International Journal of Safety and Security Engineering
Vol. 11, No. 2, April, 2021, pp. 193-199
Journal homepage: http://iieta.org/journals/ijsse

Cryptographic Solution for Security Problem in Cloud Computing Storage During Global Pandemics

Anuj Kumar Yadav*, Ritika, Madan Garg

School of Computing, DIT University, Dehradun 248001, India

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

https://doi.org/10.18280/ijsse.110208

Received: 10 September 2020
Accepted: 26 February 2021

Keywords:
cloud storage, HMS, WFH, pandemic, security monitor

ABSTRACT

Cloud computing has emerged as a potential substitute over traditional computing systems during the time of the COVID-19 pandemic. Almost all organizations shift their working from conventional ways to the online form of working. Most of the organizations are planning to permanently change some % of their work to online WFH (Work from Home) mode. There are numerous benefits of using cloud services in terms of cost, portability, platform independence, accessibility, elasticity, etc. But security is the biggest barrier when one wants to move towards cloud computing services, especially the cloud storage service. To overcome the problem of security in cloud storage systems, we have presented an approach for data security in cloud storage. The proposed approach uses the cryptographic methods and provides security and monitoring features to the user data stored in cloud storage systems. The proposed approach continuously monitors user's data for any kind of modification by attackers. Thus, approach not only provides data security but also improves user's trust on cloud based storage services.

1. INTRODUCTION

As the cases of COVID-19 increases worldwide, almost all the countries opts for lockdown to counter the spreading speed of the pandemic. But as the time grows companies have been instructing their employees to work from home and as of now many companies already instructed their employees to work from home throughout the year [1]. As employees need to access their applications and infrastructure remotely, cloud computing emerges as a potential solution. In the global world, including India, many companies and organizations want their employee's safety. Along with this, companies also want to achieve the business continuity, for that enablement of teams for WFH is a necessity [2].

To achieve the task of WFH, companies are opting for cloud computing-based solutions. In such a situation's companies are relying entirely on cloud service providers for data storage purposes [3]. Globally cloud was already in the growing phase during the current decade and COVID-19 acts as a catalyst for the demand for cloud-based services [4].

In just around three months of lockdown across the world during COVID-19, the world has become added digitally connected, and in consequence, vulnerability also got increased. In the march first quarter, everything was well placed at various organizations in India, and suddenly COVID-19 cases lead to the lockdown in the country. After few days' organizations start out to think about their work and possible way to resume the work. So, most of the organizations found WFH is the only solution in the current scenario. Organizations started connecting to their employees using different tools and applications such as Zoom, Meet, MS Teams, Cisco Webex, etc. But all these are third party applications and mostly use cloud-based storage and other facilities. These applications don't pose any problem while working for a regular organization, but whenever we talk about the defense organizations, healthcare sector, banking sector, education sector, etc. where information leakage can lead to a bigger problem all together [5]. As we know, one of the barriers while using cloud computing is security, so there is a strong need to secure data communication in such situations [6].

According to the report of McAfee on 28 May 2020, there is a sharp increase in the cyber-attacks on cloud accounts, and its percentage is more than 600 percent in the quarter January-April [7]. During the above-said duration, some of the cloud meeting related applications such as Zoom, Meet, MS Teams, Cisco Webex saw an increase in usage of almost 600 percent, and that's only in the education sector. The report also explained that cyber attackers are now targeting these collaboration tools during the COVID-19 pandemic. Risks go many folds when these applications are accessed through unmanaged and compromised devices. Thus, there is a strong need for security methods that provide data security to cloud users. Some of the most common threats that are growing during this period are given in the upcoming section.

2. EFFECT OF COVID-19 ON CLOUD DATA SECURITY

2.1 Distributed denial of service attacks

One of the most common types of attack that occurs in the cyberspace are DDoS related attacks. These attacks are easy to implement, and it can do a lot of harm if the required network system doesn't respond whenever required [8]. As the companies and organizations are relying heavily on cloud-based services, some of the platforms are becoming the soft

targets for cyber attackers [9, 10]. If someone thinks that during this pandemic, the cyber attacker would not perform any activity, then its biggest mistake as DDoS attacks has been committed to the US Health and Human Services Department.

2.2 Phishing attacks

Hackers can use phishing attacks in the most efficient way during the pandemic while exploiting the cloud security vulnerabilities in some of the widely used applications [11, 12]. Nowadays, phishing attackers can send malware attachments with attractive names such as a way to overcome COVID-19, Solution to COVID-19, etc. When a user opens such a file, the cloud network gets disrupted, and malware can spread throughout the systems to gain access to the critical data and applications [13, 14].

2.3 Cloud sprawling

Whenever any organization opts for the cloud-based services, they sometimes neglect the governing policies, sue to which resource usage becomes non-efficient. As we know, cloud resources can be provision and de-provision without any intervention from the provider's side. Due to this, some of the employees' provision or set up many such resources that have minimal usage [15]. Due to this, many resources become underutilized, and sometimes their existence even causes severe security risks if they are not appropriately managed. Some of the security-related problems can also occur due to bad configuration settings by the users. During the COVID-19 time, many companies are opting for cloud computing services for their business continuity, and they are doing this in such a hurry that they are neglecting the risks related to data security [16]. This is because their focus is just to resume their work to a pace in the COVID-19 situation. Even employees don't get proper pieces of training for such services, and they go through the manual to set up their work in the cloud environment. Due to this, security got compromised and this leads towards the cloud sprawling [17].

2.4 Already compromised cloud storage

During the COVID-19 situation during the shifting of work from the traditional way to the cloud way, organizations are looking for a cost-effective cloud security solution. To achieve this, organizations sometimes opt to use services of such organizations whose cloud storage services are compromised in some way [18]. But organizations must think twice while moving any critical data to cloud storage services, as sometimes data storage at compromised cloud storage can put companies' critical data at risk [19].

Apart from these threats, a survey has been conducted by Fugue, regarding the issue of using cloud computing services during the pandemic COVID-19. Many employees from different organizations show their concerns about cloud computing storage services that are being used during this pandemic [20]. As per the survey, 96% of the available cloud engineering teams are now working from home and out of these 84% are concerned about the new weakness in cloud services. That shows how bigger concern cloud security is during the pandemic. The significant risks among these remain the cloud misconfiguration, as said by the CEO of Fugue, Mr. Philip Merrick. To overcome such cloud security problems, a secure mechanism can be employed that can continuously monitor user data stored on the cloud [21, 22]. Using this mechanism, cloud data can be monitored at a particular time or in an automated manner as well. The working of the proposed security mechanism is as follows.

3. SECURITY APPROACH FOR CLOUD STORAGE SYSTEMS

Though we have several security solutions that provide security to cloud storage systems, but due to the COVID-19 pandemic situation is quite different now. The main reason behind this is nowadays not only cloud traditional users, but regular users are also using cloud-based services as most of the organizations asking their more than 50% of workers to work from home. Thus, there is a strong need to secure the important organization data that is to be stored on cloud storage systems. To achieve the desired security features, an approach has been proposed that can provide a solution to security issues raised by the regular users as well as the organizations during this recent pandemic. The approach makes use of cryptography-based methods to overcome the security concerns raised by end-users while storing their data on cloud storage [23]. The proposed approach uses can be visualized by having three entities working simultaneously, and these entities are End User, Cloud Storage, and Security Monitor. The security monitor can be a separate entity, or it can reside at the end user's location. The main aim of the security monitor is to check user data for consistency and unwanted modifications. The working of each entity is explained as:

- End-user selects and uploads their data on cloud storage.
- Cloud storage is used to store the end user's data.

Security monitor checks data for its consistency, integrity, and authenticity.

Out of these available entities, security monitor plays the most crucial role in our system because it periodically monitors the end-user data for any modification by the unauthenticated user, and reports to end user if any such incident happens with their data. The complete working of the proposed approach is shown in the given Figure 1.

The approach not only checks data for its consistency, integrity, and authenticity but also improves the user's trust in cloud storage services. The prime requirement for the success of this approach is that the end user must have an idea of necessary encryption and decryption as some of the essential cryptographic methods will be used at the end user's side itself. If it's not the case, then the security monitor can perform this task on behalf of the end-user. Further, end-user must divide their data into two categories as critical data and non-critical data. The main reason behind the logic is, only critical data will be checked or monitored for inconsistency, as the monitoring scheme will also require its time of computation. There is no use of monitor the data, that is not so important. Also, the operating cost will be added to the overall cost in such condition. Apart from the end user, security monitor plays the dynamic role in the proposed approach, as the security monitor will continuously monitor the end-user data for its correctness.

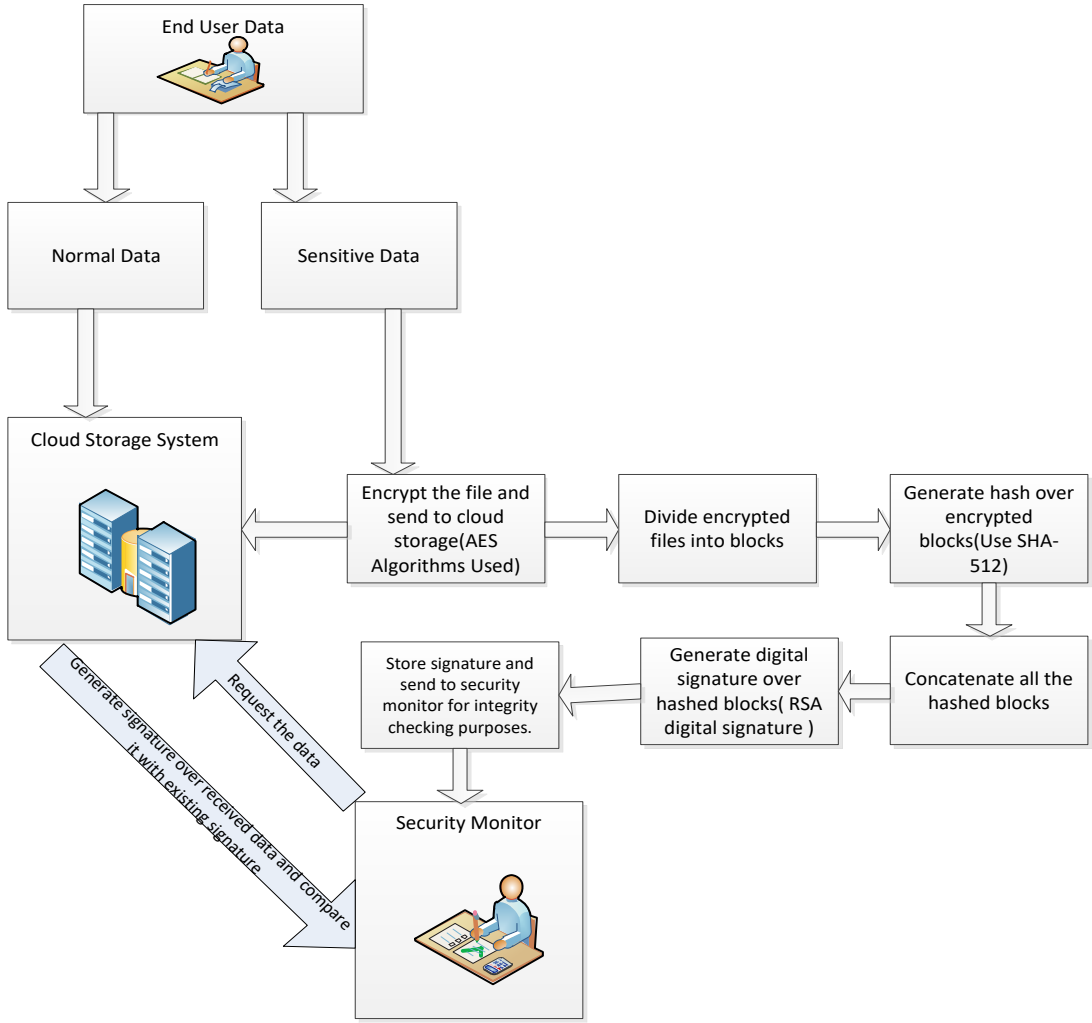

Figure 1. Sec HMS hybrid monitoring scheme

At the starting end-user separates the data as normal data and sensitive data. Normal data is stored at the cloud storage system without any transformation or alteration and, encryption is performed on the critical data using the AES algorithm. After the encryption, the data is sent to the cloud storage server. Subsequently, the encrypted data is divided into equal size blocks, and each of the block act as an input for the SHA-512 hash algorithm to produce the hash value corresponding to each of the block. Further, all the hashed blocks are concatenated with each other. Then RSA digital signature algorithm is applied to the concatenated data, the signature algorithm used in this step ensures data authentication. This generated digital signature is then transferred to the security monitor, which security monitor can use at a later stage for verification. Here we can observe that end-user and security monitors closely work together to achieve the designated task of data security.

Additionally, the security monitor also monitors user data for any changes from time to time. The monitoring can be done as per the request of end-user, or it can be triggered in an automated manner as well. In an automated monitoring method, the security monitor must mention the duration at which monitoring needs to be done for data. For example, if the security monitor mentions the term as 1 min, then every 1-minute end-user data will be monitored for its integrity. Using this scheme, the trust factor improves between cloud services and end-user with the help of a security monitor. Whenever a security monitor receives the data from the cloud storage system, the monitor generates the signature using the RSA digital signature again. The new signature produced is then compared with the previous signature stored. If signatures match, then integrity is preserved for end-user data, and if not, the incidence is reported to the end-user by security monitor.

4. EVALUATION OF PROPOSED SECURITY SCHEME

The security approach is implemented using WIN 7 OS, python 3.7 over Jet brains pycharm community edition 2019 having standard cryptographic libraries. The security approach starts with the separation of normal and sensitive data and further AES encryption on the end-users sensitive data. The security approach can accept simple text input, and input can be a file from a specified location for encryption purposes. Later the encrypted file is sent to the cloud server for storage purpose. As a next step, encrypted data is divided into blocks and hashing to be applied to each of the blocks. At the next stage, hashed blocks got concatenated, and RSA digital signature to be used on the linked blocks. The generated signature value is then sent to the security monitor, that store this signature as a reference for the integrity checking purposes. When a security monitor performs the security-related operations on end-user data, the monitor needs to mention the time interval for integrity checking purposes. The monitor can choose any positive integer value for this purpose. Here we are

using a time interval of 2 minutes for the purpose and run the monitor code for four iterations. Some of the results received from the security monitor in different iterations are as follows:

```
Time limit (mins): .2
===Iteration number: 1 ===
Download 100%.
Checking id number:
1bFMAaNHEBWVJ2tqZhpDSPehMV0fwiprX
SUCCESS
Download 100%.
Checking id number:
1Io8g6brvE55a7ImUU1GpcUlcq1zMGK1K
SUCCESS
Download 100%.
Checking id number: 1-i7VVifNlIdXcQEus-ketXbD8a6F3fJR
SUCCESS
Download 100%.
Checking id number:
11SSKELXXBdUgPOkpML7nQ4P4HUMfR1Rz
SUCCESS
Download 100%.
Checking id number: 1OuH7jpjBH_8gqnbnmRnuu5p8l-
5I8s7J
SUCCESS
Download 100%.
Checking id number:
1PsjcxodYrGuCfy2WvW287k6Vl4MzPP3Q
SUCCESS
Time used: 0:00:09.352015
Sleeping for 0.2 minutes
Number of success: 6
Number of failures: 0

===Iteration number: 2 ===
Download 100%.
Checking id number:
1bFMAaNHEBWVJ2tqZhpDSPehMV0fwiprX
SUCCESS
Download 100%.
Checking id number:
1Io8g6brvE55a7ImUU1GpcUlcq1zMGK1K
SUCCESS
Download 100%.
Checking id number: 1-i7VVifNlIdXcQEus-ketXbD8a6F3fJR
SUCCESS
Download 100%.
Checking id number:
11SSKELXXBdUgPOkpML7nQ4P4HUMfR1Rz
SUCCESS
Download 100%.
Checking id number: 1OuH7jpjBH_8gqnbnmRnuu5p8l-
5I8s7J
SUCCESS
Download 100%.
Checking id number:
1PsjcxodYrGuCfy2WvW287k6Vl4MzPP3Q
SUCCESS
Time used: 0:00:05.890009
Sleeping for 0.2 minutes
Number of success: 12
Number of failures: 0

===Iteration number: 3 ===
Download 100%.
Checking id number:
1bFMAaNHEBWVJ2tqZhpDSPehMV0fwiprX
SUCCESS
Download 100%.
Checking id number:
1Io8g6brvE55a7ImUU1GpcUlcq1zMGK1K
SUCCESS
Download 100%.
Checking id number: 1-i7VVifNlIdXcQEus-ketXbD8a6F3fJR
SUCCESS
Download 100%.
Checking id number:
11SSKELXXBdUgPOkpML7nQ4P4HUMfR1Rz
SUCCESS
Download 100%.
Checking id number: 1OuH7jpjBH_8gqnbnmRnuu5p8l-
5I8s7J
SUCCESS
Download 100%.
Checking id number:
1PsjcxodYrGuCfy2WvW287k6Vl4MzPP3Q
SUCCESS
Time used: 0:00:05.980008
Sleeping for 0.2 minutes
Number of success: 18
Number of failures: 0

===Iteration number: 4 ===
Download 100%.
Checking id number:
1bFMAaNHEBWVJ2tqZhpDSPehMV0fwiprX
SUCCESS
Download 100%.
Checking id number:
1Io8g6brvE55a7ImUU1GpcUlcq1zMGK1K
SUCCESS
Download 100%.
Checking id number: 1-i7VVifNlIdXcQEus-ketXbD8a6F3fJR
SUCCESS
Download 100%.
Checking id number:
11SSKELXXBdUgPOkpML7nQ4P4HUMfR1Rz
SUCCESS
Download 100%.
Checking id number: 1OuH7jpjBH_8gqnbnmRnuu5p8l-
5I8s7J
SUCCESS
Download 100%.
Checking id number:
1PsjcxodYrGuCfy2WvW287k6Vl4MzPP3Q
SUCCESS
Time used: 0:00:05.754119
Sleeping for 0.2 minutes
Number of success: 24
Number of failures: 0

Process finished with exit code -1
```

5. RESULTS AND DISCUSSION

Security approach has been evaluated on the basis of files of different size. We have taken file sizes starting from 100

KB up to 100 MB. Later, the security approach is compared with the already existed traditional approach, and finally, performance is evaluated based on data upload and download time.

5.1 Data upload time

Data upload time is the time that is required to encrypt the desired file as per the user's need. It is the sum of time needed by the user to upload the file to the cloud server (T_u), the time required to encrypt the user's file (T_e), and the request made by the end user's to store their file at the cloud server (T_r). So data upload time (T_{Up}) can be written as:

$$T_{up} = T_r + T_e + T_u$$

5.2 Data download time

Data download time is the time that is required to decrypt the desired file as per the user's need. It is the sum of time needed by the user to download the file from the cloud server (T_{re}), the time needed to encrypt the user's file (T_d), and the request made by the end user's to store their file at the cloud server (T_r). So data upload time (T_{dt}) can be written as:

$$T_{dt} = T_r + T_d + T_{re}$$

6. SCHEME EVALUATION

Proposed scheme provides additional security features along with integrity. To enable these extra security features, we have used SHA-512 and digital signature algorithm. The scheme can be used by the variety of users having minimal knowledge of the encryption and decryption process and the scheme can be termed as a hybrid security monitoring scheme that monitors the end-user data residing on cloud storage systems. The robust monitoring system takes a little bit of time when we compare it with traditional encryption and decryption systems as to provide the additional layer of security, the monitor needs to generate the has value on data, and further digital signature is applied over this data. Digital signatures are required for integrity verification purposes. Further scheme can be evaluated according to:

- Using SHA-512 & existing private key.
- Using SHA-512 & RSA key generation method.

These methods are compared according to the time needed to perform the desired operations on data. The time comparison is shown in the given Figure 2 and Table 1.

Table 1. Comparison of time taken using RSA key generation & using existing key

Size of file for input (in MB)	Time taken Using SHA-512 & existing private key	Time taken using SHA-512 & RSA key generation algorithm
.1	.065	.317
1	.113	0.405
20	.585	0.845
40	1.545	1.890
60	3.017	3.255
80	4.012	4.225
100	4.848	5.205

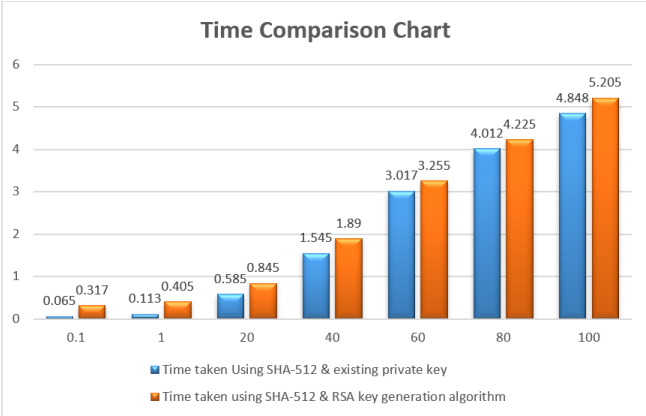

Figure 2. Comparison of time taken using RSA key generation & using existing key

These two schemes are compared according to the figure and table shown above. The results of the comparison show that if we use the current private key, it takes less time compared to the key generation scheme for RSA. This is obvious because it takes time for key generation to be a key generation process. This also takes longer for the asymmetric key algorithms than for symmetric key algorithms.

Data Verification Using the RSA Signing Scheme: When the data is stored on the cloud server, it can be retrieved at the request of the end-user. Data need to be checked for its correctness and protection after retrieval. Time taken by the verification method is given in Table 2 and Figure 3 for the different size files.

Table 2. Time taken by RSA signing scheme for data verification

File size in MB	Time taken by RSA signing scheme for data verification
.1	.085
1	0.125
20	0.603
40	1.565
60	3.025
80	3.995
100	4.953

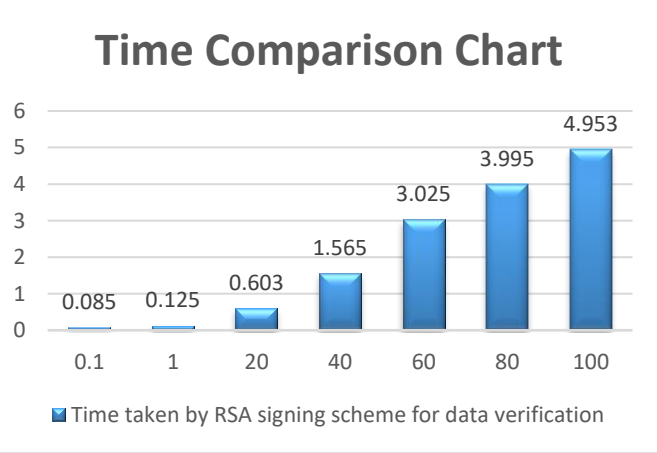

Figure 3. Time taken by RSA signing scheme for data verification

We can realize that the time taken to verify data seems to be very similar to the time taken by the data signing scheme (Using Existing Key). For the different size files, the time requirement is almost the same, and this can be shown in the given Table 3 and Figure 4.

Table 3. Time comparison of data signing and data verification scheme using RSA signing scheme and existing key

File size in MB	Time taken using SHA-512 & existing private key	Time taken by SHA-512 & RSA signing scheme for data verification
.1	.065	.085
1	.2013	0.125
20	.585	0.603
40	1.545	1.565
60	3.017	3.025
80	4.012	3.995
100	4.848	4.953

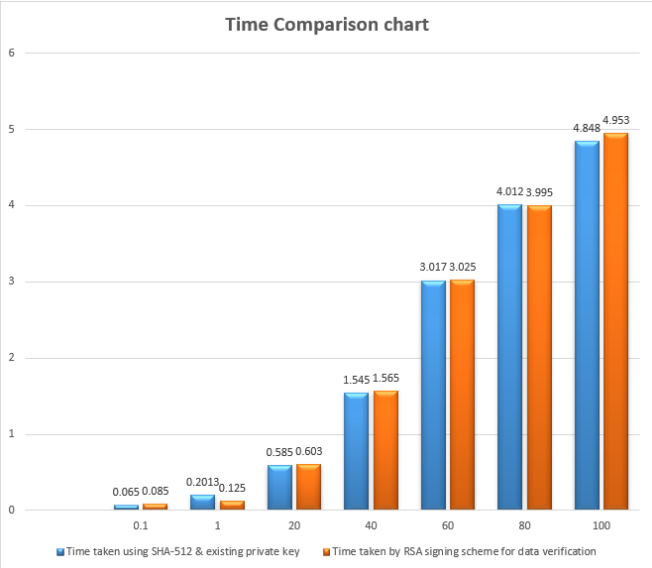

Figure 4. Time comparison of data signing and data verification scheme using RSA signing scheme and existing key

In accordance with the given Table 4 and Figure 5, we can compare the total time taken during the encryption, data signing, and storage process vs. time taken while decrypting, checking, and retrieving the original file. The distinction is for files with variable size starting from 100 KB up to 100 MB.

Table 4. Total time taken during the encryption, data signing, and storing process versus time taken while decrypting, verifying, and retrieving the original file

File size in MB	Time taken for encryption, data signing and storing process	Time taken for decrypting, verifying, and retrieving process
.1	.740	.140
1	.790	.162
20	.915	.220
40	1.962	1.025
60	4.525	3.050
80	8.890	6.535
100	10.015	8.025

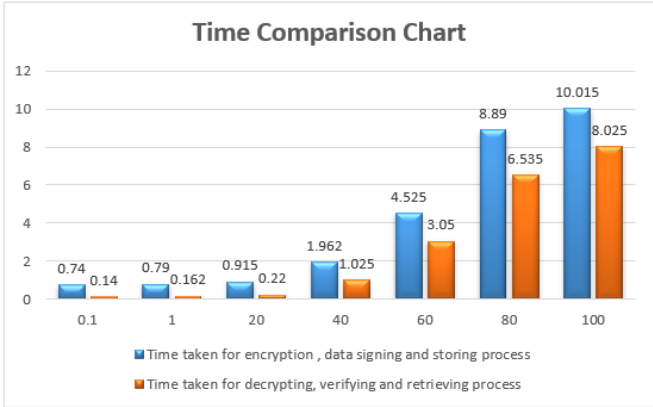

Figure 5. Total time taken during the encryption, data signing, and storing process versus time taken while decrypting, verifying, and retrieving the original file

Comparing data storage and data recovery process, we can state that the data recovery process takes less time compared to the data storage process. Our monitoring scheme uses cryptographic methods to provide cloud storage systems with a solution to the security-related problems.

7. CONCLUSIONS AND FUTURE SCOPE

In general, almost all the security-related processing is done on the server-side using cryptographic approaches (encryption and decryption) when one wishes to store data on cloud storage systems. These schemes do not provide assurance related to the data integrity and also the element of confidence on the part of the client. In our security monitoring system, the relationship between the security manager and end-user conducts all the security-related transformations at the client level. Because of this, the monitoring scheme offers better control of access, integrity, and improvement of trust for the client. Even if anyone gains access to the data stored in the cloud storage, the original data cannot be accessed as the data is encrypted. Even if somebody gains access to the data stored in the cloud storage, the original data cannot be obtained as data is stored in encrypted format using the cryptographic algorithms. Besides this, the intruder would not be able to make any modifications to the data of the customer, which contributes to the assurance of integrity. In short, we can say that our proposed scheme includes all basic and advanced security features. Apart from all the security features listed, the proposed approach has a monitoring feature, which is monitored by the security manager. The primary aim of monitoring is to increase the trust of end-users in cloud storage systems. The security monitor can monitor the user data stored in cloud storage according to the end user's demand and in an automated way. The paper showed a complete monitoring process and sample results, along with the time taken in respective approach activities. In having multiple security features along with continuous monitoring of user data, we can say that the proposed monitoring solution not only offers data protection but would also improve user trust in cloud storage systems. That is because the security monitor will keep a close eye on the user data for some form of alteration, and the incident will be notified to the end user if change occurs. A few more algorithms can also be explored as a future enhancement to reduce the complexity of time, and end-users can also suggest necessary changes as and when required.

ACKNOWLEDGMENT

I would like to thank my supervisor's Dr. Ritika and Dr. M.L. Garg, for helping me to carry out the research work. Further, I would like to extend my gratitude to Dr. Debopam Acharya, Dean CSE, for encouraging all the time for research. A special thanks to our Hon'ble Vice-Chancellor Dr. K K Raina for all the support and encouragement during the research work.

REFERENCES

[1] https://www.analyticsinsight.net/heres-how-covid-19-could-threaten-your-companys-cloud-data/. Published on 15 May 2020, accessed on 13 June 2020.

[2] Gupta, M., Abdelsalam, M., Mittal, S. (2020). Enabling and enforcing social distancing measures using smart city and its infrastructures: A COVID-19 use case. arXiv preprint arXiv: 2004.09246.

[3] Wang, R. (2017). Research on data security technology based on cloud storage. Procedia Engineering, 174: 1340-1355. https://doi.org/10.1016/j.proeng.2017.01.286

[4] https://cio.economictimes.indiatimes.com/news/cloud-computing/is-covid-19-the-long-awaited-catalyst-for-cloud-adoption/75284786. Published on 22 April 2020, accessed on 16 June 2020.

[5] Odun-Ayo, I., Ajayi, O., Akanle, B., Ahuja, R. (2017). An overview of data storage in cloud computing. 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), pp. 29-34. https://doi.org/10.1109/ICNGCIS.2017.9

[6] Zhe, D., Wang, Q., Su, N., Zhang, Y. (2017). Study on data security policy based on cloud storage. 2017 IEEE 3rd International Conference on Big Data Security on Cloud (bigdatasecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 145-149. https://doi.org/10.1109/BigDataSecurity.2017.12

[7] https://www.cnbctv18.com/technology/mcafee-report-shows-rise-in-cyber-attacks-as-cloud-services-use-goes-up-during-covid-19-6013631.htm. Published on 28 May 2020, accessed on 18 June 2020.

[8] Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S., Narayan, D.G. (2020). Distributed Denial of Service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Computer Science, 167: 2297-2307. https://doi.org/10.1016/j.procs.2020.03.282

[9] Bhushan, K., Gupta, B.B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. Journal of Ambient Intelligence and Humanized Computing, 10(5): 1985-1997. https://doi.org/10.1007/s12652-018-0800-9

[10] Tomar, R., Khanna, A., Bansal, A., Fore, V. (2018). An architectural view towards autonomic cloud computing. In: Satapathy S., Bhateja V., Raju K., Janakiramaiah B. (eds) Data Engineering and Intelligent Computing. Advances in Intelligent Systems and Computing, vol. 542. Springer, Singapore. https://doi.org/10.1007/978-981-10-3223-3_55

[11] Munivel, E., Kannammal, A. (2019). New authentication scheme to secure against the phishing attack in the mobile cloud computing. Security and Communication Networks, 2019: 1-11. https://doi.org/10.1155/2019/5141395

[12] Rawat, P.S., Dimri, P., Gupta, P. (2020). Learning-based task scheduling using big bang big crunch for cloud computing environment. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 13(2): 137-146. https://doi.org/10.2174/2213275912666190204125712

[13] Verma, R., Ruj, S. (2014). Security services using crowdsourcing. Procedia Computer Science, 32: 505-512. https://doi.org/10.1016/j.procs.2014.05.454

[14] https://www.analyticsinsight.net/heres-how-covid-19-could-threaten-your-companys-cloud-data/. Published on 15 May 2020, accessed on 19 June 2020.

[15] Luo, S., Lin, Z., Chen, X., Yang, Z., Chen, J. (2011). Virtualization security for cloud computing service. In 2011 International Conference on Cloud and Service Computing, pp. 174-179. https://doi.org/10.1109/CSC.2011.6138516

[16] Kourtesis, D., Alvarez-Rodríguez, J.M., Paraskakis, I. (2014). Semantic-based QoS management in cloud systems: Current status and future challenges. Future Generation Computer Systems, 32: 307-323. https://doi.org/10.1016/j.future.2013.10.015

[17] Gupta, M., Mittal, S., Abdelsalam, M. (2020). AI assisted malware analysis: A course for next generation cybersecurity workforce. arXiv preprint arXiv:2009.11101.

[18] Haider, Y., Selvan, S. (2016). Confidentiality Issues in Cloud Computing and countermeasures: A Survey. http://eprints.manipal.edu/id/eprint/146699

[19] Rajeswari, S., Kalaiselvi, R. (2017). Survey of data and storage security in cloud computing. In 2017 IEEE International Conference on Circuits and Systems (ICCS) pp. 76-81. https://doi.org/10.1109/ICCS1.2017.8325966

[20] https://www.continuitycentral.com/index.php/news/technology/5055-survey-finds-widespread-concern-over-cloud-security-risks-during-the-covid-19-pandemic, Published on 15 April 2020, accessed on 21 June 2020.

[21] Indu, I., Anand, P.R., Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4): 574-588. https://doi.org/10.1016/j.jestch.2018.05.010

[22] Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1): 5. https://doi.org/10.1186/1869-0238-4-5

[23] Yadav, A., Ritika, Garg, M.L. (2019). Monitoring based security approach for cloud computing. Ingénierie des Systèmes d'Information, 24(6): 611-617. https://doi.org/10.18280/isi.240608