International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||02||Pages||1040-1044||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i02.ec03

Secured Auto Encryption and Authentication Process forCloud Computing Security

Mst Zannatun Ferdus, Md. Hasan Monsur, Mst. Jahanara Akhtar, Saiful Islam

Washington University of Science and Technology
New Jersey,USA
Dhaka University of Engineering and Technology
Gazipur, Bangladesh
Professor
Dhaka International University
Dhaka, Bangladesh
Dhaka University of Engineering and Technology
Gazipur, Bangladesh

Abstract
In the IT sector, cloud computing is a rapidly expanding technology. Users are being offered more and more flexible and appropriate services by cloud service providers (CSP). Cloud computing users are increasing at a steady pace. Users and CSP are looking for appropriate security measures as cloud computing becomes a need in modern life. A large number of researchers are studying cloud computing security issues. This work introduces an appropriate cryptography and secure user authentication system, which includes auto encryption and a mechanism for updating keys on a cloud site that is not initially accessible to users. After a predetermined amount of time, this operation will recur frequently on the cloud site. This protocol can be carried out manually by CSP at any time, or it can run automatically after a predetermined amount of time. This will guarantee additional data security. Additionally, this procedure adds a level to the user's credentials. Even with legitimate credentials, these feathers will ensure that hackers cannot obtain original files or data. The suggested protocol is emulated by CloudSim, and we saw that there is an additional step requiring user credentials, requiring some time to access files or data for the first time. Although this small amount of time is insignificant and can be disregarded, it significantly improves security.

Keywords: Auto encryption; Cloud Computing; Security; Cloud Service Pro-viders.

1 Introduction and Related Works

To date, cloud computing is becoming a vast growing technology in IT industries. It has a great impact in various sectors which is why many organizations are involving to this technology and offering various services [1]. Security is a major issue in cloud computing. Although cloud computing is helping to make human life easier and simple, it has a fear of security aspect. Users and CSP always keep in mind fairness aboutsecurity of stored data or files with proper credentials. Peoples are storing and sharing real time video, audio, photos etc. contents by using mobile phone in cloud environ-ment [2]. A proper security technique can make more comfortable and prevent from data loses or stolen by hackers or intruders.

In all area of IT industries, security always consider as a dominate field. In cloud computing, security always plays a vital role for quality of services (QoS). Cloud computing handles with critical data and it can be access from anywhere of the world through internet. So it makes security as an important concern area [3].

Cloud computing has a vast growing nature in massive area of the world. So it has a high risk. When any industry wants to go with cloud computing, it considers various aspect or goals of risk such as proper authentication, data security with privacy that should be integrated with services [4]. Some authors considered Data Protection, Loss of Data, Traffic hijacking, Isolation of Resources and Malicious Insider as security con-cern [10]. Amit Hendre et. al. [5] analyzed various security threats such as Data breaches, Data loss, traffic hijacking, Insecure interfaces as well as APIs, Denial of service, Malicious Insiders, Misuse of cloud facilities, Inadequate due industry and Public Technology weaknesses. Abhirup et. al. [6] offered a dynamic resource alloca- tion technique for security purpose. Huang et. al. [7] showed Infrastructure-as-a-Service for cloud security. Asish Aich et al. [8] described various cloud environment security risk such as Data leakage, DDoS attacks, Misuse of Cloud systems, Uncertain Lines and APIs, Malicious Insiders, Shared Technology and Service Hijacking. They also advised some solution of these issues. Aarti Singh et. al [9] discussed security of cloud computing in various level and they showed Virtual Machine Security, towards Interface Security etc. as various cloud level security.

Cryptography can ensure more security in information technology. A suitable en- cryption and decryption method can ensure data security in cloud computing. Various algorithms exist for cryptography such as DES, AES, RSA etc.

Akshay Arora et. at [10] proposed cloud security ecosystem. They used multi-factor authentication for ensuring data security. They also send One Time Password (OTP) to the users by mail for successfully login. After successfully login, users can send or retrieve data from cloud environment. Once data reaches to cloud end, data undergoin encryption process and store in cloud. They used hybrid cryptography system including RSA and AES and this system seems to be good for data security. However, if any intruder gets credentials of any user, he will able to change or modify data. By taking this drawback, we offered a suitable cloud end auto encryption process that will protect data and ensure that if any intruder gets credential of any users he will not able to chance cloud end data. Author of [11] proposed File Encryption Using Clustering Technique in Cloud Computing for security. Clustering technique proposed in various research in [12]-[17].

We organized our rest description as: Proposed protocol in section II, Simulation and result in section III and Conclusion and future work describe in section IV.

2 Proposed Protocol

For high security, we have described cloud site auto encryption, Clint side entry and description with flowcharts and algorithms.

2.1 Cloud Site Auto Encryption

Securing data saved in a cloud environment is our primary objective. Numerous researchers attempted to protect different user credentials, including secure login, encrypted data or file storage, key management, etc. In any case, if a hacker gains access to the system, he may take files or data from it. There is no way to identify an invader as a thief if he is able to penetrate the cloud environment. He can access all of the system's data using his credentials. We provided a system/environment that prevents anyone from successfully accessing the cloud end to get files or data. He will undoubtedly be caught.

We provided a cloud-end auto-encryption mechanism. The system will repeatedly encrypt files, data, and KEY after a predetermined amount of time. This time frame might be appropriate and could be adjusted at the company's or CSP's request. The more recent file will replace the older one, and the key will be kept in a separate file. But neither management nor users will receive this key. Users will receive the most recent key after logging in using a secure channel, which is detailed in the next section. With the credentials they previously provided, the user will log into the cloud system. The following part will address how to obtain the most recent Key and data/files. Any hacker who obtains a legitimate user credential will be able to log in and access the cloud environment. However, as it is provided to users through a secure channel, the hacker will be unable to obtain the most recent KEY of the saved files or data. Thus, he won't be able to access files or data. The process outlined in Algorithm 1 and Figure 1. Figure 1 illustrates how the system will use the prior Key to decrypt any file, or a portion of a file. Subsequently, a new key will be used to encrypt the file or chunk, and the old one will be substituted. Additionally, a new key will be saved in an additional file that will be needed to decrypt it later. After a predetermined amount of time, this encryption procedure will be repeated repeatedly; alternatively, CSP can conduct it whenever they choose. A proper encryption system can handle both the encryption and the KEY management.

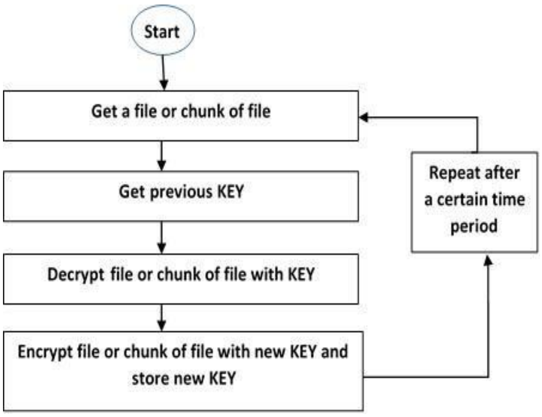
Start
Get a file or chunk of file
Get previous KEY
Decrypt file or chunk of file with KEY
Encrypt file or chunk of file with new KEY and store new KEY
Repeat after a certain time period

Fig. 1. Flowchart of cloud site auto encryption

2.2 Client Side Entry and Decryption

When any client/user will want to access his data/files, he has to login with his creden-tial. If his credential is valid, then he will enter to next section. For second verification he has to supply his other secure credential like one-time password (OTP) etc. After successful derive this level, he will enter into cloud environment. He is now ready to access his data/files. But all his data has been encrypted several time by an automatic encryption process as described in previous section. In this level cloud system will de- liver his new credential (KEY) by a secure channel like email or mobile etc. If this user is not a valid user, then he will not get this new credential (KEY). So any unauthorized users will not able to cross this level. If this user is valid, then he will get his new credential provided by secure channel. After giving this new credential, his data/files will be decrypted according to decryption algorithm and KEY that used to decrypt data/files that will be supplied to the user. This new credential is valid only for this session. As all stored files will encrypt and new KEY will generate after a regular in- terval, so this credential will not work for further. So all data/files will remain save at the cloud environment. This procedure is described in fig. 2 and algorithm 2.

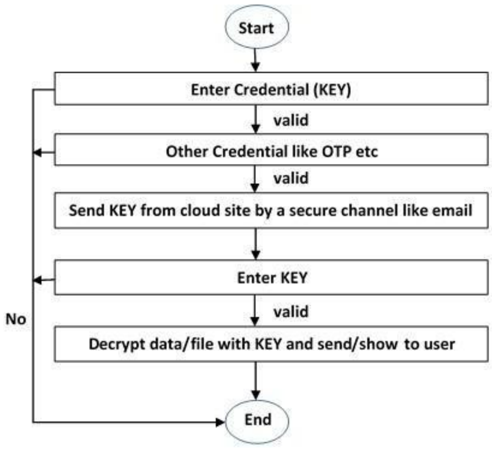
Start
Enter Credential (KEY)
valid
Other Credential like OTP etc
valid
Send KEY from cloud site by a secure channel like email
Enter KEY
valid
No
Decrypt data/file with KEY and send/show to user
End

Fig. 2. Client side entry and decryption process

2.3 Algorithm 1

1. User login will be verified by a suitable system.
2. Assume stored file is encrypted by a suitable algorithm.

3. Stored file will be further encrypted by following method:

A. Monitor which data is frequently using. More security is necessary for thisdata.

B. Get a chunk/file of stored data/files from cloud.

C. Decrypt this chunk with previous KEY and encrypt again with a new KEY.

D. New KEY will be generated by a hash function/any suitable KEY manage-ment system and store this KEY in a separate file in cloud.

E. Repeat B, C and D again and again after a certain time or according toinstruction of CSP.

F. Repeat B, C and D again and again after a certain time or according toinstruction of CSP.

2.4 Algorithm 2

1. At first, User login will be verified by a suitable system.
2. If login credential is verified, send new KEY to user with a trusted medium.This medium may be use of email or mobile or any other trusted system.
3. Decryption process will perform as following:

A. Provide new KEY to get a chunk of encrypted data/files.

B. Compare provided KEY with stored KEY, if authentic then go nextstep, otherwise get lost.

C. Decrypt data chunk by this KEY.

D. Repeat B and C until user logout.

3 Simulation and Result

We have used the CloudSim simulator to simulate our protocol. We have set up an environment for this. For the suggested algorithms, we have developed our own class. There has been an added degree of auto encryption and KEY generation when the protocol is simulated. It takes a little while, but that is tolerable. With the user's credentials, we have generated a hacker role. We noticed that if a hacker has access to the cloud, they can send a revised key to the user's email or mobile device. The hacker is unable to obtain this KEY. Once more, data and files are encrypted automatically after a predetermined amount of time, and the most recent key is saved to a different file, making it impossible for hackers to decrypt this file. Thus, using the suggested protocol, we can offer a high degree of security in cloud computing.

4 Conclusion and future works

In this article, we proposed an auto-encryption method at the cloud end and a user authentication process. This process guarantees an additional layer of encryption on the cloud's end. We have demonstrated that even if a hacker manages to obtain user credentials, he will be unable to access or alter data or files on the cloud. As a result, users and cloud service providers (CSP) gain additional benefits. This process can be put to the test in large data analysis, including data on education, health, and other topics.

5. References

1. Subashini, Subashini, and Veeraruna Kavitha. "A survey on securityissues in service deliv-ery models of cloud computing." Journal ofnetwork and computer applications 34.1 ; 1-11,2011
2. Pawar, Pramod S., et al. "Security-as-a-service in multi-cloud andfederated cloud environ- ments." IFIP International Conference on TrustManagement. Springer International Publish-ing, 2015
3. Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signatureand Advanced Encryp- tion Standard for Enhancing Data Security andAuthentication in Cloud Computing.", 2015.
4. Wang, Cong, et al. "Privacy-preserving public auditing for data storagesecurity in cloud computing." INFOCOM, 2010 Proceedings IEEE. Ieee,2010.
5. Hendre, Amit, and Karuna Pande Joshi. "A semantic approach to cloudsecurity and compli- ance." 2015 IEEE 8th International Conference onCloud Computing. IEEE, 2015.
6. Khanna, Abhirup. "RAS: A novel approach for dynamic resource allocation." Next Gener- ation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.
7. Huang, Wei, et al. "The State of Public Infrastructure-as-a-Service Cloud Security." ACM Computing

Surveys (CSUR) 47.4 (2015): 68..

8. Aich, Asish, Alo Sen, and Satya Ranjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." Computational Intelligencea nd Networks (CINE), 2015 International Conference on. IEEE, 2015
9. Singh, Aarti, and Manisha Malhotra. "Security Concerns at Various Levels of Cloud Com- puting Paradigm: A Review." International Journal of Computer Networks and Applications2.2 (2015): 41-45.
10. A. Akshay et. al, “Cloud Security Ecosystem for Data Security and Privacy”, 2017 7th In- ternational Conference on Cloud Computing, Data Science & Engineering – Confluence, pp. 288-292, 2015.
11. S. Islam, MJ Aktear, MT Islam, MNS Khan “File Encryption Using Clustering Technique in Cloud Computing”, International Journal of Interdisciplinary Innovative Research &Development (IJIIRD), Vol-4, Issue-01,pp. 75-80, 2019.
12. S. Islam, M. N. Islam Khan, M. Zannatun Ferdus, S. J. Islam and M. Abul Kashem, "Improving Throughput using Cooperating TDMA Scheduling of Wireless Sensor Networks," 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, 2020, pp. 1-4, doi: 10.1109/ICCIT-144147971.2020.9213713.
13. S. J. Islam, S. Islam, M. Z. Ferdus, M. N. Islam Khan, M. A. Kashem and M. S. Islam, "Load Compactness and Recognizing Area Aware Cluster Head Selection of Wireless Sensor Networks," 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, 2020, pp. 1-4, doi: 10.1109/ICCIT-144147971.2020.9213750.
14. M. Z. Ferdus, S. Islam and M. A. Kashem, "An Innovative Load Balancing Cluster Composition of Wireless Sensor Networks," 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2019, pp. 1-4, doi: 10.1109/GCAT47503.2019.8978385.
15. M. Z. Ferdus, M. Nurul Islam Khan, S. Islam and M. A. Kashem, "VFLT: SQA Model for Cyber Physical System," 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2019, pp. 1-4, doi: 10.1109/GCAT47503.2019.8978289.
16. MS Bhuiyan et al. “Advancements in Early Detection of Lung Cancer in Public Health: A Comprehensive Study Utilizing Machine Learning Algorithms and Predictive Models” Journal of Computer Science and Technology Studies, Vol. 6, issue 1, pp 113-121, 2024.
17. P. K. Das, M. Abul Kashem, Z. Ferdus and S. Islam, "Development and application of a new computerized smell generating system," 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2019, pp. 1-5, doi: 10.1109/GCAT47503.2019.8978397.