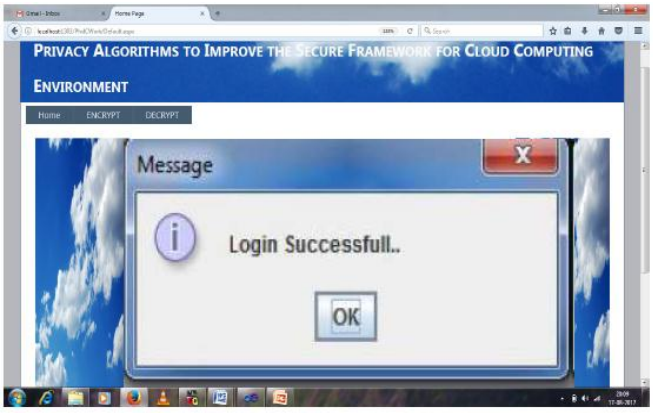

Figure 6 Snapshot Generated by Login Successful

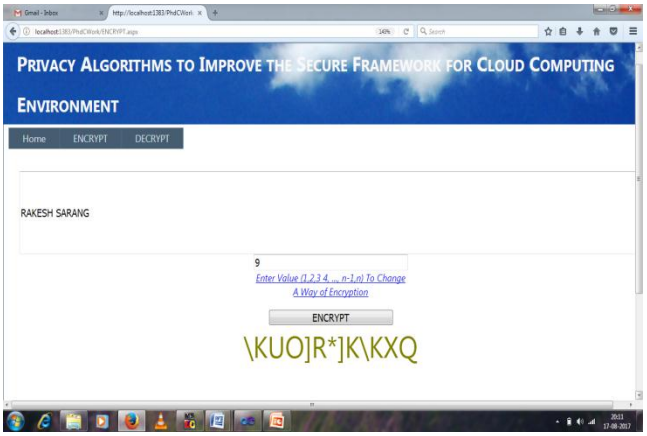

Figure 7: Snapshot Algorithm Selection: for Encryption

In the snapshot shown in Figure 7 is to save confidential information files or data.

1. The encryption algorithm to save confidential information on cloud server with safety by reducing attack probability is applied.
2. The plaintext "RAKESH SARANG" encrypted by key 9 into \KUO]R*]K\KXQ" ciphertext. After that new screen shown in Figure 8 will appear on the system screen.

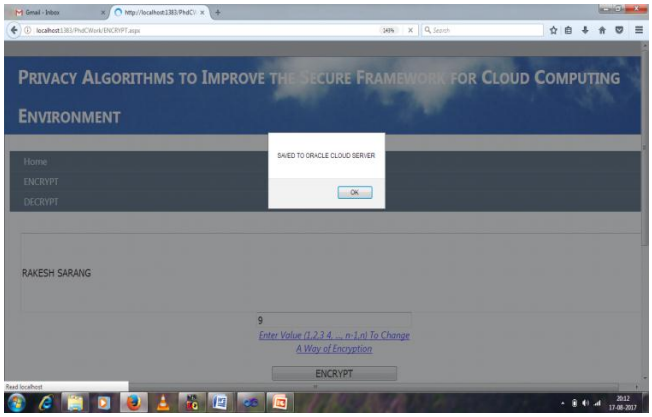

Figure 8: Snapshot Encrypted Text Saving

The encrypted text saved to oracle cloud server which could get back at decryption. After encryption the database, for this new window shown in Figure 9 will appear on the system screen for selecting appropriate decrypted algorithm for privacy.

Figure 9: Snapshot Decrypted by Appropriate key

After selection of algorithms user have to saved all the entire parameter value of ciphertext is called at encrypt, from where user can select a sample cipher information and could get plaintext by applying appropriate defined key as '9' chosen in Figure 7.

To overcome all the above snapshots clear that the entire development work with comparison through assigned

number (That number would be any one from series of integer 1, 2, 3, 4, 5……..n), below mentioned text and the important fact is only that a number can decrypt the text through which it is encrypted.

CONCLUSION

In this paper, we have proposed two factor authentication (2FA) and digital signature algorithm (DSA) techniques to provide privacy cloud storage. To use of these techniques the work is to provide privacy to the stored data in the cloud storage. Because 2FA includes both secret key and authorized user to get secure systems maintained the high security code. Digital fingerprint can also be utilized as a technique for a unique identification number. In this technique we focus on high level privacy and security to the data which is secured in cloud server system. Even though this system is evaluated in terms of uploading data encryption and decryption time. The evaluation shows that this algorithm gives very less time for better performance during execution process of encryption time and decryption time. The future work will focus on more privacy for cloud storage by using different cloud techniques to improve potency based on a digital signature processing algorithm.

REFERENCES

[1] M.S. Monisha, S. Chidambaram,"Enhanced Data Security using RSA Digital Signature with Robust Reversible Watermarking Algorithm in Cloud Environment", International Journal of Electronics & Co mmunication Technology, Vol.8, Issue 1, pp.20-24, 2017.

[2] M. Singhal, S. Tapaswi,"Software Tokens Based Two Factor Authentication Scheme",International Journal of Information and Electronics Engineering, Vol.2, No. 3,pp.383-386, 2012.

[3] N. Mashhadi,"Authentication in mobile cloud computing by combining the tow factor Authentication and one time password token",Vol.37, Part 2 pp. 220−229, 2015.

[4] Y. Kale, A. B. Patankar, "Enhanced Data Security Mechanism on Cloud using two-factor authentication, data encryption and key Sharing Mechanism", Proceedings of 11th IRF International Conference, ISBN: 978-93-84209-27-8, pp.158- 161, 2014.

[5] A.Padmapriya, P.Subhasri, "Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology, Vol.4 Issue4, pp.1067-1071, 2013.

[6] L. Arockiam, S. Monikandan,"Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue 8, pp. 3064-3070, 2013.

[7] T. Sivasakthi, N. Prabakaran, "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 2, Issue 2, pp. 3102- 3107,2014.

[8] M. A. Acha, M. J. Po, "Two (2)-Factor Authentication for Cloud Storage", researchGate,2016.

[9] G. Saini, N. Sharma, "Triple Security of Data in Cloud Computing" ,International Journal of Computer Science and Information Technologies, Vol.5 Issue 4, pp. 5825-5827, 2014.

[10] A. Chaturvedi, D. N. Goswami, R. P. Sarang, "Privacy Algorithms to Improve the Secure Framework for Cloud Computing Environment",
International Journal of Advanced Research in Computer and Communication Engineering, Vol.6, Issue 4,pp.63-69, 2017.

[11] D. Patil, P.K.Deshmukh, "Data Security in Cloud Using Attribute Based Encryption with Efficient Keyword Search", International Journal of Scientific & Engineering Research, Vol.7, Issue 1, pp. 986-991, 2016.

[12] N. Nagar, U. Suman, "A Secure Mobile Cloud Storage Environment using Encryption Algorithm", International Journal of Computer Applications, Vol.140, No.8, pp.33-43, 2016.

[13] A. Khodwe, V.R.Wadhankar, "Security Enhancement for Privacy Preservation in Cloud Computing by Anonymous Request Access", International Journal on Recent and Innovation Trends in Computing and Communication, Vol.4, Issue 1, pp. 233-237, 2016.

[14] An Braeken, A. Touhafi, " Efficient Anonymous User Authentication on Server Without Secure Channel During Registration", IEEE, 978-1-4673-8894-8, 2016.

[15] R. Sugumar, K. A. M. Joycee, "DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm", International Journal of Engineering Research & Technology, Vol.6, Issue 10, pp. 292-295, 2017.

Authors Profile

Anshu Chaturvedi is currently working as Associate Professor in the Department of Computer Applications at Madhav Institute of Technology and Sciences, Gwalior. She has obtained her Ph. D. in 2009 in the area of Security in Adhoc Networks. Her research interests include Security in Adhoc Networks, Sensor Networks, Cloud Computing, Data Mining along with Privacy Preserving in Data Sharing. She is a life member of Computer Society of India and ISTE. She has more than ten years of experience in the academic field and almost eight years of experience in the research field. She has published several research papers in the International Journals and Conferences. She has been a reviewer for IEEE conference paper as well. She won Young Scientist Award by M. P. Council of Science and Technology in 2009.

D.N. Goswami is a Professor and Head in the School of Studies in Computer Science & Applications, Jiwaji University, Gwalior. He is currently holding the post of Director, School of Engineering, Jiwaji University as well. He has done Master of Computer Applications (1989) and Ph.D. in Computer Science (2004) from Jiwaji University, Gwalior. His research interests include Reliability, Software Engineering, Data Mining, Data Base Management Systems and computer Networks.

Rakesh Prasad Sarang is pursuing Ph.D in computer science from jiwaji university, Gwalior india in Privacy and Cloud Computing Challenges: Analysis and Evaluation. He has completed MCA from Department of Computer Application Madhav Institute of Technology & Science, Gwalior MP. His research interests are in the areas of Cloud Computing, Big Data and distributed Computing.

