International Journal of Engineering & Technology, 7 (2.33) (2018) 864-868

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cloud cryptography: a new approach with distributed storage

Rakshanda Agarwal [1], Rajeshkannan Regunathan [2] *

[1] Bachelors of Technology, Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
[2] Assistant Professor (Senior), Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
**Corresponding author E-mail: rajeshkannan.r@vit.ac.in*

Abstract

With the evolution of cloud computing, there is an astounding need of security solutions. Some of the primary considerations here is brought on by inappropriate warehousing of data. This particular consideration significantly enhances users' anxiousness and minimizes the adoptability of cloud computing in numerous areas, including the financial industry and governmental agencies. The most effective method to offer risk-free data transfer is via cloud cryptography and storage techniques. Considering this, we propose a new and more secure algo-rithm for the transmission of data over the cloud. In this algorithm, the data is encrypted and then split into two different parts. Each part is stored in a different cloud. This makes the data challenging for being accessed by any type of hacker, even when accessed it will be of no use to him. This will use three encryption and two decryption keys, hence a combination of symmetric and asymmetric cryptography.

Keywords: *Cloud Computing; Cryptography; Privacy; Storage; Security.*

1. Introduction

Cloud computing is one of the magnificent advantages of information technology. Cloud computing is a model of data storage, handling, and supply in which very integrated physical resources are equipped to remote clients on request. In cloud computing, clients rather than buying actual physical devices such as storage, servers and networking equipment, lease these resources from the cloud provider. Its main advantage is potential cost reduction via efficient and optimized computing practices. It is also very flexible and portable, which means that it can be accessed at anytime from anywhere [1], [2].

The word cloud in cloud computing stands for a set of software, hardware, storage, networks, interfaces and services which all combine together to provide features of computing as a service. It permits individuals to do tasks they wish to do on a computer without the prerequisite for them to purchase and construct an IT infrastructure or to comprehend the fundamental technology. Cloud computing is dynamic in nature as the clients can access uniform IT possessions to install new services, applications or computing resources rapidly without the need to reengineer their complete groundwork [3].

Cloud Storage-as-a-service (STaaS) model has been broadly accepted approach along with big data and development of web based services. Cloud service providers such as Amazon, Dropbox, iCloud, Microsoft's OneDrive and Google drive have great storage services which provide giant and scalable cloud based services. [4] However security issues still persist and are a main problem to the users and service providers.

To securely transfer data, we need to overcome two primary challenges. First, the stored data needs to be secured against unsanctioned access. Second, both the data and its access must be protected from cloud storage service providers like the cloud system administrators. In such cases, one cannot just rely on password and other access control tools. Cryptographic encryption tools are usually used. However, simply having encryption and decryption implemented in the cloud storage systems is not sufficient [1]. One should have a proper encryption and decryption mechanism to protect data and along with it, should have a secure way to transfer this data to the user.

Now, who is responsible for this encryption and decryption of data so that it is transferred in a secure manner? A cloud broker does this job; it is a third party or individual that acts as an intermediary between the server and the client of cloud services. A cloud broker is also known as a cloud aggregator/enabler/customizer/agent. Its other functions include contract negotiations, transfer of customer data to cloud and deduplication. Basically, cloud broker is a software application which assists the organization of work between various cloud service suppliers. [5]

This paper focuses on the various issues on data security faced while the data is being transferred. We propose a smart cryptography approach which is designed to protect data from the intruders. This mechanism aims to encrypt the data first and then transfer the data via two different cloud channels without causing any latency or overhead. Here, data encryption is carried out using [3] keys and. On the other hand, the decryption process requires [2] keys only. The paper follows this specific flow pattern by first giving us an introduction about cloud computing, its storage etc. Section 2 explains the various security issues that any cloud computing practice faces, with specific focus on storage.

2. Issues faced by cloud

According to [1-3], [6-7] the major issues that a cloud faces are mainly due to data auditability and secrecy, capricious performance, scalable storage, software authorizing and bugs. This leads to many times of privacy and security attacks on cloud. These issues can be categorized as follows:

- Uncertain application programming interfaces: Cloud providers are responsible to provide a cloud interface to their

Copyright © 2018 Rakshanda Agarwal, Rajeshkannan Regunathan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

customers. These interfaces that are weak and user friendly are the foundation of security issues. A possible control can be a strong validation and admission control. [6]

- Malicious employees: Sensitive data that is handled away from the organization carries along an in-built level of jeopardy [3]. A high level of admittance to people or employees of the organization can lead to the outflow of trustworthy data. The solution of this issue is strict supply chain management practices, privileges can be set for user and employees that'll make it easier [6].
- Data loss or data leakage: Loss of encoding key and deletion of records without backup makes it difficult to restore all the data. Along with this, data theft and loss is also caused due to unauthorized access to cloud [6]. Malicious hackers are also responsible for data loss because they find ways to delete data and harm the business. Hence to avoid such loss of data, cloud brokers recommend distributing data across multiple cloud zones to increase the protection of data [7].
- Broken authentication: Huge amount of data attracts the attackers to break the security. Main reason for such security breaches mainly arise due to weak password and/or non-updated login credentials. Multifactor authentication is a way to avoid such types of attack; here the user needs to enter multiple keys to access the data. Also the credentials and keys should not be embedded in the code and must be entered by the user. [7]
- APT parasite: APT stands for Advanced Persistent Threat and are a class of threats comprising of advanced malware and botnet components which execute attack. Stuxnet is one such botnet and was used in an APT against a nuclear program of Iran. This attack caused Iran's nuclear centrifuges to spin at a great speed and then tear themselves apart [seven].
- Unknown Risk Profile: When the cloud brokers/providers are not willing to provide the organization with security logs, security practices and audit report we call it unknown risk profile [6].
- Flooding attacks: A malicious user can overload the data on cloud by sending spurious data requests to the cloud. The primary attempt of such attacks is to increase the workload of cloud servers by the intake of huge number of resources unnecessarily [1].
- Information Security: This type of security is related to information exchange between hosts or between users and hosts. It is related to issues like secure communication and authentication. Confidentiality and integrity issues are the ones related to secure communication. Confidentiality deals with the transfer of data from a user to only the legitimate receiver, while integrity indicates that the data received must be sent or modified only by legitimate senders [6].
- Data Stealing attacks: the stealing of user account password by methods like brute-force attacks is a form of data stealing attacks. In this form, the privacy and the confidentiality of the user and his data are ruthlessly ruptured. Ways in which such attacks can be prevented is by including an extra value while authenticating, this can be by SMS or any such similar methods [1].
- Cross-site scripting attacks: herein attackers inject a piece of code into the application in order to bypass the access control mechanism. With this, the attackers are able to gain free access to the data of all customers, plaintext passwords and also authentication data [1].



Fig. 1: Issues Faced by Cloud.

3. Various cryptography methods

Cloud storage being one of the most in demand service these days, there has been a continuous demand for resources and methods to keep this data secured. As discussed above, data stored in the cloud is prone to various threats and hence proper mechanism is required to protect this data in a secured fashion. Various methods have been implemented in the past which have advantages and disadvantages, here in this section we would like to point out few such methods and discuss them briefly.

Cloud security is a main topic of concern since the invention of cloud computing. There have been many algorithms proposed then and so are new algorithms being constructed as well. Paper [9] summarizes few of the existing algorithms mentioned in [15]. DES is one such symmetric key algorithm with a block cipher of 64 bits of which 56 bits is for data and 8 bits for padding. DES has a very small encryption key and hence security can be broken easily. Also DES works fast only on hardware and not software. To overcome the cipher size drawback, a new algorithm known as triple Des had been implemented. It is the enhanced version of DES and has a key size of 168 bits. Blowfish is another symmetric key algorithm with variable key size ranging from 32 to 448 bits. IDEA (International Data Encryption Algorithm) is considered to be the best symmetric key algorithm. Unlike DES which consists of 16 rounds, IDEA consists of only 8.5 rounds. The data is divided into 4 blocks of 16 bits each, while DES divides data in two blocks of 32 bits each. RSA is an asymmetric key algorithm where two large prime numbers are created then multiplied. Then, modulus is calculated and the number generated is castoff as the public and private key for the algorithm. These algorithms are not secure and there is necessity to enhance the security of data, which can be done by implementing new and more secure algorithms.

Similarly, paper [12] reviews and understands various issues in cloud security by analyzing various algorithms ensuring data security in the cloud system. Firstly, it explains all the symmetric key algorithms like Advanced Encryption Standard (AES) which has 128 bits of cipher block size and 128 bits of key size. Then is discusses about Data Encryption Standard (DES) and Blowfish algorithm just like in paper [9]. There are asymmetric key algorithms like RSA, Diffie-Hellman Key Exchange which introduces a key exchange protocol considering the help of a discrete logarithmic algorithm. Finally, a hashing algorithm known as MD5 (Message Digest algorithm 5) is widely used in cryptography that has a 128bit hash value with a variable length message into a fixed length output of 128 bits. All these algorithms require improve-

ment and have a wide scope for the same which promotes the researches for developing new and improved algorithms.

According to [6] data must always be encrypted first and then transferred when stored using a symmetric key encryption. If this encryption us carried out properly, if anyone tries to access the data the data will seem non-sensible to them. Hence, a new method has been proposed where in the key has also been encrypted along with the data. In this method a storage account is created with a cryptographic key, this account consists of queues, tables and containers. The container has a facility known as blob that is similar to files in Windows. Any existing algorithm like RSA can be used to implement this. Though a good idea, but this method can still be flawed if the encryption key is known.

The major issue according to [11] is data security and privacy while the data is being transferred. This algorithm aims to provide security to data at rest and also data during transmission; this has been achieved using Extensible Authentication Protocol-CHAP and Rijndael Encryption Algorithm. In this algorithm there is a cloud broker involved that encrypts the data first then transfers it via cloud and the data can be downloaded and decrypted using the key. The main issue of this algorithm is lack of integrity check mechanism. Also paper [13] deals with Cloud data storage and security during transmission of data which has since ever been an important aspect in determining the Quality of Service. This paper proposes an effective and flexible distribution scheme which achieves storage integration and data error localization. In the method proposed, encryption is carried out in the upper layer that is above transport layer rather than in SSL. Thus this scheme can be implemented without any modifications in the IP layer. This methodology is highly reliable to malicious data, byzantine failure and also modification attacks.

After analyzing the security issues in cloud computing [7] proposed an algorithm which aims to enhance security at the layers. This algorithm has been made using a combination of multiple existing algorithms such as DES, blowfish etc. This technique mainly uses honey encryption along with a distribution transforming encoder (DTE). In honey encryption, there exists a message space which has all the possible messages and then DTE is used to map these messages. Honey encryption when coupled with DES provides great security to messages and passwords without the need of a large database. The only drawback of this algorithm is its increased complexity due to large databases required for storage and mapping purposes.

In [10], user specified key parameters were used to encrypt data so that the system becomes more robust. This was done using a new algorithm which the paper proposes to be more light weight and has easy computation. The encrypted data is stored on a cloud based platform and token checking is performed to give a secure data. The scheme is highly buoyant against malicious data modification attacks and byzantine attack. The main focus is on token generation so that data and tokens can be verified before they are distributed to the cloud. Along with token generation this algorithm uses block storage that gives better performance and there is an easy distribution of block to different cloud storage areas, but fails in case of dynamic cloud data storage and the problem of fine-grained data error localization..

We know that cloud storage shifts the data to data centers that are remotely located and the users have no control or say towards this. This feature seems great for cloud providers in terms of storage but not in terms of security and hence one need to understand and solve these challenges. The two main issues faced between the cloud providers and clients are integrity and privacy of data. Hence, paper [14] uses a combination of digital signature and encryption. Here in, once the request is made, it is accepted using a digital signature which is then encrypted along with the message. This digital signature can be used to verify the legitimacy of data. This method seems appealing but has a flaw, if the public key is known, both the data and signature can be changed, and ultimately there will be no point on the overall existence of this technique.

Cloud security becoming a hot topic today, another method of digital signature and encryption using elliptical curve cryptography (ECC) technique has been proposed in paper [3]. Elliptical curve cryptography is an example of public key cryptosystem. In this method, once a data request has been made, keys are generated, both public and private. Then a signature is generated using hash function on the data provider's side. Now, the data and the signature are both encrypted using ECC and then transferred to the requestor. The requestor now decrypts this message and authenticates the signature. The issues faced by this paper are quite similar to the ones faced by paper [14]. It still faces many basic security issues and hence a better approach is required.

Data security being the main issue in cloud computing, paper [8] aims to design a new cryptography technique using a hybrid approach. This method is a combination of both symmetric and asymmetric key algorithms, with Blowfish symmetric key dealing with data confidentiality and RSA dealing with data authentication. This method also uses a secure hash algorithm-2 for data integrity management. Here the key is encrypted using RSA while the file is encrypted using blowfish algorithm. SHA-2 is used to transmit data over the internet. This algorithm seems alluring but there hasn't been a clear explanation on the pros and cons about this algorithm. A clear study is needed.

4. Proposed methodology

We do understand that cryptography is not the only solution for data security and privacy in the cloud environment. Hence, we propose a new algorithm which includes cloud based cryptography and also a different storage approach to store the data. This involves applying our own encryption and decryption algorithm to the plain text, and in that process dividing the data into two. This divided data will now be stored at different cloud storage locations. This will prevent any intruder from attacks on the data and if by any chance the data is accessed, it cannot be decrypted without the other half of the data being accessed.

Let us explain our proposed algorithm with an example. We will require the user's mail id, plain text and three encryption keys. First, we take a plain text and XOR it with our input binary key. This will be our first step of encryption. Next we take the second key and divide our text into two using D-K and D+K, where D represents data or text and K is our key. Now, finally using our third encryption key, we XOR these two cipher text again and store them at different locations in the cloud, let us say cloud A and B. This comprises of our encryption process. The flow diagram of the same has been shown in Fig. 8.

Now, for the decryption part, the user will have to enter a user id and two decryption keys. If the user id matches the user will have access to see the cipher text which was produced in the encryption process. To begin with the decryption, the algorithm will first access both the cipher texts stored at different locations and XOR them with the first key. After the XOR operation is performed, both the data will be added together considering their ASCII values. Now we have a single cipher text, again we perform XOR with the second key we have and the final decrypted original plain text is ready for us. This process has been explained with the help of a flow diagram in Fig. 9.

This algorithm has been built using javascript. It can be accessed using a simple nodejs server and also a heroku based web applet. The GUI for this system is very simple and hence easy to use for everyone. The cloud storage service used is mlab for mongodb databases. This is a very time and space efficient algorithm and hence can be used for future pursuit.

It has the following benefits in terms of privacy and security:

- The data cannot be accessed without a user id.
- Even if the user id is known, and the data is accessed, it cannot be decrypted without knowing both the keys.
- If the data is hacked on the cloud, and the hacker finds out the keys, it still cannot be decrypted without the access of the other part of data which is stored at some other location.

All these possibilities make the storage and the algorithm a secure one. It is free from fishing, intruders, hackers and other types of

attacks most of which we have discussed in Sec.2. It is a very simple yet a reliable method of cryptography on cloud storage. It has the benefits of both cryptography and varied possible storages, which as discussed are a must of any good algorithm to be implemented.

The algorithm has been explained below and also the figures below explain the sample GUI and input output of our program. The below figures, from Fig. 2-7 depict different stages of the algorithm. In Fig. 3, the user inputs the required parameters which include email address, 3 keys and plaintext. Similarly, Fig. 4 shows the encrypted text and how the data is distributed in two different clouds. Fig.6 shows the get data button where you can only see the encrypted text on input of email id and Fig. 7 shows the final message after decryption.

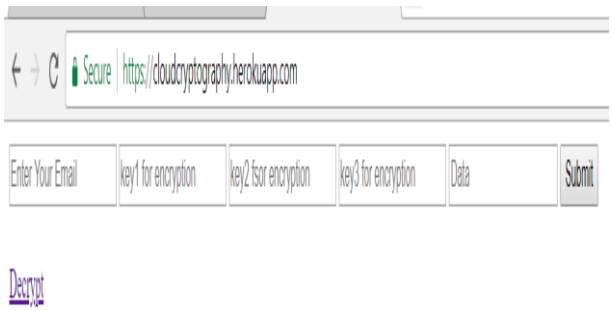


Fig. 2: Initial App Screen for Encryption.

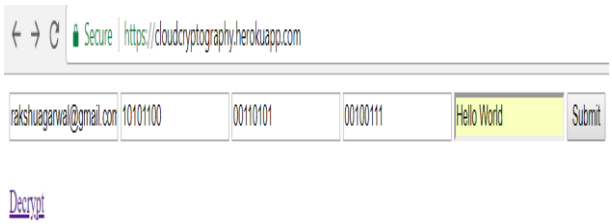


Fig. 3: Input for Encryption.

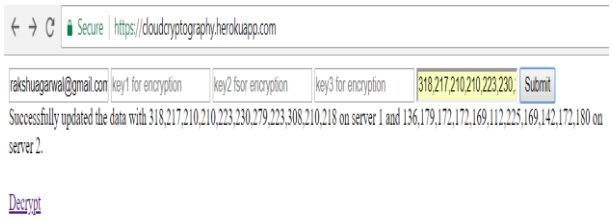


Fig. 4: The Encrypted Text Stored at Two Different Clouds.

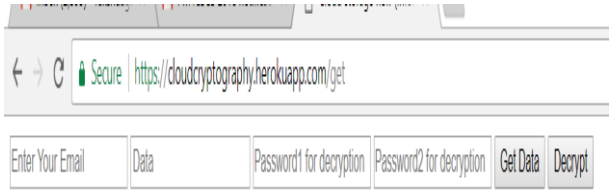


Fig. 5: Initial Decryption Screen.

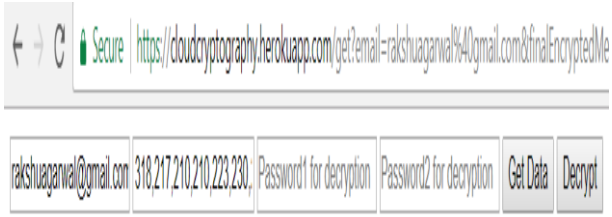


Fig. 6: Get Data Option to Get Encrypted Data.

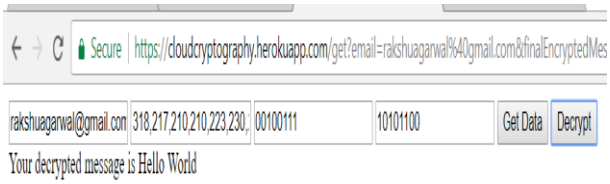


Fig. 7: Data Obtained after Decryption

4.1. Encryption process

1) Start
2) Input user id, plaintext (D) and [3] keys (K1, K2, K3) into the text box and click on encrypt button.
3) Convert the text to char array.
4) Perform XOR operation

$$D1 = D\text{^}K1 \quad (1)$$

5) Add and subtract K2 to divide data into two

$$D2' = D1 - K2 \quad (2)$$

$$D2'' = D1 + K2 \quad (3)$$

6) Perform XOR on this data D2' and D2''

$$D3' = D2'\text{^}K3 \quad (4)$$

$$D3'' = D2''\text{^}K3 \quad (5)$$

7) Store this data D3' and D3'' on cloud A and Cloud B respectively
8) Stop

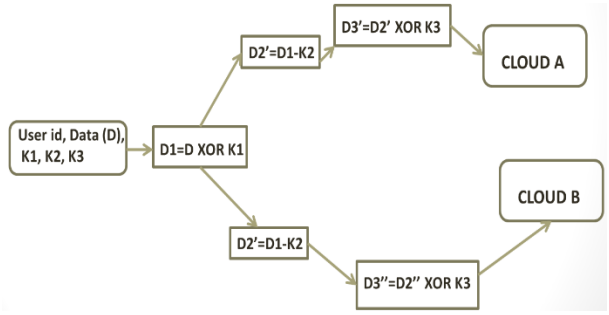


Fig. 8: Encryption Process.

4.2. Decryption process

1) Start
2) Input user id, and two keys (K1' and K2')into the text box
3) If Clicked on getdata button go to step 4
   Else, go to step six
4) Extract D3' and D3'' from cloud A and cloud B respectively for the respective user id input by the user.
5) Print it in the form D3'+D3''
6) If clicked on decrypt go to step 7
7) Extract D3' and D3'' from cloud A and B respectively for the respective user id input by the user.
8) Perform XOR of D3' and D3'' using K1

$$D4' = D3'\text{^}K1' \quad (6)$$

$$D4'' = D3''\text{^}K1' \quad (7)$$

9) Add D4' and D4'

$$D5 = D4' + D4'' \quad (8)$$

10) Right shift D5 to divide it by 2

$$D6 = D5 >> 1 \quad (9)$$

11) Perform XOR of D5 using K2'

$$D = D6\text{^}K2' \quad (10)$$

12) Display this final message on the applet. This is the de-crypted message.
13) Stop

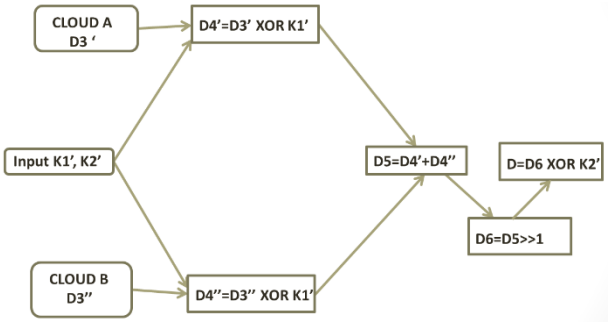


Fig. 9: Decryption Process.

5. Conclusion

Considering the security issues in cloud computing, we have successfully implemented a new algorithm that encrypts and decrypts the data. This algorithm not only uses cryptography but also uses a different storage mechanism that makes it more efficient. This special method of splitting data and storing it in two different clouds makes it more secure. This algorithm is available to everyone, portable and reliable to any party wishing to access it due to its simple architecture. This algorithm can be run as a web applet and also as a standalone application which again makes it multi-disciplinary in nature. Hence, our algorithm is better than most of the existing methods and can be used for implementation in various areas of cloud computing.

References

[1] Kumar, Shyam Nandan. "Cryptography during Data Sharing and Accessing Over Cloud." International Transaction of Electrical and Computer Engineers System 3.1 (2015): 12-18.
[2] Van Dijk, Marten, and Ari Juels. "On the impossibility of cryptography alone for privacy-preserving cloud computing." HotSec 10 (2010): 1-8.
[3] Gampala, Veerraju, Srilakshmi Inuganti, and Satish Muppidi. "Data security in cloud computing with elliptic curve cryptography." International Journal of Soft Computing and Engineering (IJSCE) 2.3 (2012): 138-141.
[4] Li, Yibin, et al. "Intelligent cryptography approach for secure distributed big data storage in cloud computing." Information Sciences 387 (2017): 103-115.
[5] http://searchcloudprovider.techtarget.com/definition/cloud-broker
[6] Thomas, G., Jose, V., & Afsar, P. (2013). Cloud computing security using encryption technique. arXiv preprint arXiv:1310.8392.
[7] Choudhury, T., & Kumar, P. (2016, November). Proposal and implementation of cloud security algorithm to enhance the security of the layers. In System Modeling & Advancement in Research Trends (SMART), International Conference (pp. 316-321). IEEE.
[8] Timothy, D. P., & Santra, A. K. (2017, August). A hybrid cryptography algorithm for cloud computing security. In Microelectronic Devices, Circuits and Systems (ICMDCS), 2017 International conference on (pp. 1-5). IEEE.
[9] Pansotra, E. A., & Singh, E. S. P. (2015). Cloud security algorithms. International Journal of Security and Its Applications, 9(10), 353-360.
[10] Srinivas, P., & Kumar, K. R. (2013). Secure data transfer in cloud storage systems using dynamic tokens. IJRCCT, 2(1), 006-010.
[11] Singla, Sanjoli, and Jasmeet Singh. "Implementing Cloud Data Security by Encryption using Rijndael Algorithm." Global Journal of Computer Science and Technology 13.4-B (2013): 19.
[12] Chatterjee, R., Roy, S., & Scholar, U. G. (2017). Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud. International Journal of Engineering Science, 11818.
[13] Bhisikar, P., & Sahu, A. (2013). Security in data storage and transmission in cloud computing. International journal of advanced research in computer science and software engineering, 3(3).
[14] Wagh, K. S., Jathar, R., Bangar, S., & Bhakthadas, A. (2014). Securing data transfer in cloud environment. International Journal of Engineering Research and Applications, 4(5), 91-93.
[15] https://www.garykessler.net/library/crypto.html#types.