IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 8, August 2020

DOI 10.17148/IARJSET.2020.7817

Cloud Computing Security Challenges

Nada Alrehaili[1], Agadeer Mutahar[2]

Department of Information Systems, Faculty of Computing and Information Technology,

Jeddah, Kingdom of Saudi Arabia[1,2]

Abstract: Cloud computing is a basic term in the development of computers; it is the ability to access, share a collection of sources that are owned and stored by another party over the internet. Once we have shared the information over the internet, we must consider the security problems such as confidentiality, integrity, and authentication. In this paper, we reviewed some of the security techniques in the field of the security of data stored in the cloud storage with combination with transitions issues. Also, we compare RSA, AES, MD5, BLOWFISH, and Diffie-Hellman, techniques. Then monitored and recorded the most important results obtained.

Keywords: Cloud computing, Security, Confidentiality, Integrity, Authentication.

I. INTRODUCTION

The idea of cloud computing dates back to the 1960s from the 20th century it is associated with John McCarthy. Also, the practical and actual application appeared at the beginning of 2000 through Microsoft and then followed by Google and Apple. Moreover, cloud computing can define as a set of services provided to a client or multiple clients over the internet to take advantage of the capabilities of the service provider without having to purchase expensive hardware in the company to do the same tasks. Besides, the cloud provides many benefit based services and applications as cost-saving, scalability, flexibility, reliability, maintenance, and mobile-accessible [1]. There are two types of cloud architecture service model and deployment model we illustrate it as follows:

• Cloud computing service model

1. SaaS (Software as a Service model): enable their users to access service through operating simple software as a browser like Gmail.
2. PaaS (Platform as a Service): enable their users to develop applications and deploy them, like Google App Engine.
3. IaaS (Infrastructure as a Service): enable their users to access the computational and storage infrastructure in a central service.

• Deployment cloud model:

1. Public cloud: infrastructure that provides all computing applications and resources to people or a large organization group by the single service provider.
2. Private cloud: infrastructure leases to a single organization so that it works for itself and at its full disposal in the data, security, quality, and efficiency of the service.
3. Community cloud: infrastructure shared between different organizations. That supports a particular community that has a common concern.
4. Hybrid cloud: infrastructure that combines public and private cloud models so that each can be provided [2].

Many of organizations small or big prefer using cloud computing, but they are apprehensive about data production. In this paper, we move to discuss the security challenges and the best way to protect the data from any possible risk and how the cloud can handle it. There are still some concerns about data breached or moved, limited control of data, insecure interface, sharing of resources, data availability, and inside attack.

II. PROPLEM AND RESEARCH CHALLENGES

Cloud computing security issues are one of the biggest challenges that lead to delaying cloud adoption. Since it is a service available on the internet so many issues will appear. First, the availability of data for the users will be in a continuous manner regardless of user location. Second, the integrity of data by ensuring that transmitted messages are the same as the received one no changing between them. Third, the confidentiality of data by avoiding the illegal user from access. Moreover, the security of the user's data depends on the cloud provider's responsibility.

In this paper, we focus on cryptography methods by making a comparison between many algorithms to provide secure data encryption to get efficient data security. Cryptography is the discipline that provides a secure data transmutation then retrieve the data by using a specific channel. Further, it includes two main encryption process to convert the data text to unintelligible data (plaintext to ciphertext) [3].

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 8, August 2020

DOI 10.17148/IARJSET.2020.7817

III. TOOLS AND APPROACH

Providing a secure cloud computing over the network need to an encryption algorithm that takes a vital role. Also, it is a fundamental tool for protecting the data. In this paper, we compare different types of algorithms and illustrate it as follows:

- Symmetric Algorithms use one key to encrypt and decrypt data. This type of encryption depends on the key used which means the person who has the key can decrypt and read the content of messages or files, like Data Encryption Standard (DES), BLOWFISH, and Advanced Encryption Standard (AES).
- Asymmetric Algorithms has two keys the first one is the Public Key (PB) and the second one is the Privet Key (PK). The PB encrypts the messages, and the PK decrypts the messages like RSA, Diffie-Hellman key Exchange (D-H9), and DSA.
- One-way encryption algorithms it is encrypted then transformed to come up with something called the (Hash Key), in this type no way to decryption and get the original message from it like MD5 [1].
- Elliptical Curve Cryptography (ECC) depends on the PB approach to creating cryptographic in an efficient and fast way by using the elliptic curve equation rather than the traditional method. Also, this algorithm can use with RSA, and Diffie-Hellman [3].
- Common Scrambling Algorithm (CSA) is an algorithm that encrypts video streams [4].

IV. CLASSIFICATION OF CLOUD DATA

Cloud computing has three types of data: storage data, transmission data, and processing data [2]. In this paper we covered the data storage part essentially with some of the combinations with transmission data part as follows: About data storage, [5] proposed architecture to have secure communication as well as cover the information from unrelated users. They use RSA encryption and MD5 hashing for the digital signature technique. While Intel [6] also discussed data anonymization as well as prevents the information from unrelated users by using only AES encryption. On the other hand, [7] proposed algorithms to improve the security of the data stored in the cloud storage by using AES and RSA algorithms. [8] proposed algorithms to make sure the security of the data store in the cloud. They made a comparison between (AES, DES, Blowfish, and RSA) consequently they figure out the best safe algorithm. Compared to [9] they also proposed a method to protect the data store in the cloud, as well as communication, is secure by using only the RSA algorithm based on time, space complexity, and throughput. [10] evaluated the performance level of security algorithms like DES, MD5, AES, RSA, and BLOWFISH, by depending on two main characteristics the speed-up ratios and the mean processing time. [4] proposed a scrambling algorithm and multilevel of encryption methods then they designed, applied, and tested the model according to an image category that was stored in a cloud area. [2] they clarified how investigates the security of cloud architecture problems by illustrated the main attributes of cloud and service models.

On the other hand data storage and transmission, [11] proposed a model depend on the grouping of AES and RSA to protect the cloud storage. Also, this method makes it hard to attack the transferring information through the cloud. [3] designed a cloud architecture to guarantee data movement by using the Diffie-Hellman key for connection and ECC for encryption.

V. DISCUSSION

[5] uses RSA encryption as well as MD5 hashing for a digital signature technique to make sure that the communication is secure furthermore hide the information from unnotarized users. As a result, they found that the RSA algorithm can support the security for confidentiality. Also, can ease the connection between the user and the system, while the MD5 algorithm can support in terms of confidentiality. Thus, each algorithm can execute in separate servers which solve the problem of the slowing system. Furthermore, the combination of the RSA algorithm and digital signatures provide strong security as well as obtained the data integrity service system. So, they found that the MD5 algorithm is more and highly secure. On the other hand, Intel [6] uses AES encryption for data anonymization hence they found that they can use the anonymization records in each of performance analysis and security analysis. In the performance analysis, they have discovered some issues such as the increase in access time. Whilst in the security analysis they found some issues such as the probes on the server of the web. Therefore, they found that the anonymization is a new case for (Intel AES-NI) which is a modern technology that uses several techniques of anonymization (e.g. hashing) and makes AES encryption faster. [7] presented a method to enhance the security of the data stored in the cloud by using AES and RSA algorithms. As a result, they found that the time of downloading is longer than the time of uploading. Also, the AES algorithm more secure, fast, has not been broken before and it is faster on each side (upload -download). Besides, the key of symmetric can change therefore the security can be improved, while the algorithm called RSA-1024 is strong and never hacked before. Finally, the data decryption has two authentications; the user must know the policy to enter both company's server and cloud storage. Whereas [8] made a comparison between (AES, DES, Blowfish, and RSA) to ensure the security of the data stored. Consequently, they have found that the less executed time of cloud data is performed by the AES algorithm while the less memory requirement in the Blowfish algorithm. Also, the less encryption time is the DES algorithm while

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 8, August 2020

DOI 10.17148/IARJSET.2020.7817

the long memory size and the encryption time is the RSA algorithm. On the other hand, [9] presented algorithms to make sure secure communication and data stored by using RSA only on three parameters which are time, space intricacy, and throughput. Hence that supports evaluating the efficiency and effectiveness of RSA algorithms. In the time complexity, they found that the equation with very little error is O(n^2), and the increase of the PK length will increase the time as well as it will be non-linear and exponential. While in space complexity, they found that the increase of PK length will increase the run time memory. Finally, the increase in throughput will increase system efficiency. So, they found that they must decrease the length of the PK and make a compromise about data security. Also, [10] they analyzed the data security model in programming-level-environment as Platform as a Service (PaaS), it provides the operating environment. They experiment with five encryption methods DES, MD5, AES, RSA, and BLOWFISH by implemented in the sandboxed area by Eclipse program.

Eclipse is an integrated improvement condition which is utilized to create and run the applications. Consequently, they implemented the comparison between the algorithms with various sizes 10KB, 13KB, 39KB, and 56KB. The comparison was according to the speed-up ratio and the mean processing time. As a result of this comparison, they found that the RSA is consumed the average time, and MD5 has a minimum time-consuming. AES and MD5 speeds-up ratio drops sharply with the increasing of the input size, and DES comes after AES in the speed-up ratio. Also, RSA, DES, and BLOWFISH remain fixed mostly with an increase of input size also they have a small change in speed-up ratio. Finally, to reduce the time and increase the security select MD5 then select AES. Moreover, [4] clarified that cloud computing issues such as security of data, file system, backup, network traffic, and host, It presented a new model based on a multi-cloud distributed system. They focused on the security of the stored images in the cloud environment, but it can apply to another type of information such as voice, text, multimedia, and even movies. Also, it has a robust security model for cloud computing based on the Scrambling Algorithm and Multi-Level Encryption to provide high-level security on the stored data on a cloud environment. As a result, they found that the algorithm is highly secured because three levels of security are applied to the data before store it in the cloud. And they also used a complex but fast symmetric encryption as opposed to a time-consuming RSA algorithm. Besides, they applied two different scenarios similar to DESSKY to increase the viability as well as accessibility. Then they found that the algorithm has a better performance than DEPSKY because the scrambled algorithm applied before the encryption. Finally, used the Malakooti Polynomial coefficient to generate the individual key and they suggest that these coefficients can be replaced with biometric features obtained from the Fingerprint, face, or even the user. Also, [2] proposed and implemented new software to choose the highest security algorithm. The software makes a performance analysis between eight algorithms DES, 3DES, Two Fish, Blowfish, MARS, AES, RC4, and RC6. The performance analysis was applied in Amazon EC2 as a case study of software by using NIST statistical. After a comparison between the Amazon EC2 cloud and the traditional ones, the researchers found that the EC2 Amazon has better secure technology, based on the NIST test. While the AES has the best security encryption algorithm, and DES or AES take less time for encryption and faster time for retrieval. In a conclusion, AES is the most suitable algorithm for Amazon EC2 which has high security and less time.

[11] they found that using symmetric encryption will raise the opportunity for the attacker to stole the secret key. So they proposed a model with a combination of the symmetric and asymmetric methods (RSA and AES) to share data in the secure cloud. They also, provide a model that contains three entities: the user, the Cloud Service Provider (CSP), and the Cloud Storage System (CSS). Which is simulated in the framework the main process is to generate a PK and PB. Besides, they used a single protocol to make communication between the user and the cloud. After they implement this model, they figure out some features as secure transmission of documents amongst clients. Also, the cloud has a poor possibility to find the symmetric secret-key, when using asymmetric encryption. Which makes it hard for attackers to read the documents until they have the PB and the symmetric encryption has less time for transmission. As well as, they found some drawbacks as asymmetric key generating leads to time-consuming. If the file size increment more than 256byte, the encryption process will be double, and the number of keys created for each document will be triple times for each document stored in cloud storage. [3] provided a cloud architecture that focuses on security issues and provides a new mechanism to ensure the security of data. The proposed model depends on Elliptical Cryptography with the linear method. Through three secure points: authentication, key generation, and data encryption. After applying this mechanism, the researchers found that the Diffie Hellman protocol is very good in the connection part. ECC has advantages compared with the linear algorithm, it has less cost and time, and ECC has advantages with a difficult to penetrate because of the complexity of sub-exponential time.

VI. CONCLUSION

In this paper, we reviewed some security problems in cloud computing. Also, discussed some different algorithms that were proposed to treat the security problems in communication, data anonymization, data stored in the cloud storage. As a result, we found that various types of algorithms can protect the cloud by different levels and different uses. If we need to support the confidentiality and provide the best security policy the RSA can be used but it needs more memory size with a long time for encryption, it is used in Google mail, Yahoo mail, etc. While the AES encryption is faster and has

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 8, August 2020

DOI 10.17148/IARJSET.2020.7817

less executed time with high security which is used in government and banks. The MD5 algorithms can be used to support authentication and have a high level of security. Finally, EC2 Amazon provides better security technology.

REFERENCES

[1] S. K. Randeep Kaur, "Analysis of Security Algorithms in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, p. 6, 2014.
[2] H. S. A. Eman M. Mohamed, Sherif El-Etriby, "Enhanced data security model for cloud computing," presented at the 2012 8th International Conference on Informatics and Systems (INFOS), Cairo, Egypt, 2012.
[3] N. Tirthani and Ganesan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," IACR Cryptol. ePrint Arch., vol. 2014, p. 49, 2014.
[4] N. M. Mohammad V. Malakooti, "A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption," in Proceedings of the International Conference on Computing Technology and Information Management, Dubai, UAE, 2014.
[5] S. R. Lenka and B. Nayak, "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm," International Journal of Computer Science Trends and Technology (IJCST), 2014.
[6] I. IT, "Enhancing Cloud Security Using Data Anonymization," Intel 2012.
[7] Z. Kartit and M. El Marraki, "Applying encryption algorithm to enhance data security in cloud storage," (in English), Eng. Lett. Engineering Letters, vol. 23, no. 4, pp. 277-282, 2015.
[8] R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," International Journal of Engineering Research and Applications (IJERA) 2013.
[9] A. Khatoon and A. A. Ikram, "Performance Evaluation of RSA Algorithm in Cloud Computing Security," International journal of innovation and scientific research, vol. 12, pp. 336-345, 2014.
[10]G. Kaur and M. Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms," Int. Journal of Engineering Research and Application vol. 3, no. 5, p. 5, 2013.
[11]N. Khanezaei and Z. M. Hanapi, "A framework based on RSA and AES encryption algorithms for cloud computing services," 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), pp. 58-62, 2014.