EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

SecHMS- A Secure Hybrid Monitoring Scheme for Cloud Data Monitoring

Anuj Kumar Yadav[1,*], Ritika[1] and M.L. Garg[1]

[1]CSE, DIT UNIVERSITY, Dehradun, India

Abstract

Cloud computing enables the data owners to store and host their data on the cloud storage servers, which is to accessed by data consumers from the cloud storage servers whenever needed. The approach provides not only better accessibility but also unlimited storage capacity to the users. Even though there are numerous benefits of the approach, but security remains the prime concern for cloud computing and cloud service users. There are few solutions that provide protection in cloud computing, but even after having these solution, trust in cloud service providers remains the prime concern for cloud users. To overcome such a situation and to enhance the faith amongst the user and cloud service provider, a hybrid monitoring scheme (SecHMS) have been proposed and evaluated in this paper. The hybrid monitoring scheme (SecHMS) uses public-key cryptography and hashing technique to provide data security in cloud computing. The hybrid scheme (SecHMS) constantly monitors the stored data on behalf of end-users. As user's data is getting continuously monitored, it leads to the enhancement of trust for the end-user in cloud computing systems. A thorough analysis has been done on different size files, and results have been demonstrated to show the correctness of SecHMS scheme.

Keywords: Cloud Storage System, DDoS, IDS, SecHMS, Monitor.

Received on 07 July 2020, accepted on 30 September 2020, published on 23 October 2020

doi: 10.4108/eai.23-10-2020.166719

1. Introduction

With its numerous advantages, cloud computing emerges as the driving force in the networking field. Cloud computing is being used in almost all fields nowadays, such as business, education, medical science, retail sector, etc. As its applicability areas are unlimited, cloud computing is changing or driving the lives of peoples in an efficient manner with many advantages [1] [2]. The foremost advantage of using cloud computing is that it offers many services using its service models, and these services are provided according to the demands of users. Cloud service models are represented in a generalized way as *-as-a-Service (*aaS), where * is used to represent the type of assistance provided by cloud computing. Usually, the assistance is provided either as software or as a platform or as infrastructure [3] [4]. The core technology or driving force behind cloud computing is virtualization, and the prime reason behind the use of virtualization is its elasticity capability and efficient resource utilization [5]. In a broader view, cloud computing is a model that enables users to use cloud computing services and resources using the internet connection and underlying interface. By this way end users can use cloud service and transfer their related data on the cloud,later the data is accessible 24x7 for users using the variety of available devices such as mobile, laptop, PDA, etc. [6].

Though cloud computing poses many advantages and associated benefits of cloud computing, there are some concerns as well [7]. All these concerns need to be addressed to declare that cloud computing is the best possible solution for end-users for a variety of services. Out of all the concerns

[*] Corresponding author. Email: anujbit@gmail.com

security is the prime concern not only from the cloud service provider but also from the end-user point of view. Cloud computing security issues can be divided into three categories named user information security, computer system security, and network security. This categorical division of cloud computing security is shown in Figure 1.

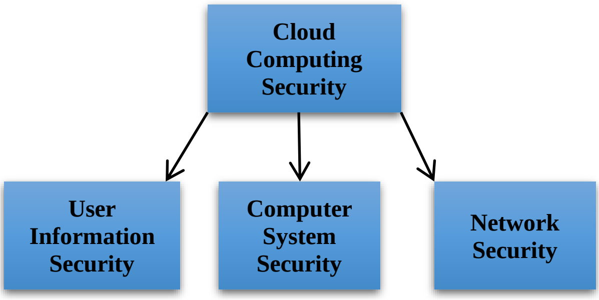


Figure 1. Categorical division of cloud computing security

In the current paper, out of the mentioned categories, our prime focus is on user information security. From a user's point of view, security is the topmost concern when they switches towards any cloud service, especially the cloud storage service. As user's data all the time resides at cloud provider's end, and there is logically no user control over the stored data. Thus, there is a strong need to develop a secure mechanism that boosts user's trust in a variety of cloud services [8]. Before developing the solution to the said problem, a thorough research review has been carried out, to understand the cloud security-related problems. After the review, a hybrid monitoring scheme (SecHMS) have been developed to encounter the said problems.

The remaining paper is organized in the following sections, as section 2 gives insight into the literature survey done in cloud computing security. Section 3 introduces the SecHMS hybrid monitoring scheme. Section 4, the results have been discussed, and finally, the paper ends with the conclusion and future scope.

2. Literature review

Some of the security solutions provided by the researchers in the field of cloud computing security have been reviewed as follows:

- Network security is one of the significant concerns when one talks about cybersecurity as security attacks increase manifolds during the time. With time their effectiveness and severity are also growing. In cloud computing, the necessity of using a service is the network availability; thus efforts must be applied to secure the cloud computing data in a network. In the current work, detailed review have been carried out for such issues and their effect on the users. For solutions, different artificial intelligence and machine learning techniques are explored to thoroughly analyze the network traffic and detect the malicious activities on the network [9].
- In the current work, a detailed overview is presented regarding the prediction and forecasting based security methods in cybersecurity, more specifically the cloud computing security. During the outline, the main emphasis is on task identification, projection of attacks, and intention of attack, and finally, prediction of the reason for the attack from an attacker's point of view. Taking all these things into consideration, enterprises can employ methods and services to counter any such situation if it occurs for the organization [10].
- The researchers perform extensive study regarding the basic operation performed on a network and how information security methods can be used to provide security solutions to these network operations. Further, an "Intrusion Detection System (IDS)" is developed that is used to detect and declare a security attack on the network. The system is compared for two categories of users; one is those who do not use security systems and one those who use security systems in the network. As a result, the conclusion drawn is that individuals having awareness about the security attacks perform correct action against malicious activities [11].
- The credibility of cloud service is one of the significant needs while evaluation of any cloud service. The work done by the researchers proposed a model that is going to evaluate the credibility of cloud computing services based on some factors. The major factors that constitute the credibility are quality of cloud service, trust factor, time of service use. The developed model is tested on a Netlogo platform, and the results generated take care of individuals' preferences by combining multiple available pieces of evidence. The model improves the quality of service and gives a slight security feature for cloud users [12].
- A monitoring keyboard or intelligent keyboard can work as a key logger tool. It may be used to generate an alarm-based system whenever the finger is pressed on the key of the keyboard, and it also records the content that is being typed by the user. This type of system is useful when someone thinks about creating the smart security system for alerting, for alarming, for recording or for identification. The

method can be used to identify and differentiate the individual characteristics based on biometrical features [13]. As further enhancement, researchers developed a keyboard that can record the user characteristics based on pressure parameter with a combination of time for individuals, while the press any key on the keyboard [14].

- As a security solution to cloud computing, researchers developed a “Probabilistic numerical method” which is a framework that is used to monitor the combination of cryptographic algorithms. The main aim of the approach is to find out the errors in the computations. Identification of the errors is one of the prime factors while designing a secure system for cloud computing. If error identification is correct, correct countermeasures can be applied to overcome these errors. The work is done to a proposed method that uses “Microsoft's STRIDE-DREAD model” to list the existing attacks and threats in cloud computing. Apart from attack identification, the list also gives insights about the significance and measurement of each of the threats.
- Further, these threats are ranked according to their severity. After identifying threats and their sternness, cloud users are informed regarding these threats and their effects on the cloud services used by the end-users. The work done is like a guideline for cloud users as well as for security personals to develop security systems for private or hybrid clouds [15].
- Security attacks related issues can be viewed as the most significant barrier for users as well as organizations when they tend to switch towards cloud computing-based services from the traditional application-based services. There are many approaches that are being developed and used by the developers to overcome such situations arising due to security attacks. In the proposed work, the main emphasis is on making use of honeypots-based security mechanism to address security issues of cloud computing. The researchers developed a scheme named “CloudHoneyCY”. “CloudHoneyCY” is an open-source method in which a variety of honeynets, which includes high-interaction and low-interaction honeypots, are positioned at the server end (Cloud Server). The aim of the method is to analyze and prepare the attack report [16].
- “Distributed denial of service (DDoS)” has emerged as a prime challenge for various server applications, whether it is an application server or database server. Thus, there is a need to counter DDoS attacks and provide solutions to the problems arising due to DDoS attacks. The most significant issues that are occurring due to DDoS attacks are massive traffic on the server and the improper use of network bandwidth. To overcome the DDoS attacks, researchers proposed an “ant-based DDoS detection technique.” The technique makes use of virtual honeypots and a multilayer secure framework to gather the information of attackers at different points of the network; for this purpose IP log table works as a helping hand. The ant colony scheme detects the intrusion attacks based on the pheromone population on the area of interest. Once the attacked region is found out, the output is sent to the proposed framework to minimize the effect of the attack. The prominent feature of the approach is that it provides complete protection to counter the DDoS attacks and reduce the network traffic overhead [17].
- Researchers developed a scheme using RSA encryption. The scheme is developed that provides security to the static data. IF the end-user makes the change into the file, the approach fails to provide the solution and monitoring [18].

3. Hybrid monitoring scheme (SecHMS)

After extensive research review, it has been observed that though there are schemes that are currently being used by the researchers for cloud computing security, but there is no such available that improves the end user’s trust in cloud-based services [19][20]. To overcome the problem, a hybrid monitoring scheme is named SecHMS. This hybrid scheme uses cryptographic techniques to ensure data security on behalf of the user and continuously monitors the user data for any kind of change. SecHMS consists of three important entities named Cloud User, Monitor, and Cloud Storage System. All these are assigned different tasks. The Cloud user is responsible for selecting and uploading the data on the cloud storage system, Monitor is responsible for monitoring the user data for its consistency and integrity checking, and the cloud storage system is responsible for storing the user data at their premises. The monitor is the most important part of SecHMS from the security point of view and to improve the trust of cloud user on cloud-based storage systems, as it continuously has a close eye on user’s data. The working of the SecHMS is shown in Figure 2.

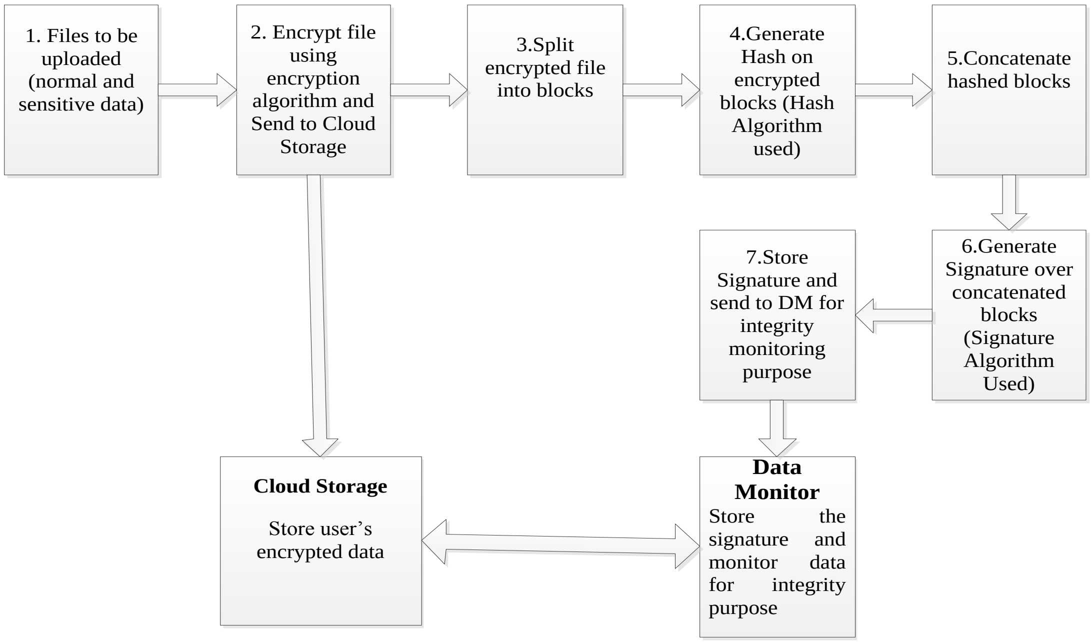

1. Files to be uploaded (normal and sensitive data)
2. Encrypt file using encryption algorithm and Send to Cloud Storage
3.Split encrypted file into blocks
4.Generate Hash on encrypted blocks (Hash Algorithm used)
5.Concatenate hashed blocks
6.Generate Signature over concatenated blocks (Signature Algorithm Used)
7.Store Signature and send to DM for integrity monitoring purpose
Cloud Storage
Store user's encrypted data
Data Monitor
Store the signature and monitor data for integrity purpose

Figure 2. The working of SecHMS

The primary goal of the scheme is to enhance the user's trust in cloud computing services. To achieve this, almost all the security-related transformation has been performed at the cloud user's end itself. In addition to the cloud user, another entity that plays a vital role in the success of the proposed scheme is monitor. In the SecHMS scheme, firstly, at the cloud user end, data is separated into two types named as normal data and sensitive or critical data. The main emphasis of the scheme is to secure the sensitive information because if we apply the SecHMS scheme on whole data then the operating cost will go at the higher side. After the separation of critical data and normal data, encryption has been performed on the critical data using the AES algorithm. This encrypted data is sent to the server for storage purposes.

As a next step, encrypted data is further divided into the blocks of equal size. In the next stage of the SecHMS scheme, further SHA-512 algorithm is applied on each block, as a result, hash value of each block is computed. Furthermore, these hashed blocks are concatenated with each other. After the concatenation, the RSA digital signature algorithm is applied on the concatenated data. The application of the RSA digital scheme ensures authentication. Later, the generated signature is transferred to the monitor for verification purposes. So, in general, roles of cloud user, monitor, and cloud storage systems have been differentiated. Cloud users and monitor are closely associated with each other, and monitor continuously monitors user's data whenever required. In addition to this monitor can also perform the data monitoring in an automated manner, where the monitor mentions the time duration. If the monitor mentions the time duration as 1 sec, it means every 1-sec monitor user's data. In this way, when user's data is being monitored continuously, the user's trust enhances on cloud-based services. After receiving the requested data from the cloud storage server, a signature is generated over it and compared with the stored signature for data integrity.

4. SecHMS scheme performance evaluation:

The performance of the SecHMS scheme have been implemented on Windows 7 operating system, Pycharm community edition 2019, and python 3.7 with standard cryptographic libraries. SecHMS scheme started with AES encryption on user's data. The data can be a simple text message, or it can be a text file selected from a given location. This data is transferred to cloud storage system. Later the encrypted data is divided into blocks, after that SHA-512 is applied to each block. Finally, these hashed blocks are concatenated, and a signature is generated over the concatenated blocks. This signature is sent to the monitor. Later, when monitor receives the data from the cloud storage server, the signature is generated using the same process, and later, the generated signature is compared with the stored signature for integrity preservance. The process working is shown in appendix A.

While running the monitoring process at the start monitor needs to mention the time interval by which monitoring works, i.e. if monitor mentions the time as 1 minute it means that after the first iteration of monitoring process there is a halt of 1 minute before the next iteration starts for monitoring. Users can select any value for this. After running the monitoring process sample results appears as:

```
===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 :  0:00:09.391216
Sleeping for  1.0  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 :  0:00:06.536411
Sleeping for  1.0  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 :  0:00:05.272809
Sleeping for  1.0  minutes
Number of success :  18
Number of failures :  0
```

As shown in the results as mentioned above, the monitoring process is shown for three iterations. In the iteration one, we can check that the monitoring process takes 07.176012 minutes for execution after that process sleeps for 1 minute, iteration 2 takes 06.536411 minutes for execution after that process sleeps for 1 minute, and iteration 3 takes 05.272809 minutes for execution after that process sleeps for 1 minute. The process continues until the monitor halts it. The status SUCCESS is treated as that the user data is intact and it is in its original form i. e. no modification have been done to user's data. The process is evaluated for ten iterations, and the time taken from iteration 1 to 10 is given in Table 1.

Table 1. Time taken during each iteration of monitoring process styles

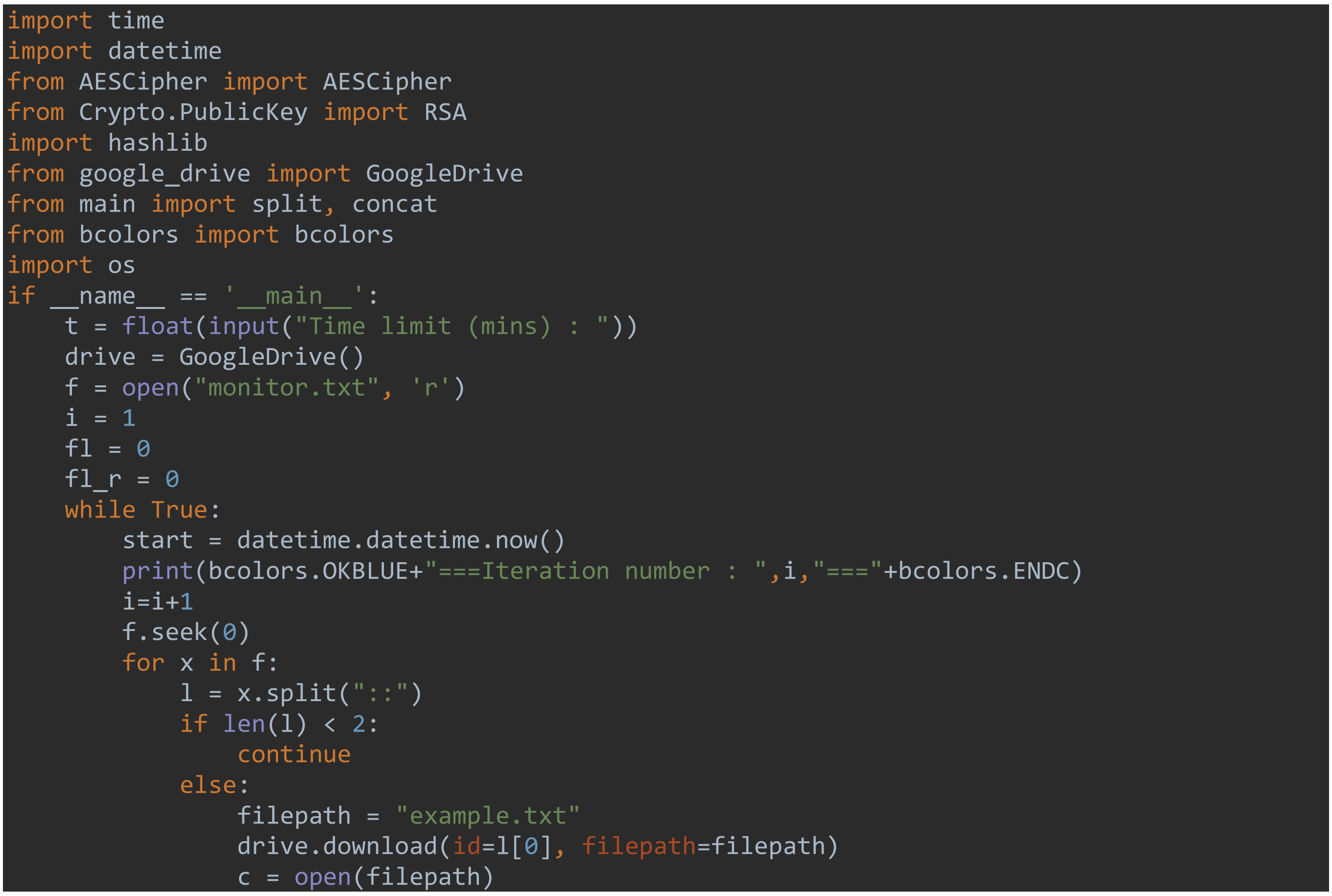
Iteration No.	Time Taken in Minutes
1	0.09.391216
2	0.06.536411
3	0.05.272809
4	0.08.018415
5	0.05.647210
6	0.05.491210
7	0.05.600410
8	0.06.692412
9	0.05.257210
10	0.05.912411

5. Conclusion and future scope

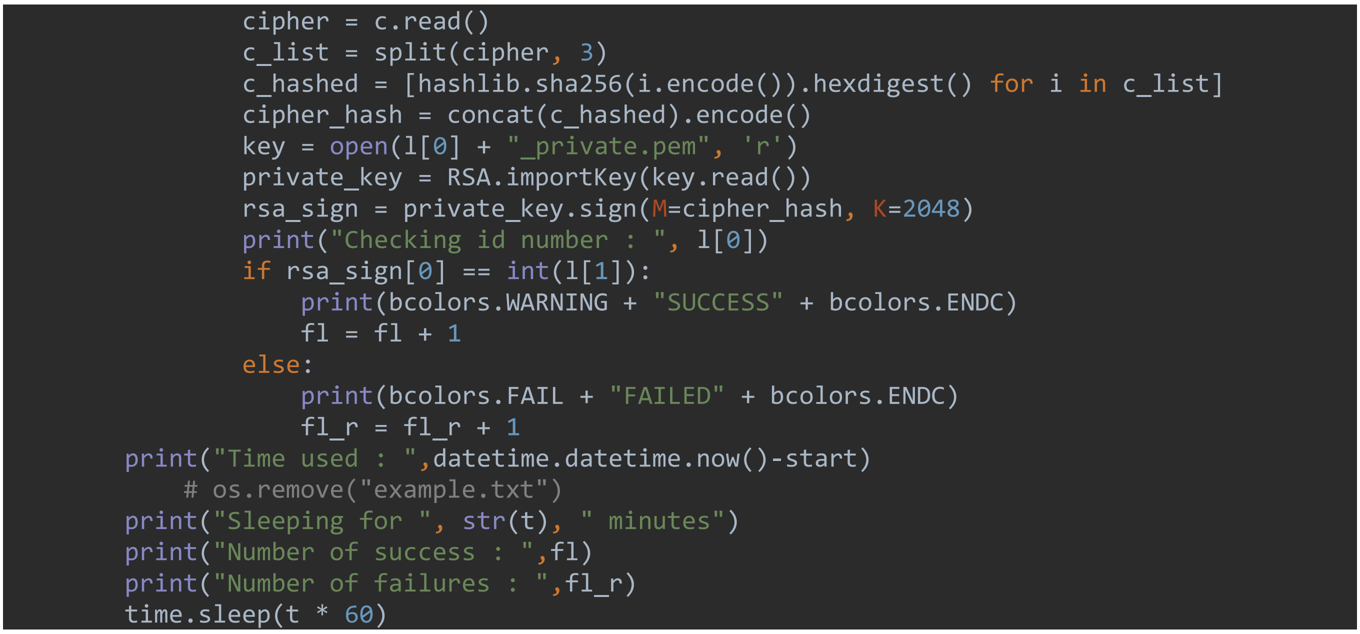
In SecHMS scheme, all the security-related operations are performed at the client-side or at the monitor side, therefore it provides better access control to user data, data integrity and, most importantly, trusts to the end-user. As we know, on the public cloud platform data is available free to all the users and hence anyone using the cloud computing service can download it whenever needed. But with the application of a hybrid cryptographic monitoring scheme (SecHMS), even if the attacker gets a copy of data, he cannot get the actual data as it is encrypted using the algorithms. Another activity that all the attackers like to perform on user data is data modification, but as our scheme provides data integrity, the attacker shall fail to achieve their motive. We can say an attacker will never be able to modify the stored data without having the private key, as whenever one wants to update the data, there is a need for a private key. If verification fails, then data shall not be updated. In addition to all these security features, our scheme also have a monitoring process, which not only monitors the user data on demand, but it can monitor data as an automated process. The idea of an automated process have been explained and demonstrated earlier. Thus, after having so many security features and continuous monitoring of the data, we can declare that our monitoring scheme helps end-users to improve their trust in the cloud storage systems. The prime objective that comes out after the literature review was to build trust between the cloud service provider and the end-user so that end-users get motivated to use cost-effective cloud services. In SecHMS scheme, monitor always have a close eye on the user data, this becomes a deciding factor for the end-user to opt for the cloud-based services. As future work, the work can be further extended to minimize the computation time while storing and retrieving the data from the cloud storage systems for computation or other purposes. Apart from this, different combinations of security algorithms can also be explored to provide additional security. Along with this approach can be tested for available cloud community platforms.

.

Appendix A.



```
import time
import datetime
from AESCipher import AESCipher
from Crypto.PublicKey import RSA
import hashlib
from google_drive import GoogleDrive
from main import split, concat
from bcolors import bcolors
import os
if __name__ == '__main__':
    t = float(input("Time limit (mins) : "))
    drive = GoogleDrive()
    f = open("monitor.txt", 'r')
    i = 1
    fl = 0
    fl_r = 0
    while True:
        start = datetime.datetime.now()
        print(bcolors.OKBLUE+"===Iteration number : ",i,"==="+bcolors.ENDC)
        i=i+1
        f.seek(0)
        for x in f:
            l = x.split("::")
            if len(l) < 2:
                continue
            else:
                filepath = "example.txt"
                drive.download(id=l[0], filepath=filepath)
                c = open(filepath)
```



```
            cipher = c.read()
            c_list = split(cipher, 3)
            c_hashed = [hashlib.sha256(i.encode()).hexdigest() for i in c_list]
            cipher_hash = concat(c_hashed).encode()
            key = open(l[0] + "_private.pem", 'r')
            private_key = RSA.importKey(key.read())
            rsa_sign = private_key.sign(M=cipher_hash, K=2048)
            print("Checking id number : ", l[0])
            if rsa_sign[0] == int(l[1]):
                print(bcolors.WARNING + "SUCCESS" + bcolors.ENDC)
                fl = fl + 1
            else:
                print(bcolors.FAIL + "FAILED" + bcolors.ENDC)
                fl_r = fl_r + 1
    print("Time used : ",datetime.datetime.now()-start)
        # os.remove("example.txt")
    print("Sleeping for ", str(t), " minutes")
    print("Number of success : ",fl)
    print("Number of failures : ",fl_r)
    time.sleep(t * 60)
```

References

[1] Gai K, Qiu M, Zhao M, Tao L, Zong Z. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. Journal of Network and Computer Applications. 2015; Vol 59: pp 46–54.

[2] Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. A view of cloud computing. Communications of the ACM. 2010; Vol 53(4):pp 50–58.

[3] Chenthara S, Ahmed K, Wang H., Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access,2019; 7, 74361-74382.

[4] Sun X. Critical Security Issues in Cloud Computing: A Survey. In proceedings of 2018 IEEE 4th 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) OmahaNE 2018; pp. 216-221.

[5] Yadav A, Garg M, Ritika. Docker containers versus virtual machine-based virtualization. In Emerging Technologies in Data Mining and Information Security, 2019; pp. 141-150. Springer, Singapore.

[6] McDole A, Abdelsalam M, Gupta M, Mittal S. 2020. Analyzing CNN Based Behavioural Malware Detection Techniques on Cloud IaaS. arXiv preprint arXiv:2002.06383.

[7] Buyya R .Introduction to the IEEE Transactions on Cloud Computing. Ieee transactions on cloud computing, 2013; vol. 1(1): pp 3-21.

[8] Gupta D, Bhatt S, Gupta M, Kayode O, Tosun A S. 2020, May. Access control model for google cloud iot. In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 198-208. IEEE.

[9] Yavanoglu, Aydos M. A review on cyber security datasets for machine learning algorithms. In proceedings of 2017 IEEE International Conference on Big Data (Big Data), Boston, MA. 2017; pp. 2186-2193.

[10] Husák, Komárková J, Bou-Harb E, Celeda P. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. IEEE Communications Surveys & Tutorials. 2016.

[11] Ben-Asher N, Gonzalez C. Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 2015; Vol, ISSN 0747-5632.

[12] Li Z, Liao L, Leung H, Li B, Li C. Evaluating the credibility of cloud services. Computers & Electrical Engineering.2017;Vol 58.

[13] Chen J, Zhu G, Yang J, Jing Q, Bai P, Yang W, Qi X, Su Y, Wang Z L. Personalized Keystroke Dynamics for Self-Powered Human–Machine Interfacing. ACS Nano. 2016; Vol 20159 (1),pp. 105-116.

[14] Sulavko A, Eremenko V, Fedotov A A. Users' identification through keystroke dynamics based on vibration parameters and keyboard pressure. Dynamics of Systems, Mechanisms and Machines (Dynamics). 2017; pp. 1-7.

[15] Anand P, Ryoo J, Kim H, Kim E. Threat Assessment in the Cloud Environment: A Quantitative Approach for Security Pattern Selection. In Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication (IMCOM '16). ACM, New York, NY, USA,2016.

[16] Gjermundrød H, Dionysiou I. CloudHoneyCY-An Integrated Honeypot Framework for Cloud Infrastructures. . In Proceedings of 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC). 2015.pp. 630-635.

[17] Selvaraj R, Kuthadi V M, Marwala T. Ant-based distributed denial of service detection technique using roaming virtual honeypots. IET Communications.2016;Vol. 10(8): pp.929-935.

[18] Cindhamani J, Punya N, Ealaruvi R, Babu D. An enhanced data security and trust management enabled framework for cloud computing systems. In Proceedings of Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, China.

[19] Yadav A, Garg M, Ritika. Monitoring based security approach for cloud computing. Ingénierie des Systèmes d'Information. 2019;Vol. 24(6): pp. 611-617.

[20] Vimalachandran P, Wang H, Zhang Y, Zhuo G. (2017). The Australian PCEHR system: ensuring privacy and security through An improved access control mechanism. arXiv preprint arXiv:1710.07778.