Security audit in cloud-based server by using encrypted data AES -256 and SHA-256

M Husni*, H T Ciptaningtyas, W Suadi, R M Ijtihadie, R Anggoro, M F Salam and S Arifiani
Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

* mhusni43@gmail.com

Abstract. Cloud service provides access to servers, databases, storage, and any application services over the Internet. Cloud computing allows users to store their data in the servers. This will ease user to access the data everywhere by only using the internet connection from any devices. Cloud service allows users to run application to many mobile users or to support business critical operations. Cloud service also provides rapid access to the flexible and low-cost IT resources. By using the cloud service technology, there is no need to invest a hardware and spent much time to manage that hardware. Although cloud technology has many advantages, there are also some disadvantages such as some security issues. The usage of internet connection gives a high risk in cyber-attacks. Sometimes the cloud service provider also misuses the data stored in the server. This paper proposes the integrity verification of data stored in the server by using Hash function SHA-256 and AES-256. The proposed scheme combines the mechanism of encryption as a strategy to verify the data integrity. This method will encrypt files stored in the servers that aims to ensure the integrity of file stored. This research is expected to help use to secure their data.

1. Introduction
Today, the cloud computing technology becomes familiar. Cloud computing use the internet technology to provide data storage and computing power, without direct active management by the user. The term is generally used to describe the data centers that can be access by many users over the internet. There are many large clouds that often have functions to distribute over many locations from central servers. The cloud computing not only provides the data storage in server, it also provides service that can help to run application to many mobile users or to support business critical operations. This cloud computing provides rapid access to the flexible and low-cost IT resources.

The rapid growth of digital technology also increases the threat. The interconnectivity from any devices by using the internet such as this cloud computing technology, can also increase the threat. There are many kinds of threat i.e. malware, spoofing/phishing, network incident, etc. Based on Enterprise Cloud Computing Survey in 2018, it is found that there are 73% organization have computing infrastructure stored in cloud. In the digital technology era, how data is stored, managed, and manipulated become important. The availability, integrity, confidentiality and non-repudiation of data become challenge in this digital technology era.

In January 2018, RightScale conducted survey known as State of the Cloud Survey on the latest trend in cloud computing. There are total 997 technical professionals across a broad cross-section of
organizations about their adoption of cloud infrastructure. It is found that the security issue become the top concern in 2018. There are 77% respondents agree about this security issue. The cloud computing technology does not provide the exact location where the data is stored or being processed. This can be a risk that can arise during the implementation and management process. There are many reports about data breaches, broken authentication, interface and API hacked, account hijacking, etc. All of these reports can decrease the trust of the third party. Sometimes the third party needs to ensure the privacy and security of the data stored. Besides, the third party needs to verify the SaaS provider to secure user identity management, authentication, and access control mechanism. The database privacy and security also need to be ensured.

To solve the problem in integrity verification of data stored in the server, this research proposes to implement Hash function SHA-256 and AES 256. This proposed scheme combines the mechanism of encryption as strategy to verify the data integrity. The file stored in the server will be encrypted to ensure the integrity of it.

Than Myo Zaw et al. implement AES (Advance Encryption Standard), Elliptic Curve Encryption and Signature to secure database [1]. The result of this research shows that the proposed method is difficult to be attacked because this proposed method generates many keys. Each element in this proposed method is represent as a key. If the attacker can get a key, this means that only one element that is lose. The disadvantage of this propose method is, it generates a thousand or millions of keys that cause difficulty to manage. Iqra Hussain et al. proposes an encryption/decryption scheme for IoT communication using Binary-bit Sequence and Multistage Encryption [2]. The proposed algorithm can be classified as symmetric algorithm. This proposed algorithm will encrypt the original data at multiple stages and a key will be generated for encryption process to convert the plain text to chipper text. That key will also be used for decryption process. Vasyl Lytvyn et al. proposes a system to encrypt information based on the synthesis of Neural Network (NN) and AES algorithm [3]. This system is based on the diagonalized matrix of weight coefficients in synaptic connection of neural network. The proposed method needs to change the key constantly to minimize the threat. But this proposes method will result a high computation and stability, if it is compared with the other existing encryption algorithms.

2. Method

File verification is a process to verify the integrity of files in computer. The file verification process will compare each part of the copied file with the original file. The popular approach in file verification is to compare the generated hash file with the original hash file. The file verification by using hash function is to ensure the file whether it is not broken or modified. The method in has function is to compare the hash number calculated with the original hash number. If it results the same number, it will be concluded that the file is not modified.

In the process of transferring or saving a file, the hash function can be used to ensure the file from modification. Sometimes, there is a malware or any malicious code or virus that is used to modify the content of the file. The hash function can be used to solve this problem. This has function is used in many applications to encrypt the file and ensure it from modification.

This research uses Laravel framework to implement the hash function. Laravel is a PHP framework developed by Taylor Otwell. The project to develop this framework was started in April 2011. The reason why Laravel is developed is because there is no framework that can be used up to date with the version of PHP programming language [4]. Laravel has a different method with the other framework. Laravel use routing class to provide interaction in the system. To generate the view, Laravel only uses the view class. Both routing and view class in Laravel have relation to the controller class. And controller class is the only class that has relation to the model class. The model class is the only class that can access the database. The architecture of Laravel framework can be describe in figure bellow.
The system is developed in Laravel and use MySQL as Database. More information about MySQL can be accessed here [5]. To implement script in verifying the data integrity and return the back up of data to the system, this research uses Python. Python is one of programming language. This programming language is claimed as a programming language that easy to learn and focus on the program that can be read clearly [6]. The Advance Encryption Standard (AES) is a cryptography algorithm that can be used to secure data. AES algorithm is a symmetric block cipher that can encrypt and decrypt information. AES is chosen because this algorithm is strong for differential attack, truncated differential attack, linear attack, interpolation attack, and square attack [7].

There are front-end and back-end system. The front-end of system is implemented by using Laravel framework, and the back-end system is implemented by using Python programming language. There are three servers of system developed i.e. database server, application server, and backup server. These servers are used to simulate the transfer and verification process. The front-end system consists of application server and verifier file system. The application provides functionality to upload, download, and verify the file. The verifier file application is used to verify the file stored in database server. The process to ensure the file integrity, designed in this research is describes in the figure bellow.

The user will upload the file from the front-end system, and the system will automatically generate the key for encryption process. System will encrypt the file and generate secret hash key. The encrypted file, file data, and secret hash key is stored in database server. The file data consists of file name and data type. System will also record the log activity in the database server. The encrypted file is not only sent to database server, but also to backup server. To download the file stored in database server the process is described as bellow.
Figure 3. The download process designed to ensure the file integrity.

Before the downloaded file is sent to the user, system will verify the file first. System will compare the secret hash key in the file with the secret hash key stored in the database server. If the there is no difference between those secret hash keys compared, the file will be decrypted and sent to the user. Every activity in the server will be recorded in the log.

3. Results and discussion
To test the reliability of the software, this research conducts functionality test. The functionality test is designed to check the system from any error, bug, or fault. There are four scenarios in this functionality test i.e. upload file, download file, file verifier, and run script to return file to the backup server. Each test has their own step to be verified. The result shows that there was not found error, bug, or any fault in the system. The functionality test consists of four tests i.e. upload file, download file, file verifier, and run script to return file from backup server.

To test the performance of the system developed, this research designs some scenarios. There are four different file type that will be uploaded and downloaded to check the performance of encryption and decryption algorithm i.e. docx, mp4, wav, and jpeg. There are total three users that will test the system. Each user will try to upload and download the file in the different size and type of file. In the download process, the file will be decrypted and sent to the user. In the upload process, the file will be encrypted and stored in database server. The result of the first scenario is shown below.

Figure 4. The performance of cryptography for document file (DOCX).

The first scenario is to check the performance in DOCX file. From figure 4, it is known that the document size will affect to the encryption and decryption process. The second scenario is to check the performance in MP4 file, and the next scenario is to check the performance in wav and jpeg file. The
result shows that there is no big different among performance of cryptography for file type DOCX, MP4, WAV, and JPEG. The result for MP4, WAV, and JPEG file are shown in Figure 6, Figure 7, and Figure 8. The other aspect that affect to the download and upload performance is the bandwidth speed. If the bandwidth is faster, it will upload or download file faster and result lower performance. But if the bandwidth is slower, the upload or download file will be slower and result higher performance. It can be concluded that the performance of encryption and decryption process depends on the file size and bandwidth speed. The file size affects to the computational process. While the bandwidth affects to the speed of transfer data.

![Figure 5. The performance of cryptography for video file (MP4).](image1)

![Figure 6. The performance of cryptography for audio file (WAV).](image2)

![Figure 7. The performance of cryptography for image file (JPEG).](image3)

4. Conclusion
From the reliability test conducted, it can be concluded as follows.

- This research tries to implement AES algorithm for encryption process. To simulate the encryption and decryption process, this research develops a web-based system using Laravel framework.
- This system will verify the file integrity to ensuring the file stored is not modified.
- The system has functionality to return a modified or deleted file into the original one.
- From the functionality test, there is not found error, bug, or fault in the system developed.
The performance of encryption and decryption process depends on the file size and bandwidth speed. The file size affects the computation. While the bandwidth affects to the speed of transfer data.

For further research, another algorithm can be used as comparison. So, it can be found the best algorithm in the file verification. Today, many algorithms are improved. The other algorithms are recommended to be used as comparison.

References

[1] Zaw T M, Thant M and Bezzateev S V 2019 Database Security with AES Encryption, Elliptic Curve Encryption and Signature in *Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*

[2] Hussain I, Negi M C and Pandey N 2018 Proposing an Encryption/Decryption Scheme for IoT Communications using Binary-bit Sequence and Multistage Encryption in *International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*

[3] Lytvyn V, Peleshchak I, Peleshchak R and Vysotska V 2019 Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm in *International Conference on Advanced Information and Communications Technologies (AICT)*

[4] Otwell T 2019 *Laravel, Laravel LLC, 2011-2020* [Online] retrieved from https://laravel.com/

[5] Affiliates O C A I 2019 *Oracle* [Online] retrieved from https://www.mysql.com/

[6] Foundation P S 2019 *Python, Python, 2001-2020* [Online] retrieved from https://www.python.org/

[7] Rouse M 2019 *Search Security: Advanced Encryption Standard (AES), Tech Target, 2000-2020* [Online] retrieved from https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard