CLOUD COMPUTING SECURITY FOR PUBLIC CLOUD USING CIPHERS AND QUEUING PETRI NETS

Shreyashi Deb, Dr V.B. Kirubanand

Abstract— Cloud computing is the most used word in the domain of Information Technology, which is making colossal differentiations in the IT business. Nowadays, a massive proportion of data is being made, and the masters are discovering better approaches for managing this data. In a general sense, the word cloud implies a virtual database that stores immense data from various clients. There are three sorts of cloud public, private and hybrid. A public cloud is fundamental for general customers where customers can use cloud benefits free or by paying. Private cloud is for explicit associations, and hybrid one is in a broad sense a mix of both. Cloud offers diverse kind of administrations, for instance, IAAS, PAAS, SAAS where administrations like a data modification, data hacking and therefore, the integrity and privacy of the data are being undermined. Here in our work our motive is to verify the information that will be taken care of in the public cloud by using the multi-stage encryption. The estimation that we have proposed is a mix of Rail Fence cipher and Play Fair cipher.

Index Terms— Cryptography Algorithm, Cloud Computing, Queuing Petri nets, Security Issues.

1 INTRODUCTION
1.1 CLOUD COMPUTING
Cloud Computing is a platform with so many IT-related services. Cloud platform offers services like as a platform to deploy any applications, offers solutions, offers massive storage area and also helps in hosting purpose too. Cloud Computing is a versatile platform where based on the needs, services can be acquired by paying a minimum amount or at free of cost. It offers various types of clouds like public, private and hybrid cloud-based on security purpose and also based on the needs of each user. The underlying cloud architecture consists of three parts: Essential Characteristics, Service models, Deployment models. The essential characteristics include Broad Network Access, Rapid Elasticity, Measured Service, On-Demand Self Service, and Resource Pooling.

Service Models includes Platform as a service (PAAS), Software as a service (SAAS), and Infrastructure as a service (IAAS). Deployment model includes several varieties of clouds: Private cloud, Public cloud, Hybrid cloud and Community cloud. The IAAS offers the Platform, storage, network and other fundamental resources. Here the consumer can deploy an application and have total control over the operating system, storage and deployed application. The PAAS offers a platform for deployment. Here the consumer can control only the deployed application. The SAAS offers to use any application running on the cloud platform. In the public cloud, we can see that data from various users can be stored. The users here are the general people. The general users or consumers can pay a minimum amount to use cloud services.

The hybrid cloud is made up of public and private clouds. Highly changeable workloads require this. The community cloud is basically for a particular community-based organization. Thus, in this way, data can be stored, used, and how applications can be run in a cloud network. Simultaneously all this data that are being saved is not at all safe and secure because there is no particular security mechanism for this. The cloud data is very much vulnerable to Data breaching, Data loss, Data modifications, DOS attacks, Malware attacks, Data stealing, Hacked API, Broken credentials and authentication, APT parasite, Shared technologies and shared dangers. So, to secure the data from hacking, we need to encrypt it by using encryption algorithms.

1.2 CRYPTOGRAPHY
Cryptography is the technique for encoding information to such an extent that the outsider can't get in contact with accurate information. Cryptography is the technique for changing the real information into nonsense or unreadable form. Cryptography is utilized when a sender sends a few information to the receiver. When the data is powerless against attack and change from an outsider, then it encodes the data into ciphertext form, and this information is being sent to the receiver. This cipher structure is again being decoded into the original structure at the recipient's side. There are two techniques for cryptography, and those are Symmetric and Asymmetric strategies. The symmetric method is only where a unique key is being utilized for encoding the original information to cipher structure before sending the data over the system. This key is known as a public key. This strategy likewise has a few downsides because the single key can be hacked and, in this manner, information can be changed. So Asymmetric approach came into the picture. Here rather than a unique key, both public key and private key are utilized. The sender's data is enciphered by making use of the public key and must be deciphered utilizing the private key of the recipient. This strategy for encryption is doubly ensured and is one of the most secure encryption strategies. In this manner, by utilizing these techniques, the information in the cloud can
be encrypted as well decrypted. This paper proposes another hybrid encryption procedure. This multi-stage encryption comprises of two stages, and these are 1. Rail-fence cipher and 2. Play-fair cipher, techniques. Mostly, the original information that will be transferred into the cloud will be first experiencing the Rail-fence encryption. Afterwards, the second stage encryption will be finished by Play-fair cipher. This last information will be transferred into the cloud. In the event of decryption, in the first stage, the Play-fair cipher will be decoded, and afterwards, Rail-fence cipher will be decrypted. At long last, the original information will be recovered. The rest of the paper incorporates portrayal about related research works done, depiction about the algorithms to be utilized, depiction about the proposed structure alongside results and example, lastly end with future extension and constraints are additionally depicted.

1.3 QUEUEING PETRI NETS
It is Queueing Petri Nets (QPNs), which joins Queueing Networks and Petri Nets, targeting wiping out these inconveniences. The new form likewise shows the demonstrating of coordinated advances and 'timeless' queues for depicting unadulterated booking systems. Queueing Petri Nets are a superset of Queueing Networks and Generalized Stochastic Petri Nets. In QPNs timing, perspectives are added to the spots of a (Colored) GSPN by coordinating queues into places. Such a timed queueing place comprises of two segments, the queue and a vault for tokens having finished their administration at this queue. The conduct of the net is as per the following. Tokens, when terminated onto a coordinated queueing place by any of its input transitions, are embedded into the queue as per the queue’s booking technique (indicated by its AC-function). Tokens in a queue are not accessible for the QPN transitions. After the culmination of its administration, a token is promptly moved to the store. Tokens on this ‘place’ are available for all the output transitions of the planned queueing place. Moreover, pure scheduling aspects can be depicted by prompt queueing places. Rather than coordinated queueing places tokens on those spots can be seen as being 'served' right away. Planning for such places has priority over scheduling/service in coordinated queueing spots and terminating of planned transitions. Empowered coordinated progress will fire after a specific exponentially circulated deferral as indicated by a race approach. Empowered prompt changes will fire as indicated by relative terminating frequencies. The firings of quick advances have needed over those of coordinated advances.

2 RELATED WORK
The idea behind my work has been inspired by few previous works where specific methods of securing data have been stated, and some works dealt with the detailed study of the encryption methods and security threats in the cloud. The following are the review of some related works:
Falko Bause [1] shows in Petri Nets A Formalism for the Combined Qualitative and Quantitative Analysis of Systems-Elaborates a new version of Queueing Petri Nets (QPNs), which is a combination of Queueing Networks and Petri Nets, aiming at eliminating these disadvantages. The latest version also exhibits the modelling of timed transitions and ‘timeless’ queues for describing simple scheduling mechanisms. Yogita Borse and Anushka Chawathe [2] show in A Survey on Access Control in Cloud Computing that cloud clients are unaware of their data, such as its storage and retrieval. Also, the cloud client has trust issues as far as data is concerned. The service provider of cloud thus brings an access control mechanism to ensure the secure handling of data. Access control is a security component that can be utilized to control who or what can view or use assets in a computing environment. W. Henderson, D. Lucictand and P. G. Taylor [3] show in A Net Level Performance Analysis Of Stochastic Petri Nets that by allowing the firing times of transitions to be non-negative random variables a Petri net can be modified to a Stochastic Petri Net (SPN). The purpose of an SPN model is to enable us to discover additional information, such as performance measures, about the protocol under consideration. Samuel Kounve, Simon Spinner and Philipp Meier [4] show in Introduction To Queueing Petri Nets: Modeling Formalism, Tool Support And Case Studies that the main idea behind the QPN formalism was to add queueing and timing viewpoints to the places of Colored Generalized Stochastic Petri Nets. It is finished by permitting queues (service stations) to be incorporated into places of CGSPNs. Deepanshi Nanda and Sonia Sharma [5] show in Security in Cloud Computing using Cryptographic Techniques that the security issues such as confidentiality and integrity of data in data security are essential in the cloud. This paper is mainly focused on security issues in today's cloud and several cryptographic techniques that can be used to improve safety in the cloud environment.

3 EXISTING METHODOLOGIES
There are several algorithms for encryption purpose, and these are being used in cloud data encryption. Listed below are some of the algorithms that are being used in our work:

a. Rail-fence cipher
b. Play-fair cipher

a. Rail-fence cipher: This is the oldest encryption technique. It is one of the symmetric encryption algorithms. The plain textual data will be encrypted using the key. The key here is the no. of rails and by following this no. The plain text is written vertically but in a zigzag pattern. The ciphertext can be understood if we read the message along the rails that is horizontal. The following example will describe the working of this:
E.g. For encryption,
Plain-text = Megha, Key or no. of rails = 2
Therefore
m........g........a..............
......e........h........
Cipher-text = mgaeh

For decryption,
......m........g........a..............
......e........h........
Plain-text = megha

b. Play-fair cipher: This is also one of the symmetric encryption techniques. Here, the plain text is being encrypted with the help of a key. This key also a random word. This key is then used to generate the 5*5 matrix. The plain text has to be grouped. There are certain rules for encryption and the rules are:

i. If both the elements of the pair are in the same row, then they will be assigned with the next immediate element in that row in the matrix.

ii. If both the elements of the pair are in the same column, then they will be assigned with the below immediate element of that
column in the matrix.

iii. If both the elements of the pair are in different rows or columns, then they will be assigned with the element in the corner of that same row or same column in the matrix.

There are specific rules for decryption and the rules are:

i. If both the elements of the pair are in the same row, then they will be assigned with the previously located part of that row in the matrix.

ii. If both the elements of the pair are in same column then they will be assigned with the above located element of that column in the matrix.

iii. If both the elements of the pair are in different rows or columns, then they will be assigned with the element in the corner of that same row or same column in the matrix.

The following example will explain the working of this:

E.g. For encryption,
Plain text = ANITHA = AN IT HA (Grouped)
Key = Playfair

P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

Cipher-text is AN = PQ, IT = DN and HA = QB

Therefore, PQDNQB

For decryption,
Cipher-text = PQDNQB

= PQ DN QB (Grouped)
Key = Playfair

P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

Plain-text is PQ = AN

DN = IT

QB = HA

Therefore, ANITHA

4.2 STEPS FOR DECRYPTION

i. The client will go back to their account that they have opened under their preferred cloud service provider

ii. The client will select the encrypted data that is to be downloaded from the public cloud server

iii. The cloud server will be performing the steps for decryption of the encrypted data

a. The server will be performing 1st stage decryption for the Play-fair cipher

b. Then the 1st stage decrypted data is obtained

c. Then the 2nd stage decryption process is being done for the Rail-fence cipher

d. Finally, the data is decrypted, and the original text is achieved

iv. Thus, the encrypted data will be decrypted finally, and the client will be able to download the file.
1st stage cipher text = RNIA
2nd stage encryption using Play-fair encryption:
Previous 1st stage ciphertext will act the plain text for this method = RNIA = RN IA (Grouped)
Key = Playfair
Therefore,
P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

2nd stage or final ciphertext = RN will be IO
IA will be BP
Therefore, the final ciphertext = IOBP

For Decryption:
1st stage decryption using Play-fair encryption:
Final cipher text = IOBP = IO BP (Grouped)
Key = Playfair
Therefore,
P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

2nd stage or final ciphertext = IO will be RN
BP will be IA
Therefore, the 1st stage decrypted text = RNIA
2nd stage decryption using Rail-fence encryption:
Pre obtained 1st stage plain text is the ciphertext for this method = RNIA
No. of rails = 2
Therefore,
...R........I........
........N........A........
Final decrypted original text = RINA

5 CONCLUSION AND FUTURE WORK
Cloud Computing is a vast application for storing data, running any application, or accessing any application. Simultaneously, data security is also at stake due to the vulnerability of the data towards the attackers. This is because the entire cloud structure is based on the internet, and there is no proper security regarding the data in the cloud. This is mostly in public cloud and general users nowadays mostly use the cloud, and their entire data is saved there, but this public cloud is not at all safe. Thus, our research work is based on encrypting the data that is to be reserved in the public cloud such that the data becomes less vulnerable towards attackers. To safeguard this data, we have implemented a multi-phased encryption model that is performing the encryption efficiently without any error. Our future works aim at the implementation of this model fully in real-time and modify it more based on real-time demands.

6 ACKNOWLEDGEMENT
I wish to thank my family for supporting me in this endeavor and also my guide, Mr. Kirubanand V.B. for his valuable suggestions and inputs without which it would have been difficult to proceed further.

7 REFERENCES
[1] Queueing Petri Nets A Formalism for the Combined Qualitative and Quantitative Analysis of Systems Falko Bause Informatik IV, Universitat Dortmund, 44221 Dortmund, Germany
[4] Introduction to Queueing Petri Nets: Modeling Formalism, Tool Support and Case Studies Samuel Kounev Karlsruhe Institute of Technology Am Fasanengarten 5 Karlsruhe, Germany kounev@kit.edu Simo n Spinner FZI Research Center for Information Technology Haid-und-Neu-Str. 10-14 Karlsruhe, Germany sinner@fzi.de Philipp Meier Karlsruhe Institute of Technology Am Fasanengarten 5 Karlsruhe, Germany mail@philippmeier.com
[5] Security in Cloud Computing using Cryptographic Techniques 1 Deepanshi Nanda, 2 Sonia Sharma 1, 2 Dept. of CSE, Guru Nanak Dev University, Amritsar, Punjab, India