IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 1, February 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

An Elevated Approach for Securing Data using Two Factor Authentication in Cloud Storage System

[1] Md. Sohel Ahammed; [2] Md. Nahid Newaz

[1] Dept. of Computer Science and Engineering, Bangladesh University of Business & Technology, Dhaka-1216, Bangladesh.

[2] Computer Science and Engineering, Bangladesh University of Business & Technology, Dhaka-1216, Bangladesh.

Abstract - Cloud computing is an internet-based computing systems where online virtual shared resources are instructed by the user as required on their needs. As our modern technology has a vast amount of digital information which can be managed by cloud computing systems so it is a new mechanism to distribute products from producer to consumer in a very different and effective style of computing. With some advantages of cloud storage system, it has a security flaws in accessing data from another user over the internet. Different types of attack can be done by the third party when sharing file is distributed among the users and hacker will get a unauthorized access to these sharing files. By distributing sharing access or storage with many other users, it is conceivable for another user to hack their data. This paper discusses the two-factor authentications mechanisms(2FA) for the cloud computing security concerns on shared resources and the way for resolving the security risk on cloud computing devices, resources, and the security credentials risk mitigation method or algorithm when a user wants to access a storage system into the cloud.

Keywords - *Cloud Computing, Encryption, Decryption, Two Factor Authentication, Cipher-text, and Plain-text.*

1. Introduction

Cloud computing is a technical term that associates with scalable services, delivering hosted services like accessing, data sharing, processing, etc. over the web-on-demand basis. It provides an including space for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate branch [1]. Cloud storage typically refers to an object storage services like Google, Microsoft Azure, and Amazon S3 Storage. Cloud computing can be defined as the use of new or existing computing hardware and virtualization technologies to form a shared infrastructure that enables web-based value-added services [2]. Depending on the size of business and requirements of infrastructure support for day to day operations, every company needs different services from cloud service provides also individuals will demand services as per their requirements [3]. For example, if a consumer uploads/stores his personal data such as files, images, videos he can synchronize to other devices from anywhere through some apps or web. An Entrepreneur hosts their apps in the cloud and operates components and services from cloud service providers, such as computing API, Virtual Machines, database, and storage, and so on etc. Cloud computing systems are consisting of large numbers of data manipulations, network, and storage devices across the widely or randomly distributed area and multiple holder can engage on the cloud systems synchronously with different resource requirements. This technology allows access to large amounts of computing power in a virtualized manner by assembling resources. One of the most recently computing area is named as Big-Data. In that area, it is an excessively successful paradigm of service-oriented computing and has revolutionized the way of computing infrastructure is used. Three most popular cloud paradigms include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) Figure 1. The concept, however, can also be extended to Database as a Service or Storage as a Service. That infrastructure needs to be secure during making cloud computing on storage devices.

Because this outsourcing data storage also can arise the security attack. When a file is distributed locally or broadly over the internet media, then at the same time it has more high-security risk that file can be unauthorized access by another user, that means, the higher distributions of locations, the more higher risk on accessing data. For example, If Alice wants to share a piece of data (e.g. a video) to Bob but it could be difficult for her to send it by message or email due to the plenty size of data. Instead,

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

Alice uploads the file to a cloud storage system (like google-drive) so that Bob can download it at any time. But in that case, if Bob can share this link or data to another user then there is a chance to create a security attack for authorization to access data but Alice doesn't know whether bob share his data or not. So, by sharing storage and networks with many other users it is also possible for other unauthorized users to access your data. This action can happen on promising the request from third-party users or to do criminal activities on shared access data. Although a user can access this data by giving password or username on the web or app but this method is not suitable for uploading or downloading data from the cloud. As cloud computing systems can be used on large or small-scale organizations but main problem is data is stored at any physical locations. So, the third-party API can easily access to take down the data from these physical locations. In that case, a bright solution to secure data on the internet that is encryption-decryption technology. Encryption means protecting the data from the unauthorized users through the network communications systems and decryption means at the end user systems, data can be retrieved from network according to a special key. From this encryption-decryption technique even if another user has access the cloud which is encrypted before but he cannot decrypt data because he doesn't know the encryption-decryption key in this network.

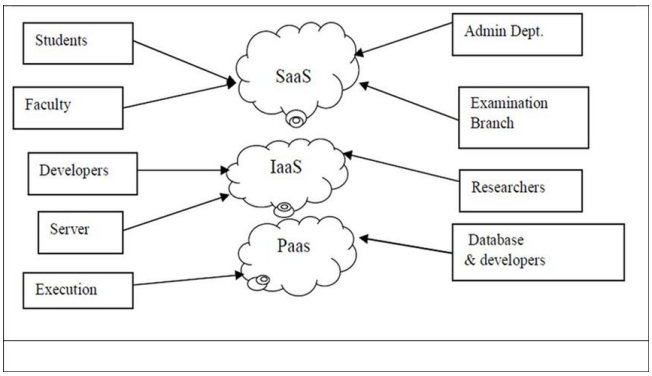

Figure 1: Data flow and storage in cloud

2. Encryption-Decryption Mechanisms

Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers [4]. Before choosing encryption-decryption process one has to learn how the key can be generated and how the asymmetric encryptions allow only public information to generate ciphertext and the other end (receiver) decrypts this ciphertext by using his private key. By definition, there is a one single private or secret key and corresponding public key or user's identity in asymmetric key distribution. By using this private key user can decrypt the ciphertext to get information. A password protection on this secret key which is saved on a personal computer so that anyone cannot access this key but the 2FA techniques can be more powerful to secure process.

2.1 Different types of Mechanisms of 2FA

We need to illustrate some approaches for establishing of security on cloud computing systems and what are the factors on taking these approach as a pure solution to remedy for security attack. As this reference are collected from different types of books, conferences, thesis paper so anyone can implement this idea in their projects.

2.1.1 *Double Encryption Method*

In this method, the process of encryption will be executed twice. First, a user encrypts the plaintext or message with his public key and then again encrypt it with public key or serial key number of security device where a security device has a unique serial number. In Decryption step, the security device first decrypt once then the partially decrypted ciphertext is passed to the computer which is used by the user as his secret key again to decrypt it, shows in as (1) and (2). Insecurity device, additional public key is required to decrypt the whole message.

$$\text{Ciphertext} = E_{sd}(E_k(\text{plaintext})) \quad (1)$$

$$\text{Plaintext} = D_k(D_{sd}(\text{Ciphertext})) \quad (2)$$

In double encryption method, there are some problems. When the security device is lost then other ciphertext from the cloud cannot be decrypted. In that case, user needs to know the serial number to decrypt the ciphertext. For this reason, the encryption-decryption process can be more difficult.

2.1.2 Attribute-Based Encryption (ABE)

The main feature of ABE algorithm [5] is collusion-resistance. That means when program tries to hold multiple keys of ciphertext only that keys are adopt to accept data when keys grant access from the system. ABE is a public-key encryption system in which the private key of the user and ciphertext are dependent on attributes. Only decryption can be possible if the set of attributes of user key matches with the ciphertext attribute. The steps are below:

a) Select File attribute1 – make File name atr-1

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

b) Convert the file name to binary codes

c) Select File attribute 2 – make file size atr-2

d) Convert the file size to binary codes

e) Execute AND Operation of atr-1 and atr-2

f) Execute OR Operation of atr-1 and atr-2

g) Result of AND Operation Stored as Secret Key

h) Result of OR Operation Stored as Public Key

2.1.3 Divide the Secret Keys into Two Parts

In this way, only divide the secret key into two parts, one part is stored on computer or personal hard drive and another part is planted on a security device. In that case, one part cannot decrypt the ciphertext without using other part. Suppose Alice send a secret key to Bob. Before sending it, Alice divide his ciphertext key into two parts. Bob will not decrypt the ciphertext until he can download the security device secret key. If Alice permit or share the link to Bob then he can download the second part ciphertext key. But there is a problem on this approach. If the attacker can go through ciphertext code, he can put a breakpoint after Alice counterattack on the key. Basically, this not a worst method to grab the key a bit by bit to make him work for it a little, but this is not really possible to hide keys in a security device. Again, if the security device is lost then bob couldn't download the ciphertext keys second part. So, he need to issue a security device for generating original plaintext. When Bob replace a security device with a new security device from the authority, the private key generator (PKG) will replace the same bits on device. But it has a disadvantage on way that if the security device is stolen another user can break his personal computer to retrieve the other part of the secret key.

For example, when a user makes a transaction in online banking system, he needs to access his security device for authenticate into the system. But if he lost his security device, he could not login onto the system also at the same time he could not manage another security device and he will not use previous security device anymore if he reports on it.

2.1.4 AT&*T and Druva NetBond for Cloud Ecosystem*

In the cloud ecosystems, AT&T and Druva also use 2FA techniques to protect message from an unauthorized user. But the systems can be suffered from a potential practical risk. In druva system, first, a user encrypts a message upon a user key k_1. Then he uploaded his key to the cloud server. In the cloud server user key k_1 is encrypted with another private key k_2 and saved in that server. The User hold the key and in order to decrypt the ciphertext then he needs to key k_2 to get key k_1 shows in as (3), (4) and (5)

$$K_2 = E_{k1}(K_1, \text{plaintext})) \quad (3)$$

$$\text{Ciphertext} = E_{k2}(K_2) \quad (4)$$

$$\text{Plaintext} = D_{k1}(D_{k2}(\text{Ciphertext}))) \quad (5)$$

2.1.5 Identity Based Encryption (IBE)

IBE means a user needs to know the identity of receiver in order to send the send encrypted ciphertext or data. Then the user uploads the ciphertext to cloud server system where the receiver end can download the data at any time. Besides the user need not any know information that means any public or private key of the receiver. IBE uses 2FA technique to resolve security issues on the both side Figure 2.A.5. Suppose, Alice store the ciphertext on the cloud which is previously encrypted with his public key. The file will be decrypted from the server by using the sender personal security device key which is connected to the computer. Here the secret key only stores to the user computer. So, in IBE the user needs to get two parameters, one is computer saved secret key another is security device (like USB/HDD) secret key. Here, if user lost his security device, he will revoke another device from the authority. When he revokes a new security device (SD) from the authority, that SD modifies the ciphertext according to his secret key and again regenerate the SD key to the user. So, the attacker could not get any chance to modify the ciphertext to gain access in the cloud system at any circumstances. Ciphertext cannot be decrypted by the cloud server at any time without other piece.

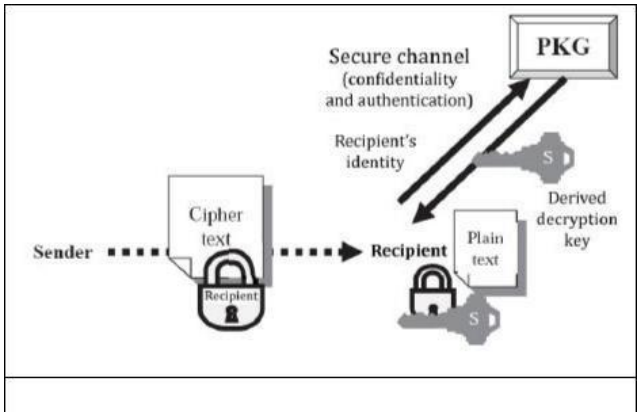

Figure 2.A.5: Identity-Based Encryption (IBE) System [6]

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

2.2 2FA Data Security Protection Mechanism for Cloud Storage System

In this mechanism, the receiver gets an encrypted message which is send by the user form the cloud storage server. As same as IBE method, the sender only knows the identity of the receiver but he doesn't need any other info like private or public key. The encryption process is executed twice. First user encrypts his message with his public key or his identity. Then again encrypt it corresponding to the public key or serial number of the security device. For decryption process first, the ciphertext is decrypted once with help of receiver private key. Then the resulted partially ciphertext is passed through a personal computer where other part of key is stored and that ciphertext is finally decrypted with the help of a security device serial number. Here some major concerns during performing this algorithm.

2.2.1 *2FA Online Certifying Authority*

Some certifying authority are also working on revoking the public keys. One is Security-Mediated Certificate less (SMC) cryptography. In SMC system user has a public key, secret key, and identity of himself. For encrypting the message or signature verification user needs the public key and the corresponding identity himself. In order to get the message or decrypt the ciphertext user needs the SEM and his secret key. As Security Mediator (SEM) is operated from the main certifying revocation authority they can deny any revocation use to give key if they are already blocked from their server. Here SMC can solve the revocation problem. But it is dissimilar from IBE system. Because only user need to know the public key corresponding to identify himself.

2.2.2 Two Secret Keys on Certificateless and Certificate-based Cryptosystem

For decryption of secret keys, there are two approaches. One is certificateless cryptosystem (CLC) and another is certificate-based cryptosystem (CBC). In CLC based cryptosystem, the identity will be fixed for a user and he choose the secret key along with public key. With the help of user identity, the private key generator (PKG) will generate a half or partial secret key. CLC is embedded on Public Key Infrastructure (PKI) and Identity Based Cryptosystems (IBC). The encryption process is done by the user's identity and his public key information. The decryption process is done by the knowledge of secret key and partial key information by KGC as Figure 2.B.2. As there is no certificate, user don't need identity of himself and the signature verification still need public key.

Certificate more generally known as signature which is given by the KGC and acts not only a certificate but also as a decryption key. In encryption process, public keys are used along with user's identity and in decryption process, the signature are validated by a latest certificate and done by a certifying authority as a secret key of user himself. The most common example of CBC is Digital Certificate, Figure 2.B.3. On digital certificate, entire information is digitally signed by CA and includes digital signature in the certificate. The CA accepts the application from a client to certify his public key. After verifying identity of client, he can issue a digital certificate.

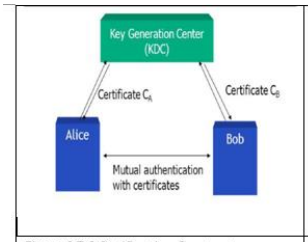

Figure 2.B.2 Certificateless Cryptosystem (CLC)

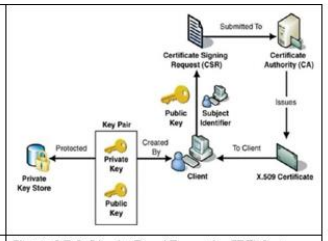

Figure 2.B.3: Identity Based Encryption(IBE) System [7]

2.2.3 *Computation of Secret Key on Security Device with Cryptosystem*

The limitations on computations of secret key security device is reserved, but this is physically stable and secure. There are two types of keys are stored in security device, one is short term key and another is long term key. By comparison of these keys, short term keys are more powerful secure than the long term keys in the system. Long-term keys that means public keys are stored in the system at life time where short time keys are computed by discrete time. It is done by with the help of user interaction. When a user issues a new secret partial key from the security device, it will add to the previous key of security keys and made a new combine security keys to the user. At each time session, the user can get a partial secret key from the SD. But in 2FA system when the key is updated from cloud server then there is no further need any information if key updated or not during the whole process of encryption and decryption. That means the security device doesn't need every time to decrypt the ciphertext that is we don't need any time to time synchronization into the system from cloud server.

2.2.4 *Issue a new Security Device using Cryptosystem*

As 2FA cryptosystem is based on a IBE method and newly revocable IBE is demonstrated by Boneh and

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

Fnaklin [8]. It is based on identity (id) and a time period T, a ciphertext is encrypted, and by using a PKG a private key $sk_{id,T}$ is generated by non-revoked user such that the user can access the data in T. Basically the revocable IBE system is associated with a tome based period. If decryption process is waited from next time period then next secret key is created by PKG for next time session period.

3. 2FA Mainframe Architecture

Our 2FA mainframe architecture is divided by some blocks. Suppose in general data distribution through cloud server, Alice (sender) encrypts the data with the identity of receiver. Then uploads the ciphertext to the cloud server. Here this ciphertext is a first level ciphertext to bob. Bob generate the second level ciphertext in the cloud server with his security device. After generating second level ciphertext from the cloud server, Bob downloads this ciphertext. Then he (bob) decrypts the second-level ciphertext using his private key and security device. Figure 3.1[9] describes that situation.

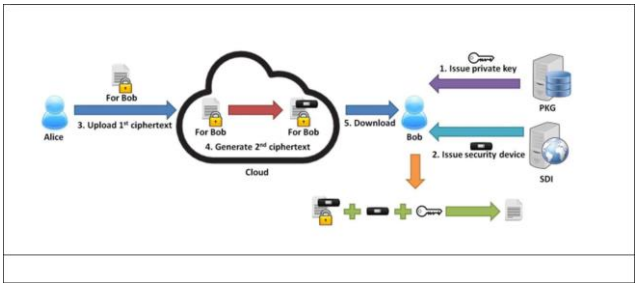

Figure 3.1 Data Uploading and Sharing System [9]

If the security device is lost from Bob, then he reports to SDI manager to issue a new certificate from the authority. When SDI issues a new security device to Bob, it sends a request to Bob for updating the ciphertext along with a special security key from the cloud server. In this process, old security cannot gain access to the cloud server. Finally, Bob can download them from the cloud with his update ciphertext secret security key and decrypt the message. Figure 3.2 [9] depicts the process below.

Here, private key generator (PKG) is a trusted authority source responsible for issuing new private key of every user. In this architecture, there are two different encryption mechanisms are used, one is IBE and another is PKE. Here constructing a second level ciphertext from the security device, which can assure to the whole system that the cloud server cannot gain any knowledge of message by accessing the special key.

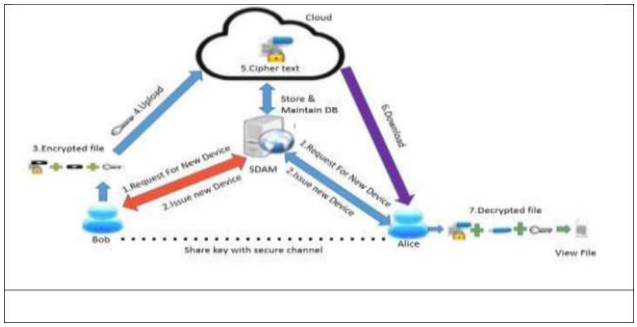

Figure 3.2 Issue a Security Device and Updating the Ciphertext [10]

4. Conclusions

This paper demonstrates that 2FA systems is a secure process for sharing the data into cloud server. If we avoid the data distribution from multiple access from the unauthorized user, this process will be very efficient in the cloud computing sector. This system target is to enhance the security and confidentiality of the data and give the revocability of the device. Once the device is revoked then SDAM will offer new unique or personal security device to user.

Acknowledgments

We are grateful to Bangladesh University of Business and Technology for giving us an opportunity of use its infrastructure and Prof. Dr. M. Ameer Ali for giving us his valuable instructions and guidance.

References

[1] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,"IEEE Transactions on Parallel and Distributed Systems, vol. 27, pp. 340–352, 2016.

[2] Joel Gibson, Darren Eveleigh, Robin Rondeau, Qing Tan,"Benefits and Challenges of Three Cloud Computing Service Models", 978-1-4673-4794-5/12/$31.00_c 2012 IEEE".

[3] G.A.Patil,S. B. Patil, "Data Security Mechanism for Cloud", International Conference on Emerging Technology Trends (ICETT) 2011 Proceedings published by International Journal of Computer Applications (IJCA), pages 24– 27, 2011

[4] Sanka, Sunil, Chittaranjan Hota, and Muttukrishnan Rajarajan. "Secure data access in cloud computing." Internet Multimedia Services Architecture and Application (IMSAA), 2010 IEEE 4th International Conference on. IEEE,2010

[5] Bethencourt, J., Sahai, A. and Waters, B., 2007, May. Ciphertext-policy attribute-based encryption. In Security

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.

and Privacy, 2007. SP'07. IEEE Symposium on (pp. 321-334). IEEE

[6] Weber, S.G., 2013. Designing a Hybrid Attribute-Based Encryption Scheme Supporting Dynamic Attributes. IACR Cryptology ePrint Archive, 2013, p.219.

[7] (TutorialsPoint Online Sources) Web Resources (year, month, day). Title (edition) [Type of medium]. Volume (issue). Available: https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm

[8] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO '01, volume 2139 of LNCS, pages 213–229. Springer, 2001.

[9] Liu, J.K., Liang, K., Susilo, W., Liu, J. and Xiang, Y., 2016. Two-factor data security protection mechanism for cloud storage system. IEEE Transactions on Computers, 65(6), pp.1992-2004.

[10] (PDF Online Sources) Web Resources (year, month, day). Title (edition) [Type of medium]. Volume (issue). Available:http://www.ijariie.com/AdminUploadPdf/Improve_Data_Security_Protection_Mechanism_For_Cloud_Storage_Using_Two_Components_ijariie3292.pdf

First Author Md. Sohel Ahammed is working as the lecturer at dept. of Computer Science & Engineering at Bangladesh University of Business and Technology, Dhaka, Bangladesh. He has achieved B.Sc. Engineering in Computer Science and Engineering from Rajshahi University of Engineering & Technology (RUET) and pursuing M.Sc. IICT at BUET. Three publication has been published in international refereed journal and conference. His research interest is like Artificial Intelligence, Pattern Recognition, Deep learning, Data mining, and Cyber Security.

Second Author Md. Nahid Newaz is currently working as a lecturer at Computer Science and Engineering department at Bangladesh University of Business and Technology (BUBT). He Completed his B. Sc. Degree from University of Dhaka in 2015. His primary research interest is Machine learning, cloud computing, data mining, and network security.

Copyright (c) 2019 International Journal of Computer Science and Network. All Rights Reserved.