Framework of Solving a Problem for Cloud Security Issues

Abstract

Along with the development of cloud computing industry, the security is drastically arising as a main concern. This belongs with the awareness of losing the stored data for all cloud users, including individuals and enterprises. This paper mainly focuses on the security concerns of cloud computing, and to address the possible current solutions to its issues. In addition, it will outline about the security issues related to storage, within the evidence of the solutions to avoid the threats through encryption. This is then followed with the summary of the result, and a conclusion.

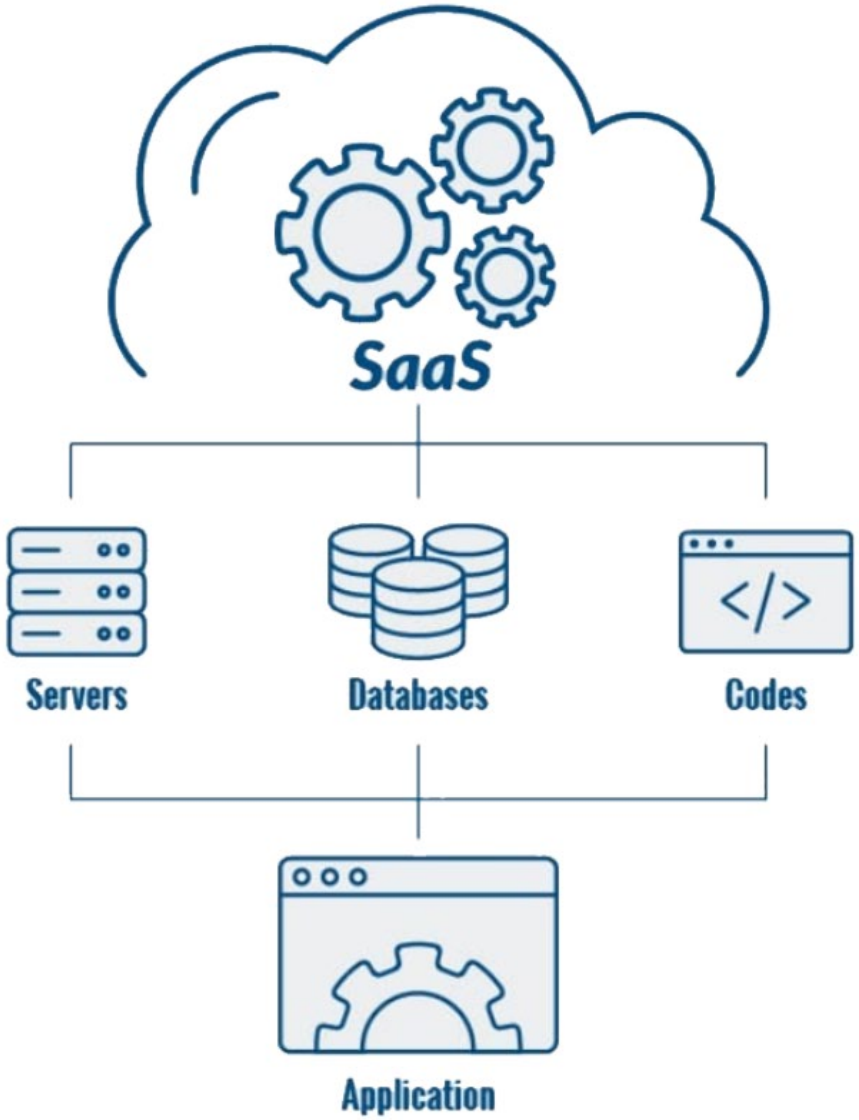
Section 1
Introduction

Cloud Computing is the next technology system to store the data for any services, which was previously done with the on-premises servers [1]. Cloud computing eliminated most of the disadvantages from on-premises servers, whilst implementing the new features such as resources pooling [2]. However, security problem came across as a main issue for cloud implementation, which mainly is the privacy issue. Since cloud computing is not yet fully developed, it is still uncertain to deal against hijacking, hacking and DoS (Denial of Service Attacks) [3]. Due to this uncertainty surrounding the security of information, I have investigated that encryption algorithms can become a solution to resolve these concerns.

Currently, the trend of using the cloud service is mostly focused on SaaS (Software as a Service) industry, such as AWS (Amazon Web Services), and Google Cloud [4]. SaaS is a software-based cloud service which software hosts a combination of servers, database, and code to create applications that can be accessed by users from their own devices. It allows any user from anywhere to access into their server, without any limitations. SaaS runs the logic in the cloud, meanwhile the other cloud service runs on the users' device.

Due to the condensation of information into one database, the weakness of cloud computing is highly emphasised where the loss of control in one database can cause the hack of the entire users' privacy. This paper provides the general information of the cloud storage, and analyses on the techniques that can be used to prevent the hacking on the cloud service.

Diagram below shows the brief explanation of SaaS.



Source: (atlantic.net)

This paper is organised with 2 sections of methods explanation, and a current solution to the problem, then followed by a summary of the method that is been analysed. Section 2 will be a brief explanation of cloud storage with the diagrams, and Section 3 will be the proposed solutions and experiments using encryption algorithms.

Methods

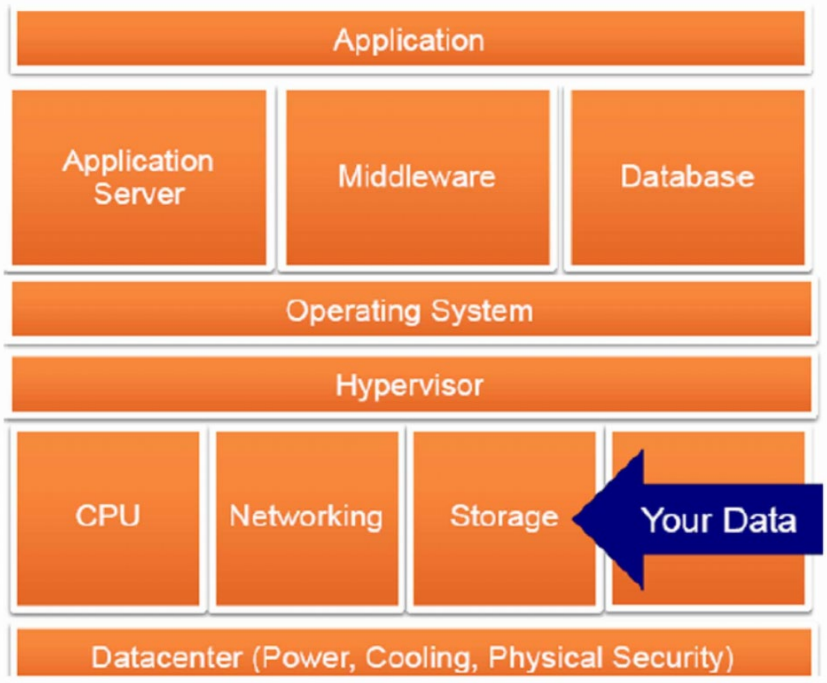
Section 2

Main key to resolve the security issue for the cloud service is to protect the cloud storage. Cloud security can be lost in many forms, where it does not always have to be the physical access to the datacentre hardware [5]. Malicious tools can be installed through network service and hijack the users' privacy. Although there are many securities software to prevent this issue, they are not sufficient to block all attacks as they are only used on specific purposes. For example, network firewall can only guarantee the protection on host and network level [6] [7]. Additionally, firewall defences cannot protect systems from cyber-attacks due to the following:

1. Firewall does not collect or store the session information, such as the conversations that happen in a user's browser. For example, it cannot determine when a user's cookies are sent and received.

2. Firewall does not provide adequate protection against web application and services attacks since these are launched on port 80, which is the network's default.

3. Since firewall only assumes that an attacker could be on the outside, this cannot be applied to cloud service as an attack could potentially be initiated from the inside.



The diagram above visually shows the data storage that is getting targeted by the criminals.

Section 3

To protect cloud storage, I have researched that encryption algorithm can be proposed as a solution to secure data safely [7] [8] [9]. Encrypting the data before the transmission avoids the unauthorised people to access into the imparting data, and so successfully protects the data. The main encryption methods that I have researched and experimented are listed below:

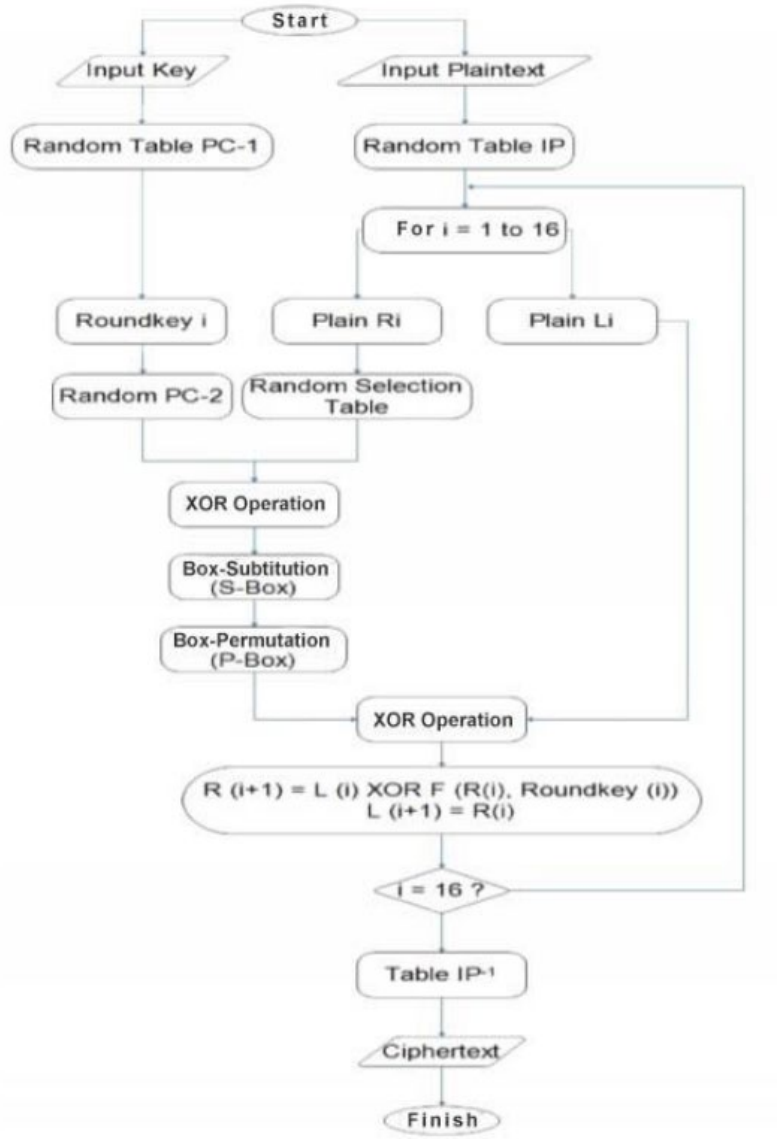
- MD5
- DES
- AES

MD5, a message-digest algorithm is a hash function that produces 128-bit has value on the encryption. This method is effective for determining the key in a partitioned database. It takes an arbitrary length of the text then creates a 128-bit fingerprint of the message. It is useful to store user passwords and any sensitive data. It can be used in Linux like below:

```
$secret_password=md5("password");
if (md5($_POST['password']) == $secret_password)
 {
 echo "Correct password";
 }
else
{
 echo "Incorrect password";
}
```

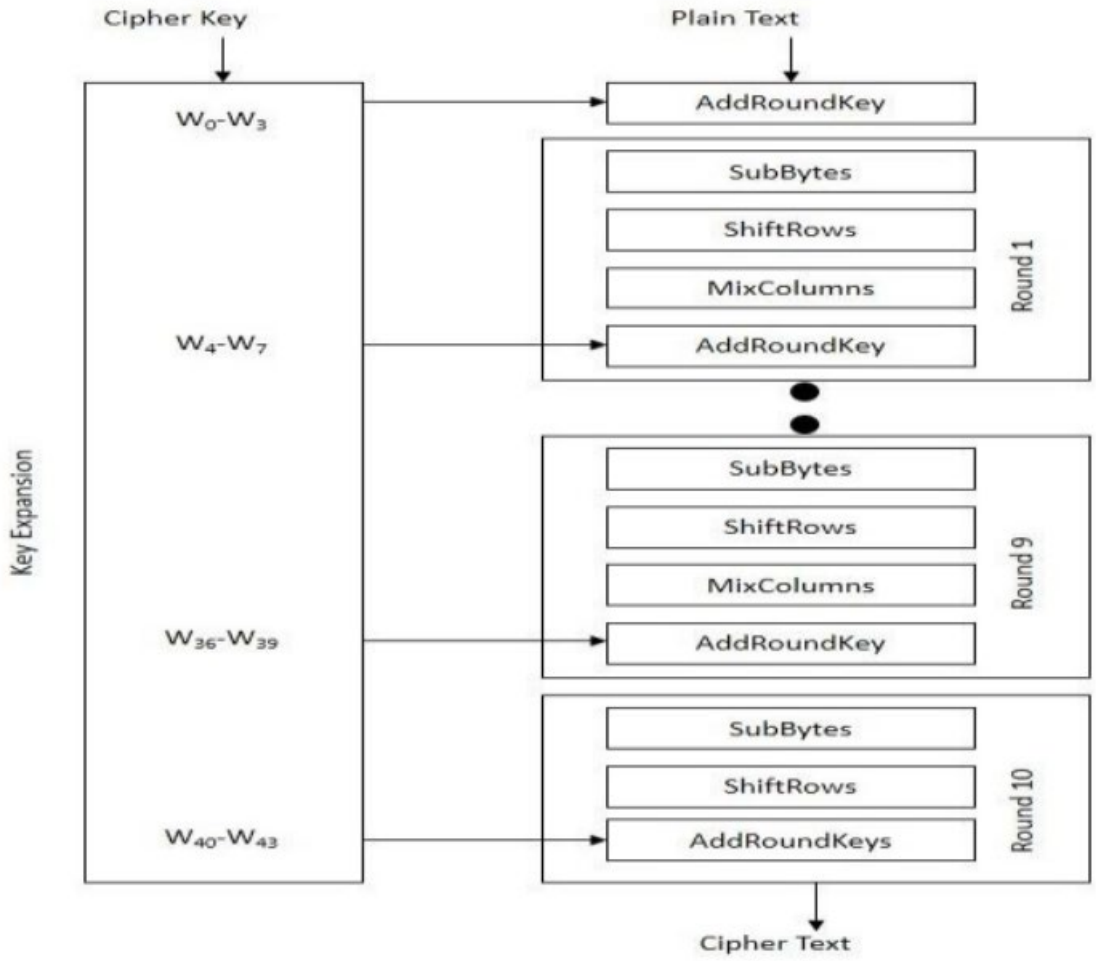
md5() is a pre-built method that contains the MD5 encryption, which automatically runs the algorithm of the password “password”. It then sends the text in $_POST[‘password’] and compare against the newest password that has been inputted. It brings to protect against the clear text transmission.

DES, a data encryption Standard is a symmetric key algorithm that has a length of 56 bits, published by NIST (National Institute of Standards and Technology). It has a block size of 64-bits, with the 16 round Feistel structure. The reason of its length being 56 bits is that it uses 8 bits out of 64 to function as a check bit only. It is working by taking a text input and splitting into small chunks to use it as a cryptographic key. It basically gets the input, then convert them into gibberish that can only be read by the approved user holding a decryption key. The flow chart of using DES algorithm is below:



The input (message) will be encrypted by DES algorithm and generate the cipher bits from each time and calculate the plaintext and the key. The algorithm gets 16 round processes, then creates 16 parts to produce a ciphertext.

AES, an Advanced Encryption Standard is the most commonly used encryption algorithm in other computing field, meaning that this can also be applied into cloud computing too. AES is a symmetric encryption algorithm to be found as 6 times faster than DES algorithm. It has increased computing power, larger key size, and faster encryption time than DES. It uses iterative rather than Feistel cipher method and comprises a series of linked operations. AES does all computations on bytes, thus when treating 128 bits, it treats it as 16 bytes. This is done to arrange in a simpler way for a faster processing time. Below is the diagram of how AES encryption is functioning:



AES algorithm is a block cipher with a length of 128 bits. It is always consisting with the lengths of 128, 192 or 256 bits. The encryption process is consisting of 10 rounds for most of cases. Each round contains 4 bytes of word, expanded into a key schedule of 44 4- words. SubBytes replaces the byte with another according to a lookup box. ShiftRows shifts each row certain number of time cyclically. MixColumns combines the four bytes in each column, then AddRoundKey derives them from the cipher. Each word is of 4 bytes and converts into 43 words key. These four words are representing W[0-3].

Conclusion

With the experiments of testing the encryption algorithms using Linux, and by theoretically drawing the flowchart and diagrams, it is proven that encryption can be applied to secure the cloud storage and security from the cyber-attacks. However, since these theoretical and practical experiments were not tested in real world fields against advanced level of hijacking tools, it cannot guarantee that this will resolve the current cloud security situation. This needs to be experimented in a more different way and need to be polished with the variety of testing. But as these algorithms are already applied into different computing fields and being used perfectly outstanding, it will not require a more complex steps to refine the method.

References

[1] Cleo. 2021. *Blog: On Premise vs. Cloud: Key Differences, Benefits and Risks* [online] Available at: <https://www.cleo.com/blog/knowledge-base-on-premise-vs-cloud> [Accessed 01 May 2022].

[2] Data Flair. 2020. *Website: Features of Cloud Computing – 10 Major Characteristics of Cloud Computing* [online] Available at: <https://data-flair.training/blogs/features-of-cloud-computing/> [Accessed 01 May 2022].

[3] TechRepublic. 2018. *Website: Features of Cloud Computing – 10 Major Characteristics of Cloud Computing* [online] Available at: <http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing survey/2384291> [Accessed 01 May 2022].

[4] Chou, David & Chou, Amy. 2008. *Article: Software as a Service (SaaS) as an outsourcing model: An economic analysis.* [online] Available at: <https://www.researchgate.net/publication/228447677_Software_as_a_Service_SaaS_as_an_outsourcing_model_An_economic_analysis [Accessed 01 May 2022].

[5] Muneer Bani Yassein, Shadi A. Alijawarneh. 2016. *Article: A Conceptual Security Framework for Cloud Computing Issues* [online] Available at: <https://www.researchgate.net/publication/302917009_A_Conceptual_Security_Framework_for_Cloud_Computing_Issues> [Accessed 01 May 2022].

[6] Haiyang Jiang, Guagxing Zhang, Gaogang Xie, Kave Salamatian. 2013. *Article: Scalable high-performance parallel design for Network Intrusion Detection Systems on many-core processors* [online] Available at: <https://www.researchgate.net/publication/261126882_Scalable_high-performance_parallel_design_for_Network_Intrusion_Detection_Systems_on_many-core_processors> [Accessed 02 May 2022].

[7] Deepika N, Durga P, Gyathri N, Murugesan M. 2019. *Article: Proficient Justification of Data Accuracy for Cloud Storage Using Dual Protection* [online] Available at: <https://www.academia.edu/44830943/Proficient_Justification_of_Data_Accuracy_for_Cloud_Storage_Using_Dual_Protection > [Accessed 02 May 2022].

[8] Ravi Kumar, Herbert Raj, Jelciana Perianayagam. 2017. *Article: Exploring Security Issues and Solutions in Cloud Computing Services – A Survey* [online] Available at: <https://www.researchgate.net/publication/321637905_Exploring_Security_Issues_and_Solutions_in_Cloud_Computing_Services_-_A_Survey> [Accessed 02 May 2022].

[9] Shahin Khan, M. Rifat Bin Emdad. 2019. *Article: A Standard Data Security Model Using AES Algorithm in Cloud Computing* [online] Available at: <https://www.researchgate.net/publication/333294905_A_Standard_Data_Security_model_Using_AES_Algorithm_in_Cloud_Computing> [Accessed 02 May 2022].