IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 24, No. 6, December, 2019, pp. 611-617
Journal homepage: http://iieta.org/journals/isi

Monitoring Based Security Approach for Cloud Computing

Anuj Yadav*, Ritika, Madan Lal Garg

CSE Department, DIT University, Dehradun 248009, India

Corresponding Author Email: anuj.kumar@dituniversity.edu.in

https://doi.org/10.18280/isi.240608

Received: 20 June 2019
Accepted: 15 September 2019

Keywords:
cloud storage server, data monitor, hybrid encryption Scheme, RSA digital signature, SHA hash

ABSTRACT

Cloud Service owner manages and maintains a variety of services for the end-users and enterprises. To provide security to user data, many security methods can be applied. The purpose of this paper is to design Monitor based scheme that provides the security to user data. The main components associated with the scheme are Client, Monitor and Cloud Service provider. The client performs various operations on the file he wants to store into the cloud. Few of the actions are the division of file into blocks, encoding the file, generation of hashing on the file and application of signature on the data. The monitor does the verification part on behalf of the client, and also responsible for matching the signature on the data files if both the signature matches then declare that integrity of the data is maintained. Cloud server just stores the data sent by the client and provide the data to the client on the request. User can guide the monitor of the monitoring process when to check the integrity of data. So the whole scheme is to develop a monitoring method, which has many security features like privacy maintenance, data integrity maintenance, and data privacy. The approach makes use of cryptography algorithms to achieve the desired results. In this approach, an efficient monitor plays a crucial role in securing the cloud environment.

1. INTRODUCTION

Cloud computing is a computing paradigm that enables computing facilities for its users round the clock. It enables users to access the resources in efficient way at a price much lower than traditional computing resource. Cloud computing authorizes worldwide, convenient, service accessibility to a common group of computing services such as networks, storage, services, applications, and servers. These services are delivered rapidly with minimal user efforts and negligible cloud service provider cooperation. By using cloud services user get benefit in terms of time as well as money, as cloud computing is a cost-effective computing system that enables unlimited possibilities for its users. The basic requirement to enable cloud computing services is the availability of internet connection 24x7 [1].

Nowadays many users opting for cloud-based storage service rather than traditional storage systems. The advantage of using cloud storage is that local storage can be used for other computation tasks and cloud storage is cheaper than local storage systems. With its features and availability, cloud storage is getting popular for individuals as well as organizations [2]. Cloud storage is an essential provision that provides nearly unlimited storage space to the users using the on-demand service model [3]. However, the user of cloud services such as cloud storage systems always worried about the security of their data, like data corruption in cloud can be either maliciously or by accidentally [4].

The main factors that make a contribution towards the cloud security are mainly data protection, confidentiality, integrity, secure communication, and data availability. All these factors must be secure from a user point of view. Considering the rapid growth of attacks on cloud services, user's data may also be modified by the attackers [5, 6]. To secure the cloud data, one must devise a mechanism that not only secures the data but also improve the trust factor between user and cloud service provider [7, 8].

So we propose a new monitoring based scheme in a cloud computing environment that provides security to user data not only when data is stationary but also during the transmission of data. The main objective of this monitoring scheme is to achieve data security and data integrity. The monitoring scheme makes use of cryptographic techniques such as AES, SHA 2, RSA DS to achieve data security and integrity in the cloud environment. The monitoring scheme monitors the user data on the cloud time to time and if detect some attacks report the attack to the end-user. So cloud data is under the scanner all the time using this monitoring scheme. A log report of monitoring scheme is also maintained for user reference. Apart from continuous monitoring, the user can also request on-demand security checks if the user feels that data is not secure [9].

The paper is organized in a different section. In the section 1 introduction is discussed. Section 2 introduced the related work regarding cloud data security. Section 3 introduced Monitoring based scheme. Section 4, focuses on the results and discussion about the monitoring scheme and finally paper concludes in section 5 that has a conclusion and future scope.

2. RELATED WORK

The work done by certain academicians and scientists in cloud computing security is reviewed as:

- Cloud computing comes to the fore as the latest

computing standard those targets for providing efficient, reliable and customized computing facilities for end-users. In Cloud computing all the applications or utilities, dependencies, and databanks are situated on various data centers situated at different geographical locations. So all the stored data and computation results may not be trusted by the cloud users [10].

- Cloud computing security bounds most of the security-related topics that may include the designing of secure architectures for cloud, minimization of active and passive attacks and protection from various types of access control related activities. But there are some aspects of cloud computing security that appear to be specific to that domain
    - The cloud is typically a shared resource, and other sharers (called tenants) maybe attackers.
    - Cloud data is usually accessible by end-users and cloud users may not be aware that they are using insecure protocols and APIs via public networks.
    - Data in the cloud is vulnerable to being lost (e.g., accidentally deleted) or incorrectly modified by the cloud provider.
    - Data in the cloud can be accessed by the cloud provider, its subcontractors and employees.

Solutions to the first three problems are easily available but none of the technique provides solution to the fourth problem. It's an open problem and major challenge to accomplish in cloud computing [11].

- In earlier times, people use their secondary storage devices to store their data, but nowadays cloud computing is being used for the same purpose. Cloud computing is internet-based computing technology that provides services to the users whenever they need. These services are generally accessed using a network connection. “Cloud is used for various business applications, it mainly provides the platform as a service, infrastructure as a service and software as a service “. People are generally enticed towards cloud computing because resources are available on-demand in cloud computing. Cloud-based storage service provides automatic storage, retrieval, and simple reporting. It also improves the overall efficiency with high quality. Trusted third parties are used in a cloud environment where the information is checked on behalf of end-user. But the trusted third parties do not ensure the security factors like integrity, confidentiality, identification [11].
- Nowadays cloud-based service has become affordable, due to which many organizations moved towards cloud-based storage systems. The main advantages of cloud-based computation are scalability, no maintenance overhead, pay as you use to service and no upgrade cost. Unfortunately, these benefits are sometimes overshadowed by security and privacy concerns in cloud computing [12]. In comparison to the organizational data center, cloud-based storage services are managed by third-party, due to which the end-user always hesitate to move their data into the cloud in contrast to privately owned datacentres, where many logical and physical controls ensure the security of the data. So it is required to have some methods or solutions that can protect confidential information from being accessed by untrusted parties.
- Cloud computing is the most influenced computing paradigms in the past few years. It not only reduces the total expenditure but also improves the computational capabilities and efficiencies. Due to these features, it attracts the attention of industry experts as well as academicians. Cloud computing is used in various IT services such as load balancing, utility-based computing, storage solutions, service-oriented computing and so on. Apart from all these benefits, network-related security issues are a major concern for end-users. However, there are some solutions available but they do not provide complete protection to the user data, and all the cloud-based services are exposed to the risk of cyber-attacks [13].
- Cloud computing is an emerging field which becomes a promising factor for users as well as industry. It started with the concept in which, someone else is responsible for setting up the necessary infrastructure and the user needs to pay only for the number of services used. Cloud services are broadly classified as Iaas, Paas, and Saas. Most of the organizations are investing in the cloud to save their expenditure and reduce the burden of maintenance. Nevertheless, besides all the benefits, public cloud computing has many security-related issues, that needs to be addressed to enhance the trust of an end-user towards cloud computing services [14].
- Privacy-preserving auditing method uses the third party for the security checks on user data available in the cloud. The Third-party monitor the data time to time and check for any vulnerability for user’s files [15].
- Here an auditing scheme is discussed, the scheme is used for storage security in the cloud computing using an auditing protocol mechanism. In the scheme, an external auditor monitors the user data for any modification. The focus of the scheme is to provide security to cloud storage systems. The scheme checks the correctness of the data without downloading it [16].
- Researchers develop a scheme using RSA encryption. The scheme is developed that provides security to the stationary data. IF the end-user makes the change into the file then the approach fails to provide the solution and monitoring [17, 18].

3. SYSTEM DESIGN

Due to security issues in cloud computing, there is a need to develop a secure monitoring scheme that provides security to user data, whenever they opt for cloud-based storage and other cloud services. In the proposed scheme we have developed a secure communication method that ensured data integrity for cloud users. The system model used for the proposed monitoring scheme is shown in Figure 1. The monitoring scheme mainly has 3 important entities named as

End-user (EU), Data Monitor (DM) and Cloud storage system (CSS). Each of the entity in the monitoring scheme is assigned different tasks. The primary aim of the EU is to select and upload the required files to the CSS, CSS provides the unlimited storage space for the EU, this space can be used to store a variety of data and the third entity DM plays the most crucial role of providing data integrity to the user data.

In the above-stated monitoring scheme EU store their data into the cloud storage, DM is responsible for time to time monitoring of stored data in the cloud, Even client can request for monitoring at any time. In case of any unwanted activity on user data, DM takes suitable action and report to the EU.

The monitoring scheme undermines such restrictions with greater performance and insufficient storage confirming flexibility compared to attacks and threats based server. The scheme also provisions to enable the high-security scheme in an organized manner for the cloud environment. A detailed view of the proposed scheme is shown in Figure 2, where the role of all three entities EU, DM, and CSS are described.

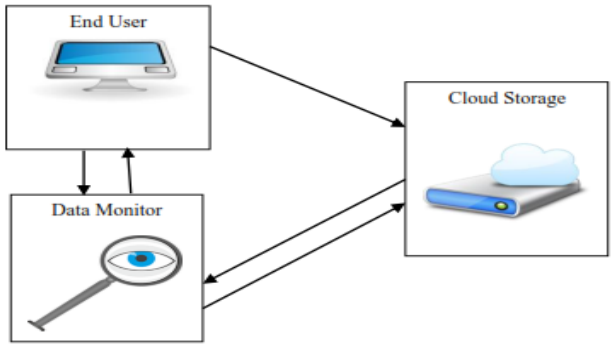


Figure 1. The system model of the monitoring scheme

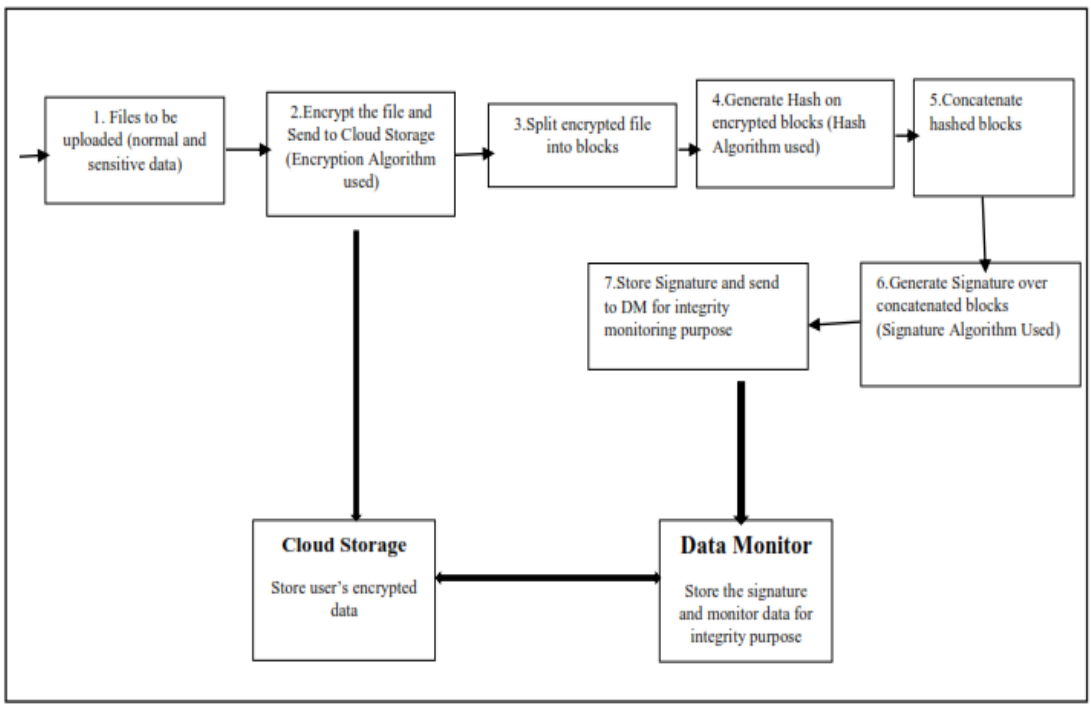


Figure 2. Detailed view of the monitoring scheme

In the scheme our motive is to enhance user trust on cloud computing systems, hence most of the security-related tasks need to be performed by the end-user (All operations performed by EU are numbered from 1 to 7). Data Monitor also plays a vital role in the system's security as it is closely associated with the end-user. In our monitoring scheme, EU firstly performs encryption on the sensitive blocks of user data using any encryption algorithm (we have used AES for the monitoring scheme). These encrypted blocks then transferred to the cloud server for storage purpose. EU then generates hash value on each of the blocks using the hash algorithm (we have used SHA 2 for the monitoring scheme). Further, all these hashes are concatenated. Then a signature is generated on the concatenated hashes using a digital signature algorithm (we have used RSADS algorithm for the monitoring scheme). Now, this signature value is stored for the integrity verification purpose, in our monitoring scheme, we have stored and also send this signature information at DM. Monitoring scheme can work on the request of the EU and it can also be automated in which timing-based continuous monitoring can monitor data for any modification. Whenever the EU demands to monitor data, DM requests the data from the cloud server. After receiving the data, DM generates the hash value on each block using the same algorithm which the EU uses. Later these hashes are concatenated and using RSADS algorithm a signature is generated. This newly generated signature is compared with the earlier signature and if both signature matches, DM inform to EU that the integrity of the data is maintained and data is secure.

The individual roles of DM, EU, and CSS are defined as follows:

3.1 Role of CSS

CSS is responsible for providing unlimited storage capacity to the EU and provides the data to the EU or DM whenever they requested the desired data. In our scheme the

stored data is in encrypted form, so CSS cannot gain access to the actual information stored. The role of CSS can be defined in pictorial form as given in Figure 3.

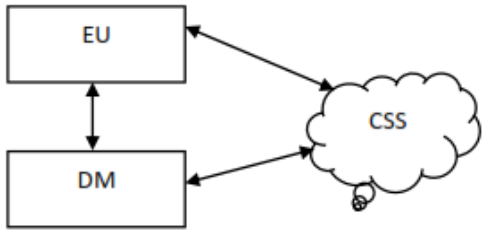


Figure 3. Role of the cloud storage server

Step by step procedure:

Step 1: EU uploads encrypted blocks on the CSS

Step 2: EU can request these encrypted blocks whenever needed

Step 3: DM can also request encrypted blocks through an automated process or on-demand basis whenever requested

In case of any security compromise, DM will inform the EU regarding the security attacks.

3.2 Role of DM

In the monitoring scheme, the most important role is played by the DM. As the EU may be busy with his own work and cannot all the time check for integrity of their data, So EU may request DM for constant monitoring of their data reside in the CSS. DM first stores the signature generated by the EU. Whenever DM receive monitoring request from the EU, DM starts the monitoring process. DM can perform the monitoring either on the request of the EU or periodically. DM requests the desired data from CSS and after receiving the data generate the signature on the received data using the same approaches that the client used. This new signature is compared with the already stored signature if both the signature matches then DM confirms that the data integrity is maintained. Step by step procedure is shown in Figure 4:

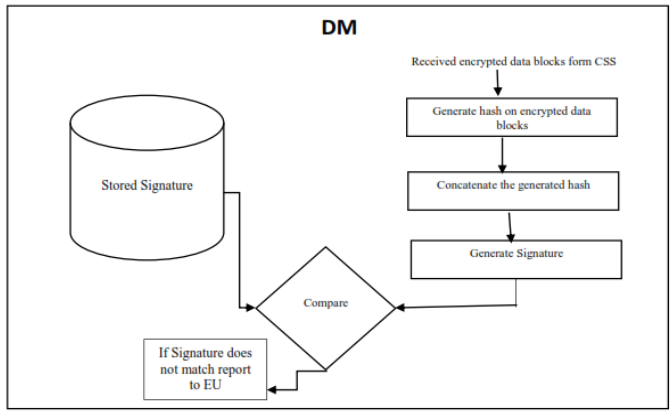


Figure 4. Role of data monitor

Step 1: Receive encrypted blocks from CSS

Step 2: Generate Hash on the blocks

Step 3: Concatenate Hash values

Step 4: Generate Signature using RSADS

Step 5: Compare the generated and stored signature

Step 6: If both signature matches, it means integrity is maintained otherwise report the issue to EU.

3.3 Role of EU

EU is the most important portion of our scheme and is provided with maximum responsibility related to the data. The detailed working of the EU can be shown in Figure 5:

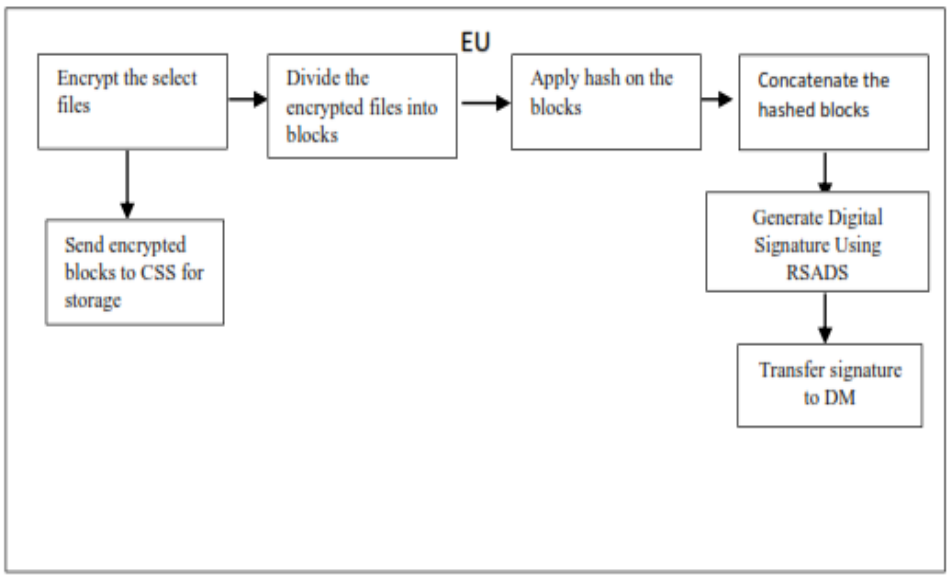


Figure 5. Role of end user

Step 1: Select files to be stored (Apply encryption)

Step 2: Divide the files into the blocks

Step 3: Apply hash on each of the blocks

Step 4: Concatenate all the hashed blocks

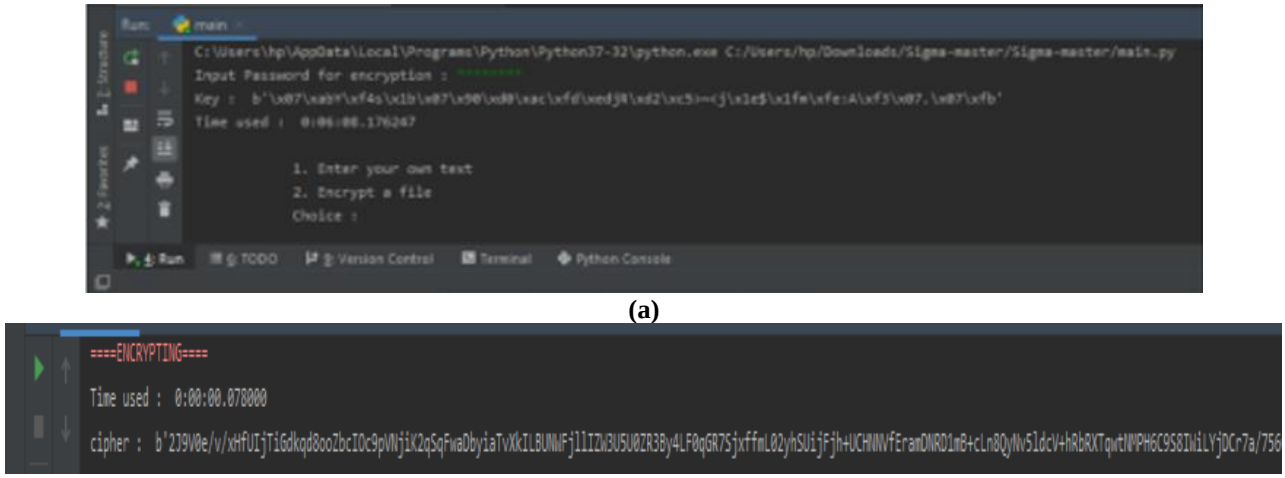
Step 5: Generate signature on the concatenated blocks using RSA digital signature

Step 6: Send signature to the monitor, which can be used for future monitoring purpose

4. RESULTS AND DISCUSSIONS

To check the performance of the above scheme we have used following experimental setup:

Windows 7/Ubuntu as OS, Python 3.7, Pycharm 2019 Community edition. In the setup phase first, the user encrypts the message using AES algorithm and key. Then this encrypted message is sent to the CSS for storage purpose. Message can be a simple text message or EU can select message from specified location as shown in the given Figures 6(a) & 6(b).



(a)

(b)

Figure 6. (a) Enter Simple Text to be encrypted; (b) Select a file from specified location for encryption

The encrypted data is then saved at the CSS. As the data is in encrypted form, no one can access the actual data apart from the authenticated users, so in this way confidentiality property is ensured by the proposed scheme.

Now for the integrity purpose EU first divides the encrypted message into blocks and generates the hash on each block using the hash algorithm. In the next step all these hashes shall be concatenated and on the resultant digital signature is generated using RSA digital signature. The result is shown in the given Figure 7.

Figure 7. Digital Signature value generated using RSADS

The signed value is now sent to the DM for monitoring purpose. DM stores this signed value received from the EU. EU shares the algorithm scheme to the DM. Now EU can ask for on demand monitoring of his data and also automated monitoring scheme can also be used for the purpose. Now DM can monitor the data stored in an automated manner as shown in the given Figure 8.

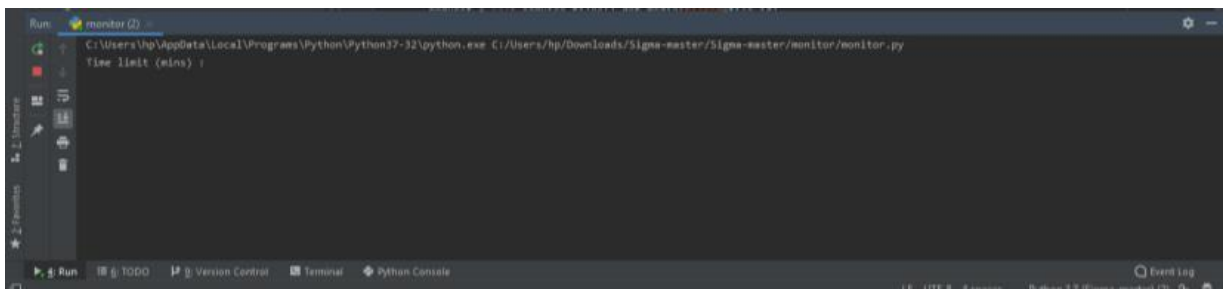
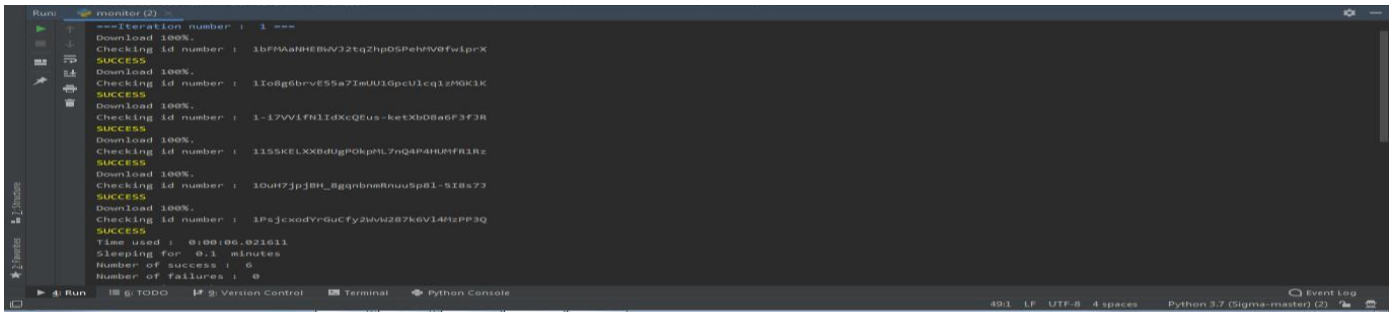
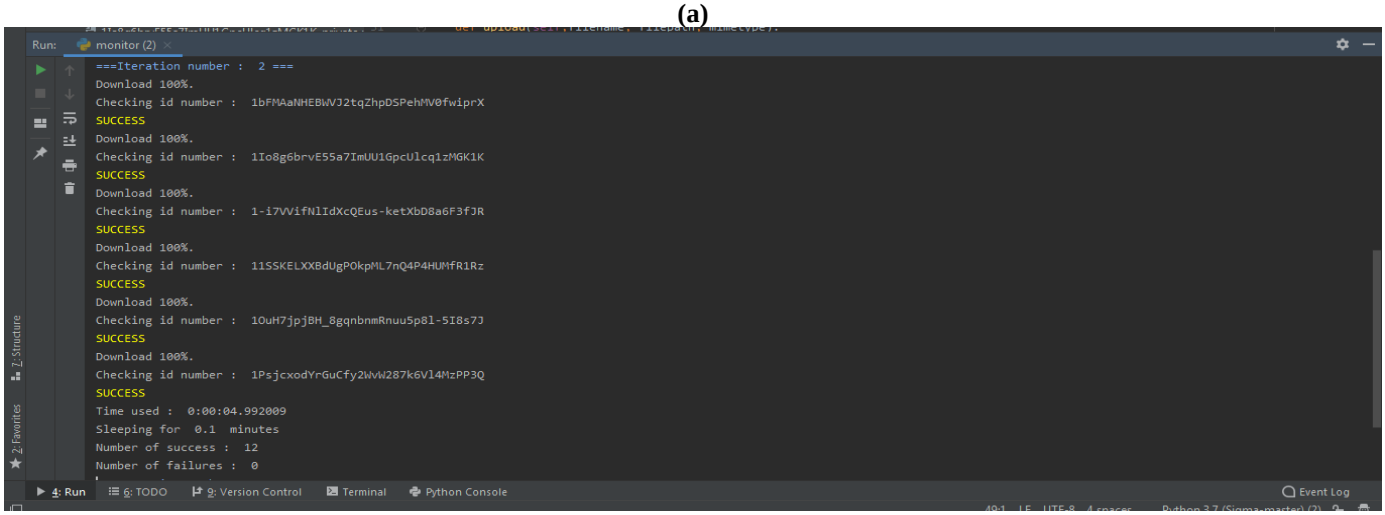


Figure 8. Data monitoring process

While running the monitor program for automated monitoring, DM needs to mention the time in a minute. Suppose DM enters 1 minute, now every 1 minute DM checks the EU data stored in the cloud. For monitoring purpose DM shall generate the signature on the data received from CSS. Signature generation steps are the same that EU uses. Now after receiving the encrypted data from the CSS, DM generates signature over encrypted data. Now the newly generated signature is compared with the already stored signature. If both the signature is the same then DM can declare that integrity is maintained and if signatures do not match, DM will inform EU regarding this. The monitoring process checks regularly in iterative manner, for integrity checking as shown in Figure 9(a) & (b).



(a)



(b)

Figure 9. (a) Integrity checking by monitor on iteration 1; (b) Integrity checking by monitor on iteration 2

So the monitoring scheme is evaluated on the random as well as on the fix block-size data. The main entity that is responsible for security is EU itself and for monitoring, DM is used.

5. CONCLUSION AND FUTURE SCOPE

During the working of the scheme, user can direct DM for periodical monitoring and DM can also request for on-demand monitoring on behalf of EU. By doing this EU always thinks that his data is under his control and in case of any unwanted modifications, he will surely get the report. With all these benefits for user, the trust factors will improve between CS and EU. As a future enhancement some modification for the current scheme can be done. In the current scheme DM reside on the EU premises. For the future enhancement and to reduce the cost of the scheme EU can also work as DM. This may happen because EU has to devote much time while request and getting response from DM. In addition to this EU needs to be aware of how verification process works. Another possible change is to use the scheme only when the user stores any sensitive data at cloud server.

REFERENCES

[1] Mell, P., Grance, T. (2010). The NIST definition of cloud computing. Communications of the ACM, 53(6).

[2] Bhatt, S., Patwa, F., Sandhu, R. (2017). An access control framework for cloud-enabled wearable internet of things. IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), San Jose, CA, pp. 328-338. https://doi.org/10.1109/CIC.2017.00050

[3] Yadav, Anuj, Mehra, Ritika. (2019). Cryptographic solutions for cloud based storage system. International Journal of Advanced Technology and Engineering Exploration.

[4] Cloud computing vulnerability incidents: a statistical overview. Cloud Security Alliance2013, Available: https ://cloudsecurityalliance.org/group/cloud-vulnerabilities/# downloads.

[5] Omari, A., Al-Kasasbeh, B., Al-Qutaish, R., Muhairat, M.I. (2007). A New cryptographic algorithm for the real time applications. Proceedings of the 7th International Conference on Information Security and Privacy (ISP'08), Cairo, Egypt, pp. 33-38.

[6] Singh, K., Rangan Pandu, C, Banerjee, A.K. (2014). Cryptanalysis of unidirectional proxy re-encryption scheme. Information and Communication Technology, 8407: 564-575. https://doi.org/10.1007/978-3-642-55032-4_58

[7] Qi, N., Wei, W., Zhang, J., Wang, W., Zhao, J.W., Li, J.H., Shen, P.Y., Yin, X.Y., Xiao, X.R., Hu, J. (2013). Analysis and research of the RSA algorithm. Information Technology Journal, 12(9): 1818-1824. https://doi.org/10.3923/itj.2013.1818.1824

[8] Sharma, N., Singh M., Misra, A. (2016). Prevention against DDOS attack on cloud systems using triple filter: An algorithmic approach. 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp. 560-565.

[9] Ruth Ramya, K., Sasidhar, T., Naga Malleshwari, D. (2015). A review on security aspects of data storage in

cloud computing. International Journal of Applied Engineering Research, 10(5): 13383-13394.
[10] Wei, L.F., Zhu, H.J., Cao, Z.F., Dong, X.L., Jia, W.W., Athanasios Vasilakos, V. (2014). Security and privacy for storage and computation in cloud computing. Elsevier, Information Sciences, 258: 371-386. https://doi.org/10.1016/j.ins.2013.04.028
[11] Ryan, M.D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. Journal of System and Software, 86(9): 2263-2268. https://doi.org/10.1016/j.jss.2012.12.025
[12] Tsoutsos, N.G., Maniatakos, M. (2015). The HEROIC framework: Encrypted computation without shared keys. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34(6): 875-888. https://doi.org/10.1109/TCAD.2015.2419619
[13] He, J., Dong, M.X., Ota, Kaoru., Fan, M.Y., Wang, G.W. (2014). NetSecCC: A scalable and fault tolerant architecture for cloud computing security. Peer-to-Peer Networking and Applications, 9(1): 67-81. https://doi.org/10.1007/s12083-014-0314-y
[14] Rajkumar, B. (2013). Introduction to the IEEE transactions on cloud computing. IEEE Transactions on Cloud Computing, 1(1): 3-21. https://doi.org/10.1109/TCC.2013.13
[15] Thosar, S.D., Maetre, N.A. (2015). Integrity checking privacy preserving approach to cloud using third party auditor. Proceedings of 2015 International conference on pervasive computing (ICPC), Pune, India. https://doi.org/10.1109/PERVASIVE.2015.7087136
[16] Wang, C., Wang Q., Ren K., Lou, W. (2010). Privacy preserving public auditing for data storage security in cloud computing. 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA. https://doi.org/10.1109/INFCOM.2010.5462173
[17] More S., Chaudhari, S. (2016). Third party public auditing scheme for cloud storage. Procedia Computer Science, 79: 69-76. https://doi.org/10.1016/j.procs.2016.03.010
[18] Cindhamani, J., Punya, N., Ealaruvi, R., Dhinesh Babu, L.D. (2014). An enhanced data security and trust management enabled framework for cloud computing systems. Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, China. https://doi.org/10.1109/ICCCNT.2014.6963097