SECURITY RELATED ISSUES AND CHALLENGES IN CLOUD ENVIRONMENT

Love Vishwakarma[1], Dr. Ragini Shukla[2] and Dr. S. Pavani[3]

Computer Science, Dr. C.V. Raman University Bilaspur, India[1]

vishwakarmalove23@gmail.com[1]

Computer Science, Dr. C.V. Raman University Bilaspur, India[2]

raginishukla008@gmail.com[2]

Computer Science, C.M. Dubey PG College Bilaspur, India[3]

spavanisantosh@gmail.com[3]

ABSTRACT

Cloud computing is a network-based environment where we use a set of available services and resources through the internet. Cloud computing refers to both the applications delivered as services over the internet and the hardware and software in the datacenters that provide that service. Cloud providers use virtualization technologies for compute the resource where several kinds of data hosted on the some physical server as infrastructure. In cloud computing technologies security has been the major concern. In cloud computing has raised security concern for both service provider and consumer. In this paper we will discussed some major security issues of cloud computing and developed an algorithm using cryptography technique for data security in cloud.

Keywords

Cloud Computing, Threats, Cryptography, Encryption and Decryption.

1. INTRODUCTION

Cloud Computing is a technology that provides online services to the cloud users over the public and private network. With the increase in data volume, data handling has become a big thing. To handle the data of a large company or organization, more storage is required which increases the cost of hardware and software and also increases the cost of data maintenance. To avoid this, all the big companies and organizations have started keeping all their data in the cloud [10], due to which the cost of hardware and software has been substantially reduced. Now it is important to ensure that the cloud server is secure and there is no risk of data hacking or breach. Since cloud allows people to work without any investment and the data of cloud is shared among a lot of users. That's why security becomes a concern for cloud owners [7]. In present time, Cloud Computing is the most popular and useful technology for online services because we can access the data from anywhere anytime. It is an on demand services technology many organizations having its own cloud that provides online facilities to its users or customers. But when we are discussing about cloud , the biggest and major issue is security of data in cloud because all the private or some very confidential data of an organization and also a customer of a cloud are access the data via internet and that can be stolen by the unauthorized person or facing some other types of cyber-attacks [9][13]. So that we can use some security techniques in our cloud to protect the data. Cryptography is the most popular and powerful techniques for online data security where we can change the original data into encrypted mode that are not easy to understand by the other people. The cloud owner provides the best data security to its user, but it is still not enough. Because privacy of data is often in danger. Various types of attacks can occur

on data such as password guessing and in-middle attacks to internal attacks and phishing attacks[11]. This research work lists some safety challenges that are harmful to the cloud.

2. SECURITY RELATED ISSUES IN CLOUD COMPUTING

Maximum businesses are using the cloud due to benefits such as low fixed costs, high flexibility, automated software updates, increased collaboration and freedom to work from anywhere and anytime [8] Also, to store large data of an organization, it does not cost much to maintain any large physical storage and maintain it. So given all these features, many businesses and institutions are using the cloud. Here many organizations are less worried about public cloud security issues and some focus only on cloud services rather than security. These concerns range from the vulnerability of cloud security systems to account hijackings to malicious insiders to full-scale data breaches. An important aspect to keep in mind is the security of a cloud. Despite the increasing awareness about the importance of cloud security, some important security issues need to be addressed to forecast cyber incidents [11].

2.1 ACCOUNT HIJACKING AND UNAUTHORIZED ACCESS

Before reaching the big issues, we move a simple and common issue called account hijacking or intrusion. The biggest reason for intrusion and data braches is the use of legitimate user account by unauthorized parties which include thing like password theft, Phishing attack and social engineering. To avoid this, it is necessary to select strong password pattern and also use strong security techniques to keep the password safe in the database [9].

2.2 INSIDER THREAT

The next security issue to display in cloud computing is an insider threat. An attack from within your organization or team that is working on the cloud and is fully aware of the network system is also a risk that you cannot ignore. Access by authorized parties with the aim of damaging unauthorized similar, cloud environment and the data contained therein is incredibly dangerous. It is too late to detect and know such type of attacks by whom it has been done a lot of cloud confidential data has been stolen or shared. To avoid this, it is necessary to use some complex security system in the cloud as well as use some information of the cloud user such as the mobile number of the user to which one time password or some security.

2.3 APP VULNERABILITIES

The cloud service provider allows its user to access cloud data anytime from anywhere or any platform for which they use software application. The danger in this that all the data can be accessed through that an application then if there is not enough security features for security in that software application, then cloud data can be used by unauthorized third party [12].

2.4 DATA BREACH

When the data kept inside the cloud is compromised or tempered with, it can be prone to data leaks. If the cloud service- or the device connected to it - is broken unauthorized access to sensitive data is done. If unauthorized person accesses this information, then they can distributed

it and misuse it. In this state, when data is transferred from storage this data gets leaked. Since data is stored logically in the cloud, cyber criminals cab distribute cloud data via online or by remembering and later distributing information. In cloud computing this is called low and slow data theft which is a common threat in cloud.

2.5 DATA LOSS

Another storage security risk in cloud computing is data loss. In this, unlike data theft and distribution of data, the data is completely erased. This can be caused by system hacking, a viruses or system malfunctions. When the data is not backed up and there is loss of data then it became an issue for the cloud service provider and also the cloud users [3].

2.6 Denial-of-Service Attack

In cloud computing, an egregious cyber-attack is **Denial - of - service** which is an attack designed to prevent the resources in the cloud from providing their services. DoS attacks disrupt the availability of cloud resources and services and often target the transmission speed or network connection of a computer network. Generally, DoS attacks fall into the Bandwidth attacks, Connectivity attacks, Resource exhaustion, Limitation exploitation, Process disruption, Data corruption and Physical disruption etc. The main purpose of bandwidth attacks is to generate large traffic to use the available resources in the network so that all existing resources are used[11]. Also, victims of connectivity attacks generate flooding conditions by sending a high amount of network interrupts that consume all available operating system resources in the victim and consequently the legitimate user is unable to control these interruptions [12].

2.7 MISCONFIGURATION

A misconfiguration of cloud security settings is a major cause of cloud data breaches. Many organizations that use cloud services do not have enough cloud security management strategies to protect their cloud-based infrastructure. Several factors contribute to cloud data misconfiguration. The cloud can be designed to be easily used and for easy data sharing, it is difficult for the cloud service provider to ensure that the data is available only to authorized parties. In addition, organizations that are using cloud services also do not have full visibility and control over their infrastructure, which means that the user needs to configure their cloud service provider to secure and protect the security technologies provided by their cloud service provider there is a need to trust [12].

3. PROPOSED WORK

Researcher commits step by step process to gather information in order to complete a work. Proposed work of this research can be started in better way with following points.
The proposed architecture represents **EN-Shift Substitute** Encryption process.

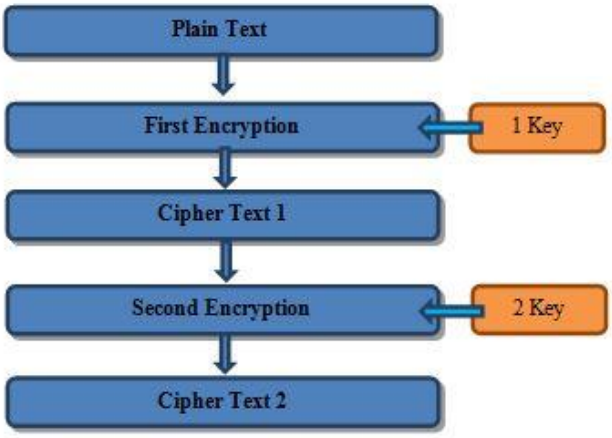

Fig. 1. EN-Shift Substitute Encryption Architecture

The proposed Encryption architecture having five steps which are shown in figure 3.1.

1. **Plain Text** – Plain text is a words or private message that is not shareable to any other person. In the plain text section, the text or message is stored that is to be encrypted.
2. **Substitution Cipher** – Here substitution cipher algorithm are applied to encrypt the data that are stored in the plain text section by using a substitution key.
3. **Cipher Text 1** – This section having a cipher text/data that are encrypted by the substitution algorithm it is also called first cipher text.
4. **Caesar Cipher** – Here the second cipher technique/algorithm is applied to encrypt the first cipher text the cipher text 1 has to be encrypted again by using the other shift key.
5. **Cipher Text 2** – this having the final encrypted data that are encrypted by both Substitution and Caesar algorithms. Here we are getting the strongly encrypted text.

4. METHODOLOGY

Cryptography is a technique using which the true meaning of information is changed to an incomprehensible meaning. This technique is used when we are sending very confidential or private data to someone and want that the data sent is not used by any unauthorized person. Then we change the meaning of data using cryptography technique. Stored data is sent through the network, the probability of data being stolen increases.

There are two-stage of cryptography

- Encryption
- Decryption

The meaning of data is changed using some mathematical equations or algorithms in the encryption method. And the data changed by the decryption method is brought back to its original form.

4.1 SUBSTITUTION CIPHER

Substitution cipher is an encryption technique where plain text is converted to cipher text. In this technique, plain text (Alphabets, Numbers) is replaced with their substitutes (Alphabets, Numbers, and Symbols). In this technique only one key is used for encryption and decryption. In

substitution cipher random key can be used for encryption, in this technique no mathematical formula or equation is used to create encryption key. But the key used in encryption should not contain any alphabets, numbers or symbols repeat. Since a random key is used, it would be difficult to decrypt without a key.

4.2 CAESAR CIPHER

The Caesar cipher is the first and simplest technique to replace a certain number of positions below alphabets in plain text. For example, with a shift of 3, L will be replaced by O; M will become P, and so on. But if **+3** is being used as the key in encryption, then -3 has to be used for decryption.

4.3 ALGORITHM

The algorithm of **EN-Shift Substitute** is given below. The algorithm starts with examining the encryption key and plain text that are to be encrypted by using this encryption algorithm. The EN-shift Substitute algorithm is done under two steps. In the first step plain text is encrypted using substitution key and in the second step received cipher text is again encrypted using shift key.

4.3.1 ENRYPTION (key, ch)

```
SET MAX ← 20
DECLARE i,j,k
SET plaintext [MAX] ← {}, ciphertext[MAX] ← {}
DECLARE Array p[MAX], c[MAX], r[MAX]
DSIPLAY “Enter plain text”
READ the entered data and STORE in ARRAY  p
REPEAT FOR i← 0 to LENGTH(p) BY 1:
REPEAT FOR j← 0 TO MAX BY 1:
IF plaintext[j] = p[i] THEN
ciphertext [i] ← ciphertext [j+3]
END IF
END FOR /* INNER */
END FOR /* OUTER */
DISPLAY “ First Encrypted text”,c
SET Key ← 4
REPEAT FOR k← 0 TO LENGTH(c) BY 1:
SET ch← c[k]
IF ch>=’A’ AND ch<=’Z’ THEN
Ch←ch + key
IF ch> ‘Z’ THEN
SET ch←ch – ‘Z’ + ‘A’ – 1
END IF /* …..*/
SET c[k] ←ch
END IF
END FOR
DISPLAY “Final Encrypted text”, c
```

STOP /* Algorithm ENCRYPTION END Here*/

4.3.2 DECRYPTION

```
REPEAT FOR k← 0 TO LENGTH(c) BY 1:
SET ch← c[k]
IF ch>= ‘A’ AND ch<=’Z’ THEN
SET ch←ch + ‘Z’ – ‘A’+1
SET c[K] ←ch
END IF /* …..*/
END IF /* …..*/
END FOR /* …..*/
DISPLAY “First Decrypted Text”, c
REPEAT FOR i← 0 TO LENGTH (c) BY 1:
REPEAT FOR j← 0 TO MAX BY 1:
IF ciphertext[j] = c[i] THEN
SET r[i] ← plaintext [j-3]
END IF /* …..*/
END FOR /* …..*/
END FOR /* …..*/
DISPLAY “Final Decrypted Text “, r
STOP /* Algorithm DECRYPTION END Here*/
```

5. RESULT AND ANALYSIS

By using EN-shift Substitute encryption algorithm (Substitution and Caesar cipher) then obtained the following result.

5.1 First Encryption (Substitution Cipher)

STEP 1 - Key Initialization

Key='Z','Y','X','W','V','U','T','H','G','F','E','D','C','B','A','z','y','x','w','v','u','t','s','r','q','p',' ','o','n','m','l','S','R','Q','P','O','e','d','c','b','a','N','M','L','K','J','I','k','j','i','h','g','f'.

STEP 2 - Table Initialization

Alphabets = 'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z',' ','A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'.

STEP 3 - First Encryption

Plaintext = Credit

“By using the Substitution cipher, first find the index of character that are present in Alphabets, and then replace the character with their substitute cipher text that is present in Key.”

First Encryption Result = RuHTDs

5.2 Second Encryption (Caesar Cipher)

STEP 4 - Key Initialization

Key = +4

STEP 5 - Table Initialization

First Cipher Text =RuHTDs

Alphabets = 'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z',' ','A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'.

STEP 6 - Second Encryption

First Cipher Text =RuHTDs
Key = +4
Second Cipher Text = VyLXHw

'By using second encryption (Caesar Cipher) get the final encrypted text. In second encryption, each character of cipher text 1 replaced with their +4 index character that is present in English alphabets not in key of Substitution cipher."

5.3 First Decryption (Caesar Cipher)

STEP 1 - Second Cipher Text= VyLXHw
STEP 2 - Key = - 4
STEP 3 - First Decrypted text = RuHTDs

5.4 Second Decryption (Substitution cipher)

STEP 4 - Key Initialization

Key='Z','Y','X','W','V','U','T','H','G','F','E','D','C','B','A','z','y','x','w','v','u','t','s','r','q','p',' ','o','n','m','l','S','R','Q','P','O','e','d','c','b','a','N','M','L','K','J','I','k','j','i','h','g','f'.

STEP 5 - Table Initialization

Alphabets = 'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z',' ','A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'.

First Decrypted text =RuHTDs

STEP 6 - Decryption

First Decrypted text =RuHTDs

Final Decrypted text =Credit

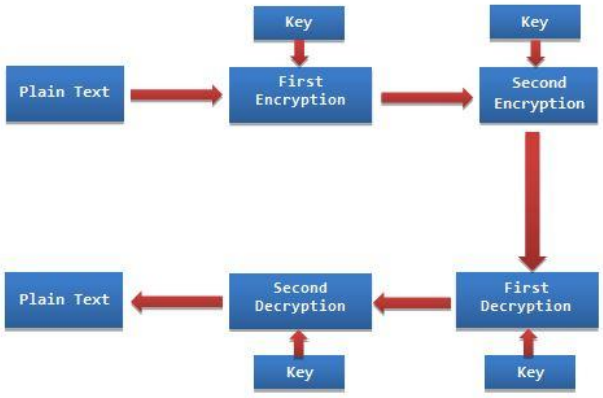

Fig. 2. EN-Shift Substitute Encryption and Decryption

Above figure 2 represent the working of EN-shift Substitute algorithm, here plain text is encrypted by using two different key and encrypted text is decrypted using same key.

6. CONCLUSION

The use of cloud computing has steadily increased over the years, mainly due to the better and simpler feature of the cloud. This provides the facility to store data and access data through internet at a very low cost and very easy. Most of the big and small companies, private and government institutions around the world are making their large data base cloud based. They store and access their public and private data on the cloud through the Internet and are enjoying the services of the cloud. Now that private and public data is being accessed on the cloud through the Internet, some serious cyber-attacks are coming in it. The main purpose of that is to steal and misuse precious data of the cloud. In the present times we hear and read about many such cyber-attacks. In appropriate research, we have used cryptography techniques for data security. We can see that the obtained encryption model uses two encryption algorithm (i.e., Substitution and Caesar cipher) is more secure than the scheme that only uses single algorithm (i.e., Substitution Algorithm) alone. This is because the Caesar cipher algorithm converts the cipher text resulted by the Substitution Algorithm into second cipher by using shift index key.

References

[1] Arya, A. and Ameta, G, "2-key Based Substitution Encryption Model for Cloud Data Storage", International Journals of Research and Scientific Innovation (IJRSI), Vol. 5, no. 3, 2321-2705, 2018.

[2] Bala, S., "Cloud Computing and Database Security", International Journals of advanced studies in ecology, development and sustainability, Vol. 6, 2354-4252, 2019.

[3] Chatterjee, R. and Roy, S. , " Cryptography in cloud computing: A basic approach to ensure security in cloud", International Journal of engineering science and computing (IJESC), Vol. 7, no. 5, 2017.
[4] Choudhari, S. and Bhat, S., "A Research paper on New Hybrid Cryptography Algorithm", International Journals for Research and Development in technology, Vol. 9, no. 5, 2349-3585, 2018.
[5] kumar, V and Vineeth, "Cryptography in cloud computing: A Basic Approach to Ensure Security in cloud", International Journals of Electrical Electronics and Computer Science Engineering, Vol. 035, 2348-2273, 2018.
[6] Kumari, S, "A research on Cryptography Encryption and Compression techniques", International Journals at Engineering and Computer Science, Vol. 6, no. 4, 2319-7242, 2018.
[7] Kumar, P. and Kaur, J., "To propose a novel technique to isolate and detect virtual side channel attack in cloud computing", International journal of computer science and mobile computing (IJCSMC), Vol. 4, 2320-088X, 2015.
[8] Karajeh, H., Maqableh, M. and Masa'deh, R., "Privacy and security issues of cloud computing environment", University of Jordan, 2015.
[9] Prashanth, S.K and Rao, N.S., "Vulnerability, Threats and its countermeasure in cloud computing", International Journal of Computer science and mobile computing (IJCSMC), Vol. 4, 2320-088X, 2015.
[10] Sharma, O., Das, P. and Chawda, R.K., "Hybrid cloud computing with security Aspec"t, International Journal of Innovations & Advancement in Computer Science (IJIACS), Vol. 4, no. 1, 2347-8616, 2015.
[11] Soni, P., Upadhyay, A., Maheshwari, A. and Lakkadwala, P., "Security related issues in cloud computing: survey", International Journal for Innovative Research in Science & Technology, Vol. 2, 2349-6010, 2015.
[12] Singh, A., "Cloud Computing: A brief descriptive review along with its security issues and challenges", International Journals of Applied engineering research, Vol. 14, 0973-4562, 2019.
[13] Venkatesh, A. and Eastaff, M.S., "Study of data storage security issues in cloud computing, International Journals of scientific research in computer science", Engineering and information technology (IJSRCEIT), Vol. 3, 2456-3307, 2018.