Privacy Secure Data Two-Factor Authentication(2FA) Encryption and Decryption with Aspect in Cloud Computing

Rakesh Prasad Sarang[1], Anupam Kumar Srivastava[2], Rajesh Kumar Bunkar[3], Gajendra Singh Rajput[4]

[1]Department of School of Computer Science Engineering & Technology, ITM University, Gwalior (M.P.), India.
Email: sarang.nit@gmail.com

[2]Department of Computer Science and Engineering, S R Group of Institutions Jhansi (UP), India.
Email: anupam.srivastava82@gmail.com

[3]Dept. of Computer Science, BBM Govt College Divyagawan Rewa MP. Email: bunkar.rajesh@gmail.com

[4]Department of School of Computer Science Engineering & Technology, ITM University, Gwalior (M.P.), India.
Email: Gajendrasingh.rajput26@gmail.com

***Corresponding author: Rakesh Prasad Sarang, Department of School of Computer Science Engineering & Technology, ITM University, Gwalior (M.P.), India.**

***Abstract*—** In present cloud computing is a new concept of the modern world. Cloud computing consolidates every one of the administrations models and advances together to convey IT capacities. The main objective of this paper is to design 2FAuthentication in cloud system. Utilizing Two-Factor Authentication (2FA) technology with One-Time Password (OTP) providing strong privacy to the data stored in cloud server system. We are proposing a technique to protect data were identified with encryption key secure framework on cloud system. The aim of this paper is to present encrypt and decrypt algorithm. In this paper, we have designed 2FAuthentication techniques algorithm for the cloud framework with an attempt to bring solutions of such problems. 2FAuthentication technology and One-Time Password (OTP) for providing strong security system to the data stored in cloud system**.**

Keywords: Cloud computing, Cloud Storage, Threats, Security Risks, Encryption and Decryption Algorithm.

How to cite this article: Sarang RP, Srivastava AK, Bunkar RK, Rajput GS. Privacy Secure Data Two-Factor Authentication (2FA) Encryption and Decryption with Aspect in Cloud Computing. Int J Drug Deliv Technol. 2026;16(67s):296-300. DOI: 10.25258/ijddt.16.67s.31

I. INTRODUCTION

THE term cloud computing is becoming a new paradigm platform model. It allows the fast technological changes and related research has led to the development of many cloud techniques and services. Now-days providing privacy to the data stored in cloud is an important and security is a very major challenging mission in cloud computing. The increasing popularity, continuing enlargement of cloud computing services is one of the core components in privacy challenges. All information stored locally on a computer can be stored in the cloud, including audio, videos, photos, records, financial information, word processing documents, spreadsheets, presentations and scheduled time calendars etc. In this paper, we have designed two factor authentication (2FA) techniques algorithm for the cloud environment with an attempt to bring solutions of such problems. 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. Two-Factor Authentication (2FA) technology and One-Time Password (OTP) provides strong data security in cloud system. The main advantage of this technique is to provide high level privacy to the data is secured in cloud server system. This technique increases the assurance that has been authorized to access secure systems but helps to maintain the security code. The 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 [1, 2].

II. CLOUD SECURITY THREATS

The threats to information resources residing in the cloud can be different according to the cloud release models used by cloud client associations. There are number of security threats to which cloud computing is vulnerable. In this section presents an outline of the threats for cloud clients categorized according to the confidentiality, integrity and availability (CIA) security model and their significance to each of the cloud service delivery model.

A. Insider User Threats

The threat of assignment of client data within the cloud is better as each of the delivery models might introduce the need for multiple users:

SaaS –is a model of software deployment where an application is hosted as a service to client's access via the internet. cloud client and provider administrators.

PaaS- is another application delivery model. PaaS supplies all the resources required to build. Function developers and test environment managers.

IaaS- IaaS refers to the sharing of hardware resources for executing services, such as CPU processing, memory, data storage and network connectivity. That is third party platform consultant [3,4,5,7].

B. External Attacker Threats

The threat formed from external attackers could be perceived to apply more public internet facing clouds, however all kind of cloud delivery models are affected by external attackers. Particularly in private clouds where user endpoints could be targeted where cloud sources with big data asset credit card details, personal and sensitive information of government or intellectual properties which would subject to attacks from groups, with significant resources, attempting to retrieve data. This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers.

C. Data Leakage Threats

The widespread data leakage may cause threat among many potential competitor groups by the same could provider may be fail by humanoid error or hardware failure those could lead compromise in information saving.

D. Data Quality Threats

The threat of data quality is increased as cloud providers hosted many customers' data. So that preface of faulty component made by another cloud user who could improve potentially impact of the integrity of data to cloud users sharing infrastructure.

E. Technical Issues Threats

Due to some serious malfunction could lead to denial of access to information and data from the cloud anytime and anywhere in world. The fact this technology is always prone to outages and other technical issues. Even cloud service providers (CSPs) got trouble, in spite of maintains high standards of maintenance. Because, consumer needs a very good internet connection (broad band link) to be logged onto the server at all times [8].

III. Cloud Security Risks

The cloud security risks associates with cloud delivery model vary and depend on some factors with sensitivity of information assets, cloud architectures and security control system involved in particularly provided cloud environment. The following we discuss these risks in a universal framework, but where an exact reference to the cloud delivery service model is completed. In this section summarizes the security risks applicable in the cloud computing model.

A. Privileged User Access

Cloud providers commonly provide unlimited access on user data, controls are require to address the appropriate risk on privileges of user access leading to compromised customer information or data.

B. Data Location and Segregation

Clients may not know where their information is being stored and there may be a risk of data being stored along new clients' information.

C. Data Disposal

Cloud data disposal is a risk where hardware issued dynamically to customers according to their needs. The risk of data might not be deleting from data storage, backups and physical media during decommissioning is enhanced within the provided cloud services updates.

D. E-investigations Protective

The ability of cloud to invoke electronic investigations procedures of customer within the provided cloud services could be limited by the delivery models. Those models are being used to access and to evaluate complexity of cloud system. Customers cannot deploy and monitor systems on infrastructure for that they must rely on the systems in use by cloud service provider to support various investigations.

E. Assuring Cloud Security

Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements [9].

IV. Proposed Algorithm for Encryption and Decryption

During the development of the new algorithm, special unique keyword is taken for making algorithm. The idea of proposed algorithm is to maintain or stored data in the cloud. However, it is very complex to manage or store the whole database into web cloud server in one go. A two layer of security for any current website or corporate login. It is necessary to enter the login and password first. Two Factor instantly texts you a pass code in a text message. To authenticate, just reply to the text message with the pass code. Another excellent two-factor authentication product is this one. It consists of two procedures, for example, $Enp = etx - (p/2) + (p \ mod \ 256)$ encryption and $Dep = dtx + (p/2) - (p \ mod \ 256)$ decryption functions. The database of each user is stored in the cloud server.

V. Encryption Algorithm for Privacy

In this section we describe, the encrypted techniques where data is stored in the cloud storage server. The most important of this technique is to secure the privacy data of both the encryption and decryption algorithms [6,10,11]. The general architecture of the proposed system is shown in Figure 1.1, the secure data storage in cloud server.

When the aforementioned step is confirmed, the cloud server waits for the second authentication step, as depicted in Figure 1, and sends OTP to both registered email addresses (OTP1) and mobile addresses (OTP2) [12].

This section is a presentation of encryption technique to make, two factor authentication (2FA) securities in cloud computing

by using two special privacy algorithms.

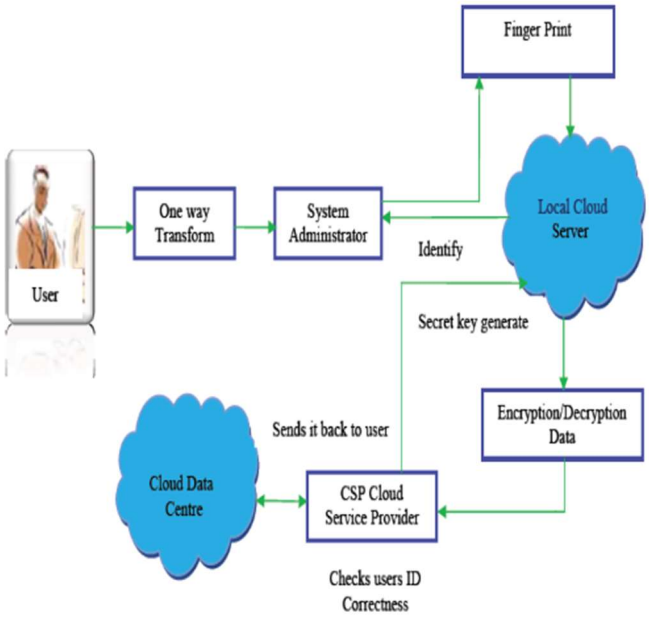

Figure 1.1

Proposed method classified in two categories- one is secure data storage in cloud and second is encryption, decryption search in cloud system. Following notations used during the pproposed algorithm:

etx: Plain text value function
p: Assigned fixed key value
dtx: Cipher text value function

Enp: Encryption
Decp: Decryption

Following steps in proposed encryption algorithm are given below:

Step 1: Get the fixed key length from the range of numbers (0 to 256).
Step 2: Insert confidential key value from ASCII character.
Step 3: Assigned same fixed value length is considered as a key.
Step 4: The converted plain text which is equivalent ASCII code.
Step 5: Retrieve the values of each character of plain text.
Step 6: Encrypted by using the following formula

$$Enp = etx - (p/2) + (p \ mod \ 256)$$

Step 7: Considered the without space no. of character in the message.
Plain text message = "RAKESH"
Step 8: R (ASCII character value) is 82 i.e. R is 82 in decimal integer value.
Step 9: Let fixed key (p) length is 6 to apply the above given formula.

$$Enp = etx - (p/2) + (p \ mod \ 256)$$
$$= \ 82 - (6/2) + (6 \ mod \ 256) = 85$$

Step 10: Now add this key value as per the algorithm, the cipher text would be 'U'. Once data encrypted using an algorithm, it will be transmitted and stored in the cloud database storage.
Step 11: Similarly let the next character from 'A to H'.
Step 12: Similarly let the last character is 'H'.
Step 13: H (ASCII character value) is 72.

$$Enp = etx - (p/2) + (p \ mod \ 256)$$
$$= \ 72 - (6/2) + (6 \ mod \ 256) = 75$$

Step 14: Now add this key value as per the algorithm, the cipher text would be N.
Character level Encrypted cipher text is: UDNHVK.

VI. Decryption Algorithm for Privacy

The encrypted data is stored in the cloud storage server. To 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. There for decryption is defined as the process of converting the encrypted into the original text. In figure 1.2 represents the simplified model for encryption and decryption technique.

Here, you can see that a message is ready to be sent to the receiver. It will first go to the encryption technique where a secret key is used by this algorithm. Now, this key is actually shared between sender and receiver, and no other entity other than sender or receiver must get the key.

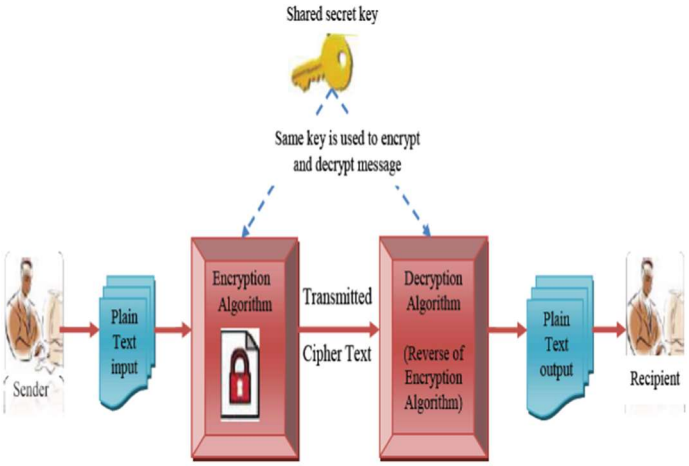

Figure 1.2

Following steps in proposed decryption algorithm are given below:

Step 1: Count the number of character in the decrypted text.
Step 2: Assigned the same fixed key (p) value used in decryption.
Step 3: Let add the key value with ASCII character code.
Step 4: Came cipher text ASCII character values 85.
Step 5: Let fixed key (p) length value is 6, so encrypt the value.
Step 6: To apply the following formula given below

$$Decp = dtx + (p/2) - (p \ mod \ 256)$$

Step 7: 88 is the ASCII value of the Cipher text character 'U'.
Step 8: Here the same key value 6 is used.

Step 9: The function of decryption is applied to the ASCII character value 85 of the Cipher text character and value is 6. Plain text

$$Decp = dtx + (p/2) - (p\ mod\ 256)$$
$$= 85 + (6/2) - (6\ mod\ 256) = 82$$

Step 10: Now subtract this key value as per the algorithm, the plain text would be 'R'
Step 11: 'R' is the ASCII character code the decimal 82. The character R would be the original plain text.
Step 12: Similarly the next character from 'D to K'.
Step 13: To apply the last character is 'K'.
Step 14: K (ASCII character value) is 75.

$$Decp = dtx + (p/2) - (p\ mod\ 256)$$
$$= 75 + (6/2) - (6\ mod\ 256) = 72$$

Step 15: Determine 'H' is the original plain text ASCII character of the decimal is 72.
Step 16: Convert the ASCII code into equivalent character, then decrypted result is 'RAKESH'
Because both are cipher text is UDNHVK and plain text is 'RAKESH'. Decryption is performed to get the original data.

VII. Implementation of Proposed Algorithm

To investigate the proposed algorithm's implementation, validation getting to database encryption strategies are utilized and every one of the experiments have been performed on Pentium IV 4GHz Intel corei3 PC machine with 4GB RAM, association MS Windows10. This algorithm is implemented in .net C# and oracle-based cloud. All the runtime reports incorporate both CPU time and I/O time. To demonstrate the near examination of execution, time required to encryption and decryption for cloud frameworks in various information document measures has been determined. This section displays the consequences of proposed systems. The information are put away into the dataset in the encoded arrange. The current encryption and decoding based systems considered in this work.

Figure 1.3: Snapshot Login Window

Figure 1.4: Snapshot Generated by Login Successful

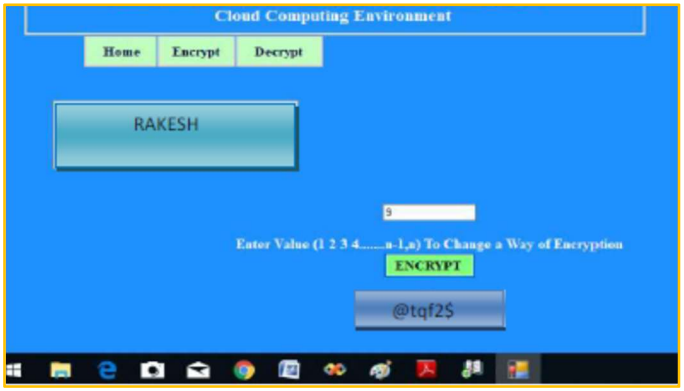

Figure 1.5: Snapshot Algorithm Selection for Encryption

In the snapshot shown in Figure 1.5 is to save confidential information files or data.

1. The proposed encryption algorithm to save confidential information on cloud server with safety by reducing attack probability.

The plaintext "RAKESH" encrypted by key 9 into "@tqf2$" cipher text. After that new screen shown in Figure 1.6 will appear on the system screen.

Figure 1.6: Snapshot Decrypted by Appropriate key

VIII. Conclusion

This paper focuses on the execution process in encryption and decryption techniques. In this paper we investigation different kinds of security risks, threats and 2FA their functionality. This algorithm includes such as, encryption, decryption and 2FA secure storage in the cloud data centre. The main advantages of this effort are only the authorized client can access the cloud storage data. Because privacy cloud computing is vary the way of IT and all sectors. By the completion of all these steps in the decryption algorithm, the original texts are retrieved by the user. Everyone could know algorithm but that key should be known only to authorized user through secure the channel.

REFERENCES

[1] Mashhadi, N., "Authentication in mobile cloud computing by combining the tow factor Authentication and one time password token", *Science*, pp.220-229, 2015.

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

[3] Sriram, I., & Khajeh-hosseini, A.,"Research Agenda in Cloud Technologies", *Methodology*, 2008.

[4] Rao, Srinivasa and V Nageswara Rao, "Cloud Computing: an Overview", Computing, 2008.

[5] Jones, M. T.,"Cloud computing with Linux Cloud computing platforms and applications", pp 1-8, *2009*.

[6] Arockiam, L., & Monikandan, S., "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", *International Journal of Advanced Research in Computer and Communication Engineering", Security*, vol.*2, issue8*, pp3064-3070, 2013.

[7] Krishna, B. H., "Security Issues In Service Model of Cloud Computing Environment". *Procedia - Procedia Computer Science*, *87*, 246-251, Elsevier Masson SAS, Doi: 10.1016, 2016.

[8] Kelkar, S.,"Challenges and Opportunities with Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering,vol.3, issue4, pp 2719-2724, 2015.

[9] Sen, J., & Labs, I., "Security and Privacy Issues in Cloud C loud Computing".

[10] Saini, M. & Sharma, N.,"Triple Security of Data in Cloud Computing", *Journal of Computer Science*, vol.*5*, issue4, pp 5825-5827, 2014.

[11] Subhasri, P., & Padmapriya A.,"Multilevel Encryption for Ensuring Public Cloud", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol.3, Issue 7, pp 527-532, 2013.

[12] Kaur S, kaur G and Shabaz M," A Secure Two-Factor Authentication Framework in Cloud Computing", Hindawi Security and Communication Networks Volume 2022, pp 1- 9 pages,22.