Homomorphic Technique for Secure Data Transmission in Cloud Computing

Garima Jain
Assistant Professor, Department of Computer Science and Engineering,
Swami Vivekananda Subharti University, Subharti Institute of Technology and Engineering,
Meerut, Uttar Pradesh, India.

Namit Kumar
Student, Department of Computer Science and Engineering,
Galgotias College of Engineering and Technology
Gr.Noida, Uttar Pradesh, India.

Abstract

Cloud computing model is used because of its diverse and extensive phenomena. The architecture of cloud computing is one in which there is no existence of central manager which results in various breaks occurred in the network. To guarantee the transmission of data from the source to the destination, two types of cryptographic schemes are introduced, i.e., the fully homomorphism and fully disk encryption are familiarized. The completely homomorphic cryptography scheme is safer and lighter than fully disk encryption. In the paper, an improvement of completely homomorphic cryptography is planned using elliptic curve cryptography and OTP generation**.**

Keywords: Homomorphic encryption, OTP, Elliptic Curve

INTRODUCTION

Weather Cloud Computing enables user for their future use to store their sensitively large amount of data in an untrusted distantly providers of cloud service to achieve scalable services on-demand as well as services that can be available with least efficiency. The group that can store data in centralized can be retrieved as well as modified by the user as per the requirement. Fully homomorphic cryptography schemes in the recent scenario maintained as highly suggested for data security in cloud computing [13].

A system through which services are provided to the user by the cloud facility provider as what the demand is known as a cloud. Cryptography could be an electronic technique that wont to shield valuable information over transmission. Primarily cryptography is science to produce security to data. Coding is happened at the sender facet. Encrypted algorithm program is created to form data indecipherable by all supposed receiver.

Encryption (plaintext, key) = cipher text

Decryption (cipher text, key) = plaintext

We defined decryption as the reverse process of encryption. There are two main terms which is used for the defining cryptography method are Encryption and Decryption. Elliptical curve cryptography is defined as a recent research in the field of cryptography. The ECC i.e.., elliptic curve cryptography is evolving as a crucial cryptography, and shows a promise to be an alternate of RSA.

Objective

Cloud facility Provider is another name for this system that is generated based on its functioning. This system thus works on the fundaments that the cost and facilities charged to the user depend upon the services required by him. Thus, large numbers of applications are given under several topologies within this technique. Further, some new specialized services are provided by each of the topology. Cloud security is termed as the mechanism through which the network and the information being exchanged are secured from any unauthorized users. Various types of data and applications that exist within the cloud computing scenarios are secured by applying various sets of policies, technologies and controls [1]. To avail any service, security is considered to be the most important factor. Each field requires both internal as well as external security approaches. The integrity as well as privacy of a cloud is ensured through privacy measures. However, every security mechanism has certain loopholes due to which the privacy of the system is interrupted. Security is the only problem we should focus on cloud computing.

In fact, you do not know what is happening with your data, since it is stored by a third party, such as the application and the web browser. Data centralization is the main advantage for cloud computing.

When data is stored on the hard disk without any encryption, there are many possibilities for data loss.

When you upload your data to the cloud, there are adequate encryption standards to encrypt the data and no one can take benefit of it, if the data obtained is encrypted [2]. The general conclusion is that your data is safe in the cloud compared to local storage.

The major advantage of the cloud is; you don't have to do anything yourself. Everything depends on the provider. They will provide you the security. If you believe your defined data has been cooperated, there is an online service or service for this. You can make replica for

all data offline and analyze it.

Fully homomorphic cryptography offers the best protection against full disk encryption. Unlike FDE, encryption does not apply to the entire disk; Encryption is applied in every function. Encrypted text and plain text are not related, but have a key point of algebraic operation that works in both [3].

After the invention of RSA i.e.., Rivest, Adleman and Dertouzos present the idea of fully Homomorphic schemes[20]. Without providing any preliminary decryption of the operands, the data is encrypted using encryption function. The privacy homomorphism is known as the approach that collectively operates those schemes. Fully homomorphic cryptography can be used to query a search engine, without including that for what you are looking for. More precisely, we can say that FHE has many properties. The entire physical disk is encrypted with a physical key for the maximum speed and simplicity in the disk firmware in the case of fully disk encryption. In the case of a stolen laptop, we can find it a very effective technique to protect.

Therefore, it cannot fulfill the requirement in which physical theft are not main threat but it can visualize on data protection goals [4]. We can evaluate the full disk encryption is one of the most effective ways to protect our data which is private on various electronics devices like laptops, tapes, etc. Your data may be lost permanently when an encrypted hard disk becomes corrupted. The FDE solution includes several methods for receiving admission to the unit when a consumer can no longer authenticate. This can find to be a recovery key, or we can say that a recovery password, or an emergency login. Once we can verify that it is common with practice, make sure that recovery information is centrally supported, testing recovery strategies.

The Diffie-Hellman algorithm is one of a first simple algorithm for agreeing on a key to make use over an insecure connection ever developed.

The keys are exchanged by the protocol in a limited manner. In the result of there is no mechanism for entity authentication.

Man-in-the- middle attack is an attack in Diffie- Hellman algorithm due to which protocols of Diffie –Hellman are easily attacked.

It proposes the use of randomized limitation in both schemes, so that both the two parties on each side need to choose two numbers n and p this will allows to produce a new shared secret key each time a communication session is build pab(mod n) from the known values of pa (mod n) and pb (mod n) and to produce various types of different encryption messages for every kind of messages even for similar message.

The Diffie–Hellman method does not allow for encryption and decryption, in this both agree with symmetric key in which master and slave agree to exchange a data. It allows two end parties that do not have preliminary information of each other to commonly initiate a shared secret key through an unsafe communications over a channel.

Two major challenges which come from the idea of public key cryptography.

In key distribution the very first problem faced: The use of predictable encryption would like to communicate using digital systems as a means, using conventional encryption for all who have never meet before. The other problem was the problem of signatures: this is a method of providing a person with a view of a person on request.

Elliptic Curve Cryptography is one of the recent fields in the area of research in the field of Cryptography. The elliptic curve cryptography (ECC) is progressing as an important cryptography, and it shows a capability to be an alternative of RSA. Elliptic Curve Cryptography can be used to form smaller, faster, and more effective cryptographic keys. Elliptical curve cryptography (ECC) is a (PKC) public key encryption method which is grounded on elliptic curve theory that can be used to produce various possibilities i.e.., faster in speed, smaller in size, and more efficient Cryptographic keys to provide authentication scheme to system [15].

ECC authentication scheme is well suitable for wireless communications medium. ECC point of development operation is found to be computationally much more efficient than RSA Algorithm, using fast and effective computational time. It is defined by various parameters that is small in size, highly secure and other features describes ECC. It is established on the theory of ECC.

This work considers its different advantages over various other cryptographies and focuses on its principle.

It provides very great level of security in which we have lesser key size as compared to other Cryptographic techniques.

RELATED WORKS

Definition

Around the world secure data transmission is one of the most challenging difficulties, due to its practical value in popular scope for scientific study and meteorology.

Cloud computing gives an environment in which technically it allows access to the application, via secure internet network that is shared to a set of computing resources. There are different methodologies i.e., Homomorphic encryption and Elliptic Curve. Many of the authors have oppressed the power of ECC and have developed an important implementation in several public-key cryptography tasks such as authentication, digital signature, key agreement and cryptography.

Generally, all the data which is stored in the cloud is always be in encrypted form. Whenever the authorized user requires any managed data, the cloud provider must decrypt that

managed data, and can performs computation on it and then provides the result to the user. Here comes the requirement of security as while processing that data the hacker can hack the data on cloud. In case what if the cloud service provider is not going to decrypt the data while processing? This concept of securing data from hacker is called Homomorphic Encryption.

Background

Ahmed EL-YAHYAOUI, et.al (2017) proposed a novel approach to provide security within cloud systems. This approach is known as fully homomorphic encryption since it is made by the highly symmetric, free of any noises also is a probabilistic cryptosystem. Since it is easily applicable to the big data security, several applications related to smart computations being performed on encrypted data can be applied by this proposed encryption mechanism [12]. The issue of calculations of an over-defined system is solved by providing the security through this efficient and practical approach.

Haohao Zhou, et.al, (2016) proposed a queuing system within which on the basis of stochastic process, the base can be touch by the user and several resources can be requested to be used. For enhancing the usage of system within stable state, a relationship amongst all of them the proper use and how to maintain steadiness of cloud systems is provided through this paper [7].

The effects caused by several parameters on the algorithm are also studied here. Various factors are need to be considered when scheduling is done on the real cloud such as utilization, QoS.

Peidong Sha, et.al, (2016) presented a study related to the partially homomorphic cryptosystem known as RSA. An encryption system is designed here depending upon the characteristics of RSA algorithm. Initially, depending upon the availability of prime number within the morals of public and private key created during the encryption method, the discrimination of encryption system is done initially. Further, the theorem known as Pascal's triangle, RSA algorithm model and the inducting approaches are combined within this approach for generating new cryptosystem. The fully homomorphic encryption is completely satisfied by the new cryptosystem [11].

Huangke Chen, et.al, (2015) proposed the major concern of green cloud computing in all the fields such as industry and academia. Since the cloud computing scenarios are assumed to be deterministic in nature and also pre-defined plan results, the scheduled execution will be followed [8].

Author in this paper raised this issue. For describing the uncertainty of computing scenarios, an interval number theory is also introduced by the authors. There are three proposed strategies to progress energy efficiency, improve the use of resources for the data center in the cloud. The PRS is compared with the four different typical basic planning algorithms based on the experiments performed. On the basis of the experiments carried out, it is concluded that the given proposed method of PRS is superior with the existing algorithms, since it improves the given presentation of the statistical nuclei.

Doulamis ND, et.al,(2014) proposed that in distributed computing surroundings, asset allocation and resource selection are essential operations with respect to the network and the cloud, as they also required resources for their work. Customer satisfaction metrics are not just the criterion for measuring the corresponding algorithms for making decisions. Most activities are performed without breaking the quality of service requirements based on the performance metrics of the resources used. Because a particularly large number of properties are used to obtain the work and efficiency of its application [9].

With the help of the planned method, the concepts derived from the graph partition are grouped to minimize the temporal overlap of the tasks assigned to the given resources and also to maximize the temporal overlap between the activities assigned to multiple resources. Based on the experiments, it is concluded that the proposed method is superior to other programming algorithms.

Abdul Hameed, et.al, (2014) has proposed a key problem in the allocation of energy proficiency of resources to many virtualized ICT properties, such as servers, load disks and systems, and many others. This problem is elaborated in various research work to improve the allocation of given energy resources in the cloud computing environment to all applications that help to minimize the problem. According to the author, they have searched several articles but have not found an optimal solution to the problem mentioned above [10]. The main objective of this research is to present the main problem and the tasks related to the efficient allocation of resources. The accessible techniques presented in the literature are integrated on the basis of the energy-efficient research-based taxonomy.

PROPOSED ALGORITHM

1. Select the node for the communication
2. Enter the credentials to start communication
3. Enter the prime number of the user and server
4. Enter the public and private keys of users and server
5. The user calculate its own key $a^* = q^a \bmod$
6. Server calculate $b^* = q^b \bmod p$
7. The user compute x $x = (b^*)^a \bmod p$
8. The server compute x $x = (a^*)^b \bmod p$

if (x==x)
Secure channel established
Else
Discard request

9. Check number of login times
10. Calculate OTP

OTP= x+ Number of login times

11. If user enters correct

Give channel access
Else
Discard Request

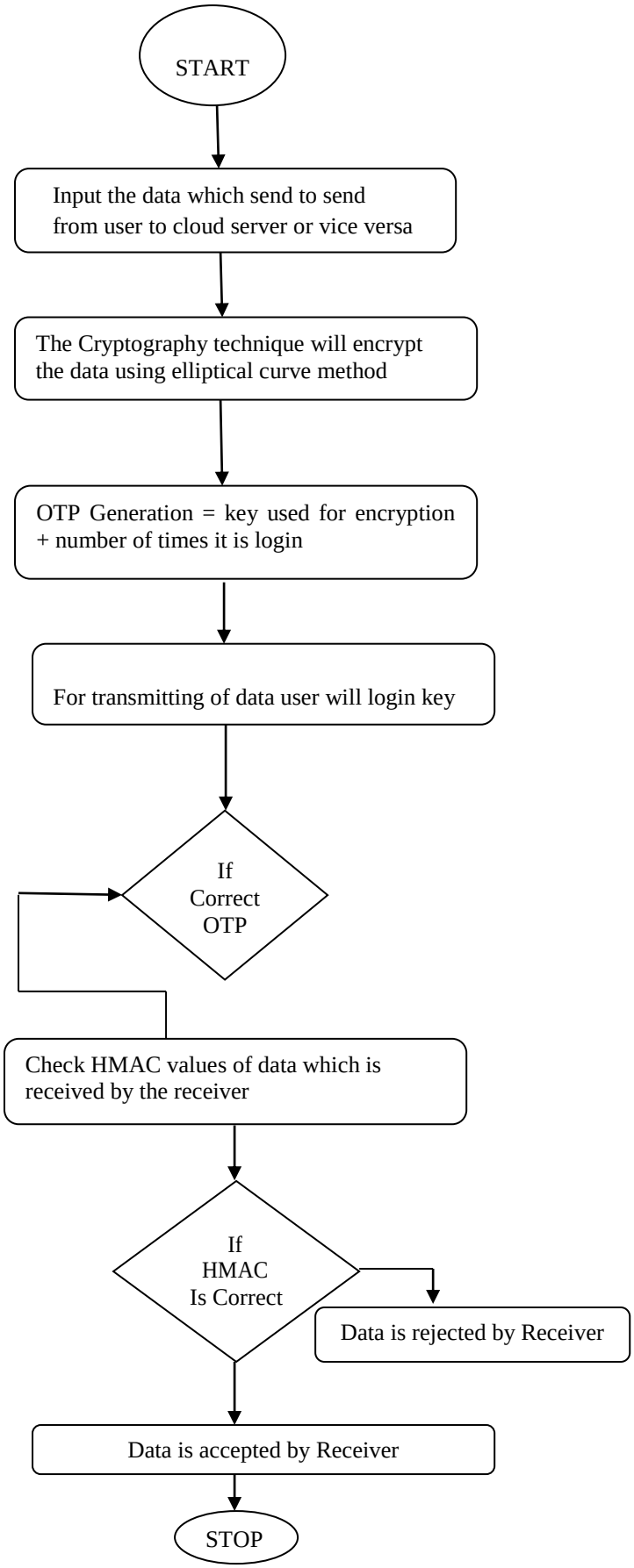

Figure 1: A Flow Chart

RESULT

The outcomes are calculated in terms of interruption, space and likelihood and the approach used in evaluation is MATLAB. The main objective of encryption is to assure data privacy and confidentiality in both storage and treatment processes[14].

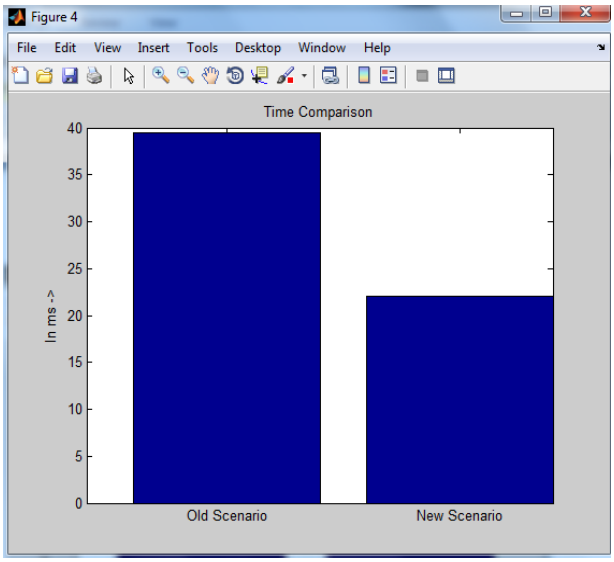

Figure 2: Comparison graph of delay

As shown in figure 2, the preceding and future method is going through the comparison which is shown in terms of delay. The exchange of numbers increases randomly when the delay in the prior art increases. In the proposed voluntary approach, the delay is reduced due to the increase in the number of messages.

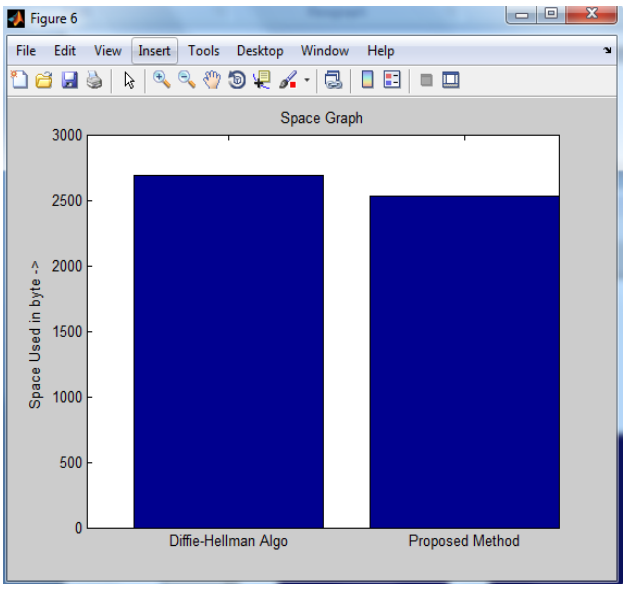

Figure 3: Comparison graph of Space

As we can show in fig. 3, the space utilization of existing Diffie-Hellman Algorithm is higher in comparison to the space utilization of proposed algorithm. Cloud Service earns keeps computing resources and data repeatedly through software [19].

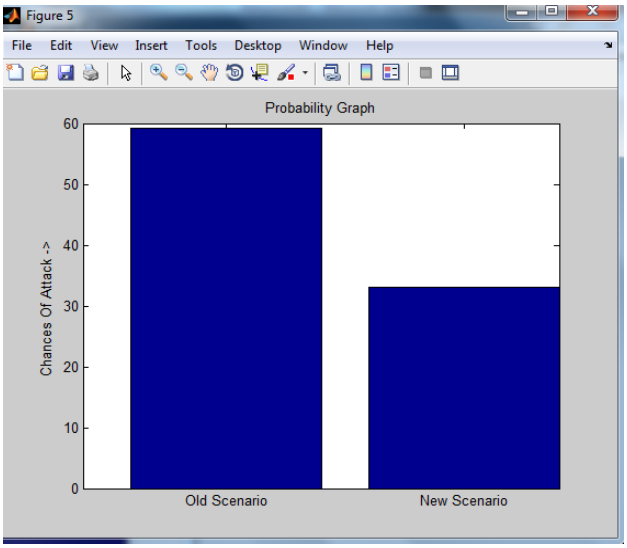

Figure 4: Comparison graph of probability

CONCLUSION

According to the given effort, we estimate that the fully homomorphic cryptography technique is much more proficient than full disk encryption. But in the general formation of the results, the main problem that must exist in fully homomorphic cryptography is due to the management of the keys and the exchange of keys that moderate the coherence of the scheme. In the cryptographic scheme used for key management and key exchange, a development is proposed which, in turn, is used for the development of the elliptic curve cryptography algorithm and HMAC generates the OTP based on the key secret generated by the elliptic curve cryptography algorithm. This session key is formed using this algorithm between the consumer and the cloud. Before communication each time a new key is generated between both. This helps to reduce the time that occurs in the management in which the exchange of keys is established and the secure channel between, for example, the user and the service provider in the cloud. Imitation shows that the planned improvement is more capable and coherent than the existing one. In the future, we will plan to extend this work for access control management using a completely homomorphic cryptographic scheme.

REFERENCES

[1] Barron, C., Yu, H., & Zhan, J., 2013 ―Cloud Computing Security Case Studies and Research Proceedings of the World Congress on Engineering 2013 Vol II.

[2] Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45.

[3] Deyan Chen, Hong Zhao, 2012‖ Data Security and Privacy Protection Issues in Cloud Computing‖ International Conference on Computer Science and Electronics Engineering, pp 647-651.

[4] Young-Gi Min, Hyo-Jin Shin and Young-Hwan Bang, 2012 ―Cloud Computing Security Issues and Access Control Solutions‖ Journal of Security Engineering, pp 135-14.

[5] Simarjeet Kaur, 2012 ― Cryptography and Encryption In Cloud Computing‖ VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249., pp 242-249.

[6] Dian-Yuan Han, Feng-qing Zhang, 2012 ―Applying Agents to the Data Security in Cloud Computing‖ International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128.

[7] Haohao Zhou, Su Deng, Hongbin Huang, 2016. ―Stability property of clouds and cooperative scheduling policies on multiple types of resources in cloud computing‖ , J Supercomput volume 72, issue 46, pp- 2417–2436.

[8] Huangke Chen, Xiaomin Zhu, Hui Guo, Jianghan Zhu, Xiao Qin, Jianhong Wu, 2015. ―Towards Energy-Efficient Scheduling for Real- Time Tasks under Uncertain Cloud Computing Environment‖ , J Syst Softw volume 99, issue 58, pp- 20–35.

[9] Doulamis ND, Kokkinos P, Varvarigos E, 2014. ―Resource selection for tasks with time requirements ing spectral clustering‖ , IEEE Trans Comput Vol. us63, No. 2, pp. 461–474.

[10] Abdul Hameed, Alireza Khoshkbarforoushha, Rajiv Ranjan, Prem Prakash Jayaraman, Joanna Kolodziej, Pavan Balaji, SheraliZeadally, Qutaibah Marwan Malluhi, Nikos Tziritas, Abhinav Vishnu, Samee U. Khan, Albert Zomaya, 2014. ―A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems‖ , Computing, volume 5, issue 6, pp- 1–24.

[11] Peidong Sha, Zhixiang Zhu, ―The Modification Of Rsa Algorithm To Adapt Fully Homomorphic Encryption Algorithm In Cloud Computing‖ , Proceedings of CCIS, 2016.

[12] Ahmed EL-YAHYAOUI, Mohamed Dafir ECH-CHRIF EL KETTANI, A verifiable fully homomorphic encryption scheme to secure big data in cloud computing‖ , 2017, IEEE.

[13] El-Yahyaoui, Ahmed, and Mohamed Dafir Ech-Chrif El Kettani. "Data privacy in cloud computing." 2018 4th International Conference on Computer and Technology Applications (ICCTA). IEEE, 2018.

[14] Alkharji, Majedah, Hang Liu, and Washington CUA. "Homomorphic Encryption Algorithms and Schemes for Secure Computations in the

Cloud." Proceedings of 2016 International Conference on Secure Computing and Technology. 2016.

[15] Rastogi, Garima, and Rama Sushil. "Cloud Computing Security and Homomorphic Encryption." IUP Journal of Computer Sciences 9.3 (2015).

[16] Bensitel, Yasmina, and Rahal Romadi. "SECURE DATA IN CLOUD COMPUTING USING HOMOMORPHIC ENCRYPTION." Journal of Theoretical & Applied Information Technology 82.2 (2015).

[17] Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh. "Implementation of text encryption using elliptic curve cryptography." Procedia Computer Science 54 (2015): 73-82.

[18] Patel, Namrata, Parita Oza, and Smita Agrawal. "Homomorphic Cryptography and Its Applications in Various Domains." International Conference on Innovative Computing and Communications. Springer, Singapore, 2019.

[19] Mohanaprakash, T. A., et al. "A Study of Securing Cloud Data Using Encryption Algorithms." (2018).

[20] Sakharkar, Sneha, et al. "A Research Homomorphic Encryption Scheme to Secure Data Mining in Cloud Computing for Banking System."(2018).