International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I8P101

Volume 72 Issue 8, 1-6, August 2024
© 2024 Seventh Sense Research Group®

Original Article

Password Security using Mutation Technique in Cloud Computing

Priyank Singh[1], Shobhit Kukreti[2], Tanvi Hungund[3]

Independent Researcher, USA.

Received: 01 June 2024 Revised: 07 July 2024 Accepted: 26 July 2024 Published: 12 August 2024

Abstract *- In recent decades, Cloud computing has gained importance in the field, whether it is the IT sector, the Health sector or Supply Chain Management. Thus, due to its convenience, many people are turning towards the Cloud. Therefore, this demand creates the need for a new CSP to come into the market so that end users can store and share their private and sensitive data. Nevertheless, the greatest concern in Cloud Security is the customer's utilization and the prevention of the services. Hence, the following security measures have been taken by the cloud service provider. This paper aims to enhance the level of password protection. To overcome this, we have proposed a password security technique which is known as the string mutation technique to avoid such attacks. Also, the password is stored after applying the md5 hash which is the popular method of converting the plain text password into a hashed format. We have employed them. Thus it can be stated that the described technique can be applied through the Net platform. In the result section, the result of execution has been represented.*

Keywords *- Cloud Security, Password Encryption, MD5 hashing, Data security*.

1. Introduction

Cloud computing consequently has an impact on business in the present era. Cloud computing is not only limited to the IT sector, but it is also implemented in other sectors such as healthcare or manufacturing. As for the developing names, the usage of Cloud systems is increasing among organizations continuously [1]. Despite the fact that cloud management has received broad support, the fear concerning the Security and protection of such systems is still a big issue. These systems could have been efficiently eliminated using the PDAs with fast, creative advancements, thus enabling the clients to exchange videos, papers, photos and other crucial data in various stages and within the organization [2]. Still, a security breach in their cloud data could lead to the leakage of taken information, which, in fact, would result in huge losses. This paper focuses on the area of information technology, where security has always been a concern. Another critical concern is security since Cloud management deals with crucial data from any location via the internet [3]. The consideration of the Cloud and its dispersion of information in various geographical regions increases the likelihood of protection. When speaking about the Security of the Cloud, several points of view are viable, for instance, sharing of information, legal authentication, security of info, and protection. Here are some of the important basic security objectives that are quite relevant to all cloud vendors [4]. Since security is among the factors of data innovation, data encryption has been a significant strategy in the protection of data security. In the past, another approach has been put forth for controlling capable data encryption. These are RSA, DES to AES, 3DES, Diffie-Hellman, and RC4. Each of these algorithms has its advantages together with its disadvantages. These algorithms are well-defined and can be of the symmetric or unbalanced type. Here, our focus is to develop a Cloud Security Network, which should include both the asymmetric and the symmetric encryption key advantages. In the encryption of files, we have employed the AES (Symmetric) method and for passwords we have employed string manipulation.

We aim at having a very broad Cloud Environment with measures of creating and storing usernames and passwords, multiple controls, transfer of customer information and data encryption. The remaining research is structured as below: The second section of the paper, which is section II, elaborates on the aspect of cloud safety. Segment III defines the work to be done where the proposed system and its operations are described. Therefore, Section IV presents the algorithm that specifies the workflow of the entire framework, while its beneficial replication and its outcomes are discussed in Section V. Finally, the conclusion of the paper is presented in Section VI.

2. Issue in Cloud Safety

As we know, data on the cloud is managed and processed. The security risk is on the cloud service providers. This leads to the formulation of beliefs and faith that the CSP has with the customer. CSP is supposed to ensure protection from attacks and ensure that end-user data is not compromised. The following points are mentioned, which need to be provided by the CSP to the end user's data:

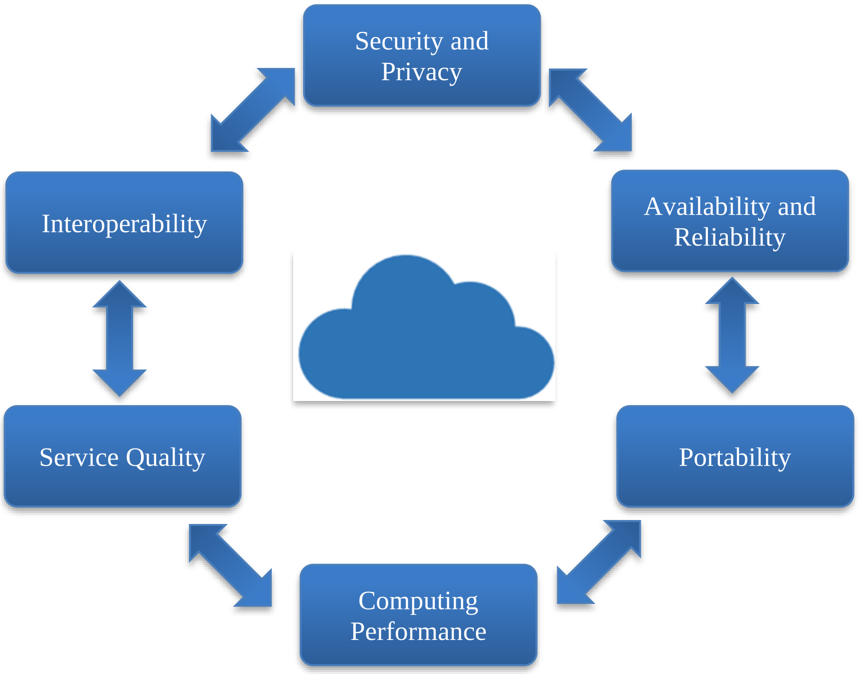

Fig. 1 The main concern on the use of cloud computing services

2.1. Safeguarding of Data

Numerous security breaches occur at the client, CSP and brokers' level in cloud platforms.

Multiple types of SLAs are defined between the cloud users, providers and the agent to outline the particular information theft. As a result, it has been observed that it becomes difficult for the cloud client to verify the information concerning the practices of the cloud provider [5]. Also, there are challenges arising from the basic uncertain positioning of the cloud and the end user, which exposes many organizational threats.

2.2. Data Loss

At times, the application does not employ correct encryption during the data transfer and it results in the appearance of the data in the browser. Some of the common mistakes include SQL injection and Cross Site Scripting (XSS). But the same application also shares the same application pool with other applications and this also leads to security issues. Services such as Azure and Aws have a Tags feature through which one can connect to their instance via a remote desktop. This feature also has one disadvantage; if the user allows this feature to all IPs, then any user can access the instance if he or she gets the pem file and the IP address.

2.3. Hijacking of Traffic

It is, at the same time, one of the concerns that consumers of distributed computing have to deal with when working with it. It was ranked third as the least potent assault by the cloud expert organization in the year of 2013. In such an assault, programmers will, when all is said and done, obtain a customer's security concurrences and gain unauthorized access to its data. Then, all the customer tasks, including the unknown trades taking place in the cloud, are finally provided to a developer [6]. Thus, the programmer can effectively use the customer's data and access the applications running on the cloud. A similar case was observed in Amazon in 2010 when a programmer impersonated the meeting ID to get into the client's records.

2.4. Resource Sharing

In the recent past, the two basic attributes of cloud computing include; Multi Tenancy and Resource Sharing. This vulnerable class encompasses measures, works and resource management such as management, memory, data transfer, and even acting as a mediator for different occupants. Therefore, the cloud provides a separate platform for different kinds of uses from the various clients. Also, this shared asset pool leads to security issues, and thus, the client information becomes vulnerable to data fragmentation.

2.5. Vindictive Insider

Normally, it is observed that the loss resulting from the actions of malicious insiders is much more than anticipated. These attackers use their devices to inject the code into any website of their target. However, there comes into the picture what is known as the Ip jumping technique. In this technique, hackers change their Ip address from time to time to make sure that other genuine users cannot trace its Ip. Following that, the malicious user can easily obtain the file access.

3. Proposed Work

In the past few decades various security mechanisms have been presented in the domain of cloud computing. However, every method is not without its drawbacks. Some methods are restricted to Cloud security; some methods are linked to data breaching prevention techniques; some are related to unauthorized access. None of these methods can be used to solve all these issues at the same time. The proposed method has concentrated on the password security technique and a data security technique using several algorithms in one application to strengthen Cloud security data and user privacy.

3.1. Password Mutation Technique

In this Method, We explain to the users that they need to create their account in our application. When capturing, the User is required to enter the Username, Email, and three passwords, namely, password1, password2, and password3, when the User is registering, though the password should have at least six characters. Then, we alter the password and keep it in the database; we encode the plain text to MD5 before storing it in the database. The mutation is the process of exchanging the characters of the passwords in a way that, for instance, the first character of password one is swapped with the first character of password two, the second character of password two with the second character of password three and so on up to sixth character thus generating a new password.

3.1.1. Encryption of Files using AES

However, there is one symmetric encryption computation that is more acclaimed and is, for the most part, accepted today, and that is the Advanced Encryption Standard (AES). It is much faster than triple-DES both in time and memory usage.

The reason behind the requirement of a new algorithm more than DES was the length of the key. The length of the key used in DES is relatively very short. Due to increasing figure control, it was regarded as vulnerable to extensive key search attacks. Triple DES was proposed with the aim of overcoming the above limitation; however, the algorithm is slow in n and consumes a lot of memory.

The salient characteristics of AES are as under −
Cipher block is Symmetric
Bit sizes are 128/192/256
Faster and stronger than Triple-Des.

AES is a Feistel Network and not an iterative cipher. Hence, it is based on a ‘replacement stage organization’. It’s not a sequence of interrelated tasks, some of which involve substituting contributions for detailed outcomes, and others involve rearranging elements around (modifications).

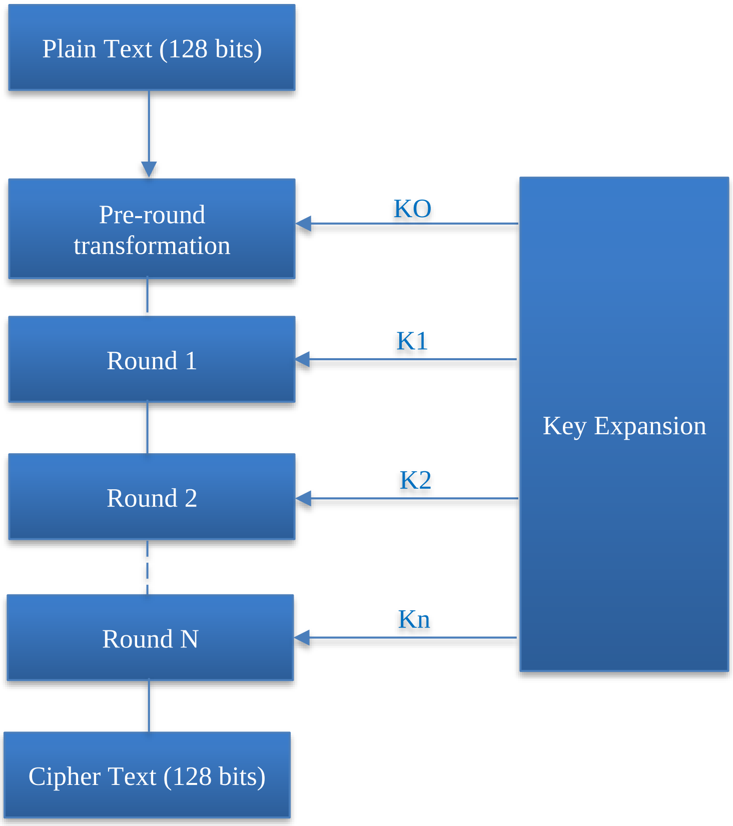

Fig. 2 AES encryption

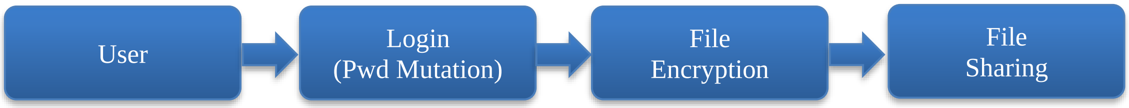

Fig. 3 System design

However, AES implements all its estimations in terms of bytes, not bits, which can be seen as ironic. Consequently, AES operates on 16 bytes, which is 128 pieces of plaintext. The course of action was measured as a network containing 16 bytes and divided into 4 lines and 4 segments.

In comparison to DES, the number of rounds in AES is not fixed and it varies based on the key length. AES applies 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. All of these rounds employ another 128-digit round key derived from the main AES key.

3.2. System Design

Here in this section, we are going to describe the proposed system which we are using in this project. The proposed system entails the following on how we are building a system to safeguard the password of the user and the files in our application and hosting it on the AWS cloud using a Windows instance. The following figure describes the general workflow of the present paper.

3.2.1. Authenticated Entry

A real user can come to our application if he/she wants to use it, thus being able to enter it. They have to fill in their username, Email and three passwords to create an account.

3.2.2. Password Mutation

Password mutation technique is applied in the system. Thus, using this technique can increase password security.

3.2.3. Hashing

The password that is generated is secured by using the MD5 hashing technique to enhance security in the storage of the password.

3.2.4. File Encryption

As for data protection, the system employs AES Encryption to encrypt the user's files. Before saving the file to the cloud server of our system, we ask the user if they want to encrypt the file first. The key we are using in our program has been set to a hard-coded value. Rijndael Managed is a class in the DotNet framework that has properties such as Key KeySize, BlockSize and IV. Using this class, we have encrypted and decrypted the file and presented it in this paper.

4. Proposed Algorithm

Our proposed work describes the steps of the calculation that define the center for it. The analysis describes the functioning of the framework by discussing the entire interaction, from client validation to client information capacity and recovery from the Cloud.

Step 1: Make a new record with Email and Name have three password fields that are Password1, Password2 and Password3.
Step 2: Password generation Based on String Mutation. For instance, there are three passwords: 123456, 234567, and 345678. The string Mutation will then mutate each character.
Step 3: Using the MD5 hashing Technique to the newly created password.
Step 4: Login details are to be filled by entering the Email and three passwords, namely Password1, password2 and password3.
Step 5: We need to hash the password using MD5 to match it with the one stored in our database as the password.
Step 6: Display all the files that are saved in the cloud for the account of the currently logged-in user.
Step 7: To transfer the user's data over the network, we use an FTP and a TLS protocol.
Step 8: AES encryption algorithm is applied for the secure storing of files on cloud technology.
Step 9: The user is permitted to share the files.
Step 10: Other people can look at the files that are shared.
Step 11: The other user downloads and decrypts the file.

Steps 1 to 5 depict the verification process of the users, where the users are required to enter their Email, contact and three passwords. The string mutation happens and is depicted in the next figure.

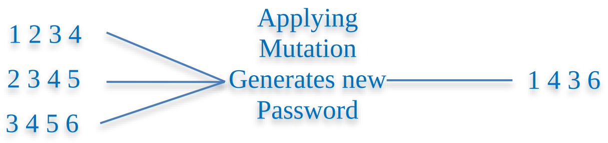

Fig. 4 String mutation

In the 6th step, the User will be able to see the list of files that he has uploaded earlier on the application. Steps 7 and 9 allow the User to share files with other users. The files which are to be shared must be secured in the form of codes. To encrypt the file the algorithm used is AES. In Steps 10 and 11, the User is able to view the files and also download them if they wish to.

5. Implementation

The above said system is developed in Asp. It is a network developed with c# which is a programming language that employs a dotnet framework that has many predefined classes.

We have incorporated password mutation with the help of these classes. For the string mutation, we used the string array and split function of this framework.

In this case, for MD5[8] hashing we have used an MD5 class that has a function named Create and compute hash. The compute hash function has an input of a string, in this scenario, the mutated password. This function produces a byte array. Once the return value is obtained as a byte array from this function, the Append function of the StringBuilder class is used to append every byte using a for loop, and this results in a new hash password. This hashed password, along with the email and name, is saved in the database.

The same technique is used to compare the password when the user enters the account details to log in. To display the list of files which the user can view after successful login, the following technique is used, it is known as Entity Framework, which is the ORM provided by Dotnet framework.

For file encryption, Dotnet has an Aes class, which has a created function.

Rfc2898DeriveBytes [12] is a constructor that takes parameters as encryption key and byte length where the byte length is optional. This class has a member variable named key to assist with setting the key of the byte value. FileStream is a class that has parameters of path and mode. The path is the source from which files that are to be encrypted are chosen, and the mode is the way to create new documents or open existing ones. The goal, in our case, is to create the file in the particular directory. CryptoStream can be used in order to create the encrypted file, and to set the location of the file to which the user wants to save it. In the file-sharing part, the file upload control that is available in the ASP is applied. net. This control has a property called save as. This function takes the parameter as the location where the file is to be stored in the server. This assists the user in uploading the files to the respective server folder. As for the download section, we obtained the list of files provided by the other participants. Again for download of the files we used the FTP for the download of the files. Thus, we have realized the general approach.

6. Result

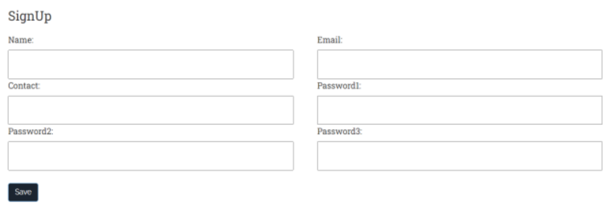

Fig. 5 Registration page

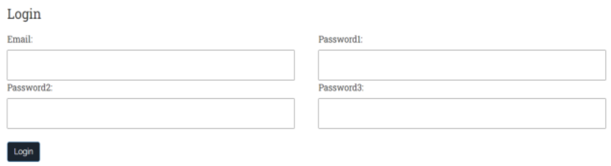

Fig. 6 Login page

7. Conclusion & Future Work

In this paper, the authors have introduced a password mutation technique that strengthens the user's password. We also integrated the MD5 hash algorithm and encryption algorithm for password and file storage security.

In the future, we can replace some other advanced encryption algorithms, and we can also eliminate the constraint of password length from six characters to higher. We also attempt to incorporate the various hashing algorithms and let the users apply the encryption of their preference.

References

[1] S. Subashini, and Veeraruna Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[2] Pramod S. Pawar et al., "Security-As-A-Service in Multi-Cloud and Federated Cloud Environments," *Trust Management IX: 9th IFIP WG 11.11 International Conference*, Hamburg, Germany, pp. 251-261, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] Nikhitha K. Nair, K.S. Navin, and Soya Chandra, "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing," *International Journal for Research in Applied Science & Engineering Technology*, vol. 3, no. 3, pp. 240-244, 2015. [Google Scholar] [Publisher Link]

[4] Wang Cong, et al., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *2010 Proceedings IEEE INFOCOM*, San Diego, CA, USA, pp. 1-9, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[5] Amit Hendre, and Karuna Pande Joshi, "A Semantic Approach to Cloud Security and Compliance," *2015 IEEE 8th International Conference on Cloud Computing*, New York, NY, USA, pp. 1081-1084, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[6] Abhirup Khanna, and Sarishma, *Mobile Cloud Computing: Principles and Paradigms*, Krishan Makhijani, pp. 1-232, 2016. [Publisher Link]

[7] Abhirup Khanna, and Sarishma, "RAS: A Novel Approach for Dynamic Resource Allocation," *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, Dehradun, India, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[8] MD5 Class, System.Security.Cryptography, .NET. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.md5?view=net-5.0

[9] Wei Huang et al., “The State of Public Infrastructure-As-A-Service Cloud Security,” *ACM Computing Surveys*, vol. 47, no. 4, pp. 1-31, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[10] Asish Aich, Alo Sen, and Satya Ranjan Dash, “A Survey on Cloud Environment Security Risk and Remedy,” *2015 International Conference on Computational Intelligence and Networks*, Odisha, India, pp. 192-193, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[11] Aarti Singh, and Manisha Malhotra, “Security Concerns at Various Levels of Cloud Computing Paradigm: A Review,” *International Journal of Computer Networks and Applications*, vol. 2, no. 2, pp. 41-45, 2015. [Google Scholar] [Publisher Link]

[12] Rfc2898DeriveBytes Class, System.Security.Cryptography, .NET. [Online]. Available: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.rfc2898derivebytes?view=net-8.0