# Secure Key Exchange for Cloud Environment Using Cellular Automata with Triple-DES and Error-Detection

Govinda.K[1], Sathiyamoorthy.E [*2], Surbhit Agarwal[3]
[#] SCSE,VIT University
Vellore,India
[1] kgovinda@vit.ac.in
[3] sax@aksamity.com
[*] SITE,VIT University
Vellore,India
[2] esathiyamoorthy@vit.ac.in

***Abstract*—The information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it critical for you to understand the security measures that your cloud provider has in place, and it is equally important to take personal precautions to secure your data. In the world of cloud computing, security is the big issue because of open system architecture. The data transferred through cloud should be secure and there is a possible to attack the data in middle. In this paper, we deal with key exchange between cloud user's using cellular automata. It is hard to trace the key by man-in-the-middle-attack because of Strong encryption algorithm (Triple-DES) with CA (Cellular Automata) Rules. Besides CRC (Cyclic Redundancy Check) is done to ensure data integrity at the user's end.**

Keyword- **Key Exchange, Triple-DES, Cellular Automata, Cloud, CRC**

## I. Introduction

Cloud computing become a popular taxonomy in the Internet world. Nowadays all the services are being provided by cloud computing. The term 'Cloud' means collection of all data placed somewhere in the server. In cloud computing, everything is by means of service. There are Three main services in cloud computing which can be seen in the cloud architecture namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). There services are the basic service provided to the cloud consumer. In this environment, consumers are billed as per their usage. Generally it is called as "Pay-as-you-go". In other words, If you have used for an hour, you are about to pay for the used hour. It is based upon the services. Each service has its own cost. Currently, there are various cloud computing service provider such Amazon.com, Google App Engine (GAE), IBM and so on. Most of the professional companies are being shifted to cloud computing architecture environment because of Space, Speed and Resource availability. Only you need to pay the rental cost for the service you have been consumed.

In addition to that, cloud computing provides you various advantages such as Virtualization, High-end systems, Scalability. Virtualization is used to run multiple Operating System (OS) in a single machine. Each and every service is pointed to business oriented view[5]. Cloud layer architecture consists of four layers. Infrastructure as a Service (Iaas), Platform as a Service (Paas), Software as a Service (Saas) and Business Process as a Service as shown in Fig1. In case of cloud computing the security is a major issue. Key is the vital part of the system, If a key is revealed to the stranger then the system would be in the insecure scenario. So overcome these kinds of problem we focus to secure the key while transmission takes place between a cloud service provider and a cloud consumer.

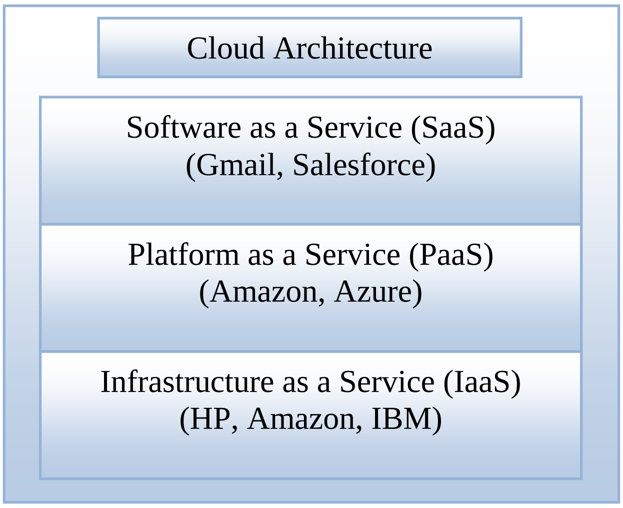

Cloud Architecture
Software as a Service (SaaS)
(Gmail, Salesforce)
Platform as a Service (PaaS)
(Amazon, Azure)
Infrastructure as a Service (IaaS)
(HP, Amazon, IBM)

Fig 1.Layered Architecture of Cloud Computing

Basically, error is happened in internet based transmission so it could be detected using the traditional method CRC (Cyclic Redundancy Check).

The paper is organized as follows Chaper1 describes the introduction to service models, Cellular automata and Key generation using cellular automata rules, Chapter2 describes the literature review, Chapter3 describes the proposed method. Chapter presents results and Chapter5 describes conclusion followed by references.

## II. Cellular Automata

Cellular Automata (CA) was introduced by Ulam and John Vonn Neumann. CA is collection of lattice cells and each cell is executed parallelly. By applying the function $f$ on the state$t$ , we get $t+1$ is called as Transition state. A function $f$ is a local rule applied on the neighbouring cells based on the radius $r$ . There are two types of CA: 1. One-dimensional Cellular Automata and 2.Two-dimensional Cellular Automata. A one-dimensional cellular automaton is also said to 'Elementary CA' because of Elementary Rules (0 to 255). Function is Boolean expression applied on the cells.

$$CA = (\pi, \alpha, d, f)$$

Where $\pi$ is a completed entire of states, $\alpha$ is the cellular vicinity, $d$ is the size of CA, $f$ and is the function (Local Rule. Eg., Rule 30, Rule 90 where Rule 30 is more random used for cryptography)[2]. Each rule is defined by a Boolean expression[7].

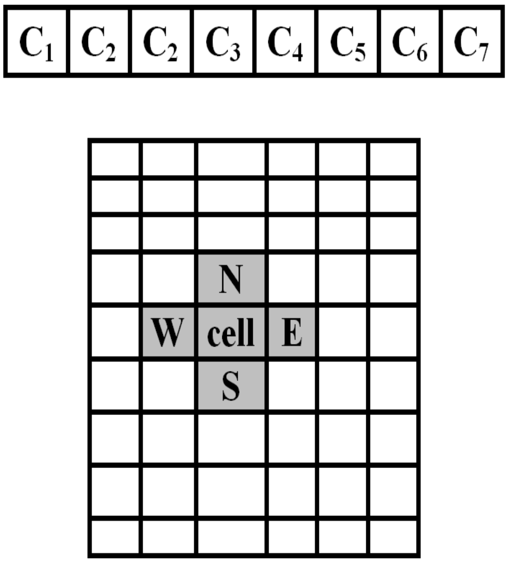


Figure 2. 1-D and 2-D Cellular Automata

1-D cellular automata follows periodic boundary for the transition state where as 2-D cellular automata used four directions: North, East, West and South[5].

### A. *Key Generation*

Key generation is done with sender and receiver. Basically, key generation algorithm uses cellular automata and it will be explained as Alice and Bob. Alice acts as a sender and generates the key with CA rule 30 which is more random and Bob acts as a Receiver. A key will be generated by Alice  and uses 3DES to encrypt the data as well as he computes the CRC for the data and it is sent to Bob. Bob also uses the same concept generates the key to decrypt and checks for CRC error. There are types of keys: 1. Symmetric Key (Encrypting and Decrypting with same key called Public key) , 2. Asymmetric Key (A shared Public key is generates a Private Key which is used for encryption/decryption).

## III. Related Work

Presently, Key Exchange Protocols are being used to exchange the keys with a digital signature. Most of the digital signature vendors use RSA as a key exchange algorithm. DHDSA (Diffie-Hellman Digital Signature Algorithm) is a standard algorithm used with various security algorithms such as 3DES (Triple-Data Encryption Standard, RSA (Rivest, Shamir and Adleman), ECC (Elliptic Curve Cryptography)[4].

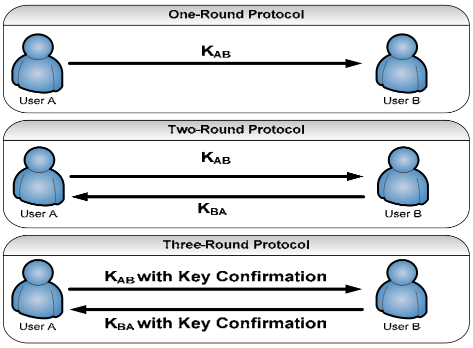


Fig 3. One-Round, Two-Round and Three-Round Protocol

In the Integrated DHDSA, the proposed protocol is given for single, two and three rounds. Each round uses modulus, addition and concatenation operations. Each round protocol is used for different purposes. For Instance, One-round protocol could be used for Email application. Two-round protocol could be used for two-way secured communication such as Chat application. In addition to two-rounded protocol, third one has a key confirmation for every communication. It supports for Key exchange applications. The Figure 3 represents the different round protocols used to exchange the key between the sender and the receiver [1][6][7].

| S.No. | Method | Example |
|---|---|---|
| 1 | Elliptic curve Diffie–Hellman (ECDH) with RSA | Gmail.com, Android Market |
| 2 | RSA | vit.ac.in |
| 3 | DHE_RSA | cPanel |
| 4 | PSK (Pre-shared Key) | VPN Mobile Networks |

Table 1. Table Content current Key exchange methods with an example

The above table shows the present key-exchange techniques. Most of the key exchange uses RSA method because of the prime number logic. RSA reveals that Prime number is most powerful mathematical concept used in cryptography. Nowadays, the key length is increased to the extend (i.e., we can see the key size 4096 bit).

## IV. Methodology

This methodology is new model rather generating the key using existing method. Cellular Automata (CA) is the strengthen method to generate strong keys. In CA, key could be generated using Local Rule and also bit length is variable. In other words, any key bit size length could be generated using CA. Triple-DES Algorithm contains several levels and rounds. For each round, a round key is used. In the case of Encryption, three processes are done (Encrypt, Decrypt, and Encrypt). For this encryption process three Private keys are used which are generated by using CA the Public key. In the case of Decryption, three processes are done (Decrypt, Encrypt, and Decrypt). For this decryption process three Private keys are used which are generated by using CA the Public key. The encrypted data is sent over the network and the data is decrypted at the receiver's end.

CRC (Cyclic Redundancy Check) is used to check the error-detection. It is generally checked at the receiver side. A long Integer CRC value is obtained for the original data and it is padded with the encrypted message. The stream is sent over the network. At the receiver side, the encrypted message is decrypted and the CRC value decrypted message is obtained. If the CRC value of decrypted message and given CRC value is same then the data is error-free. We used in-built CRC java packages for the error detection

### *A. Mathematical Model*

The methodology could be give mathematically as follows. Generally, a security algorithm has two processes: 1. Encryption, 2. Decryption. For the both process we need a key (Public Key or Private Key depend upon the process method).

Let $PUB_K$ be the Public Key shared by both sender and receiver which is generated by the Random Number R

***Sender***

Let CA be the Cellular Automata, which generated three Private Keys applying the Local Rule (Eg., 30 or 90) on the $PUB_K$.

The three Private Keys are: $PRI_{K1}$, $PRI_{K2}$, and $PRI_{K3}$.

Let $P_T$ Plain text, by applying the Encryption process and the final outcome would be the Cipher Text $C_{T.}$

***Encryption Process***

$$C_{T1} = E_{PRI_{K_1}}(P_T)$$

$$C_{T2} = D_{PRI_{K_2}}(C_{T1})$$

$$C_T = E_{PRI_{K_3}}(CT_2)$$

***Receiver***

Using the same Public Key $PUB_K$, the decryption process is done as follows:

Let $C_T$ be the Cipher Text, to perform deciphering we need three Private keys which could be generated using Cellular Automata (CA).

The three Private Keys are: $PRI_{K1}$, $PRI_{K2}$, and $PRI_{K3}$.

***Decryption Process***

$$P_{T1} = D_{PRI_{K_3}}(C_T)$$

$$P_{T2} = E_{PRI_{K_2}}(P_{T1})$$

$$P_T = D_{PRI_{K_3}}(P_{T2})$$

Keys are generated using CA Rules. It has a specific window size and initial condition. Based on the initial condition values the randomness is depended. In addition that, java inbuilt CRC package is used for generating CRC value and check over at receiver end.

## V. IMPLEMENTATION

The proposed model is implemented in Java TCP Socket Programming. Besides CRC values is checked in the receiver's side. Figure 2 represents the layered architecture of implemented design. The proposed methodology is implemented in Java using Java Socket Programming. We are considering the cloud environment; sender has the key to share with the receiver. The sharing key is encrypted using Triple-DES with CA and the corresponding CRC value is obtained. Which is padded as stream, the stream consists of encrypted data, CRC value and Public Key. This stream is sent over the network. While the receiver check the CRC value and decrypt the cipher to obtain the original data**.**

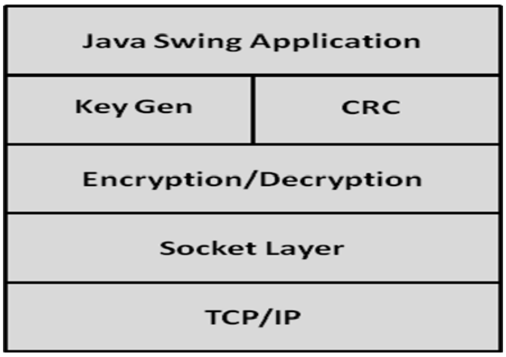
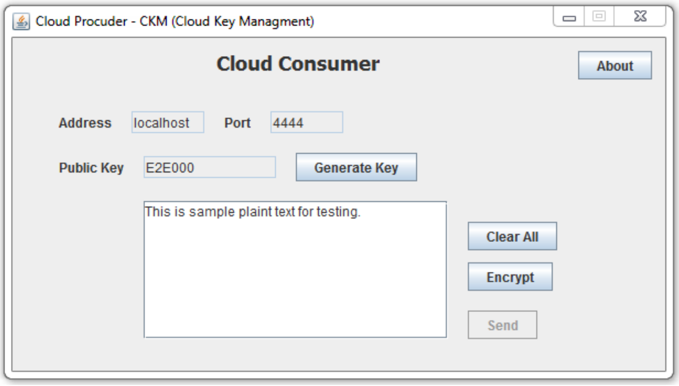


Fig 4. Layered Architecture of  Secure Key-exchnage model

## VI. Results

The Fig5 shown the input screen where user is generating the key using CA rule and encrypts using Triple DES.


Cloud Procuder - CKM (Cloud Key Managment)

Cloud Consumer

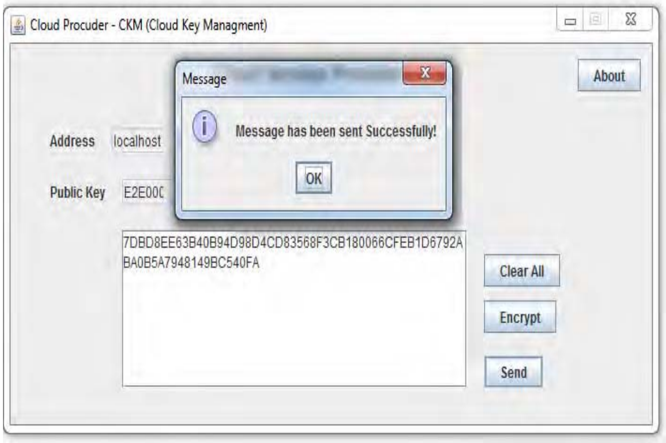
Address localhost Port 4444

Public Key E2E000

This is sample plaint text for testing.

Fig 5. Shows Input String with Key generation and Encryption

The Fig6 shows the data encryption  using Triple DES.


Cloud Procuder - CKM (Cloud Key Managment)

Message

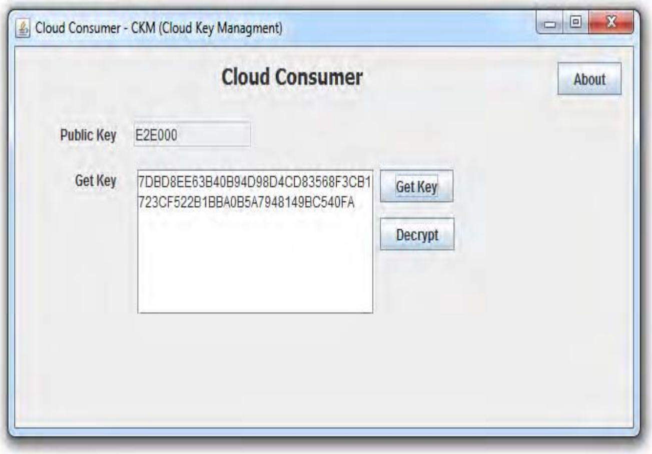
Message has been sent Successfully!

Address localhost

Public Key E2E00C

7DBD8EE63B40B94D98D4CD83568F3CB180066CFEB1D6792A
BA0B5A7948149BC540FA

Fig 6. Shows Data Encryption



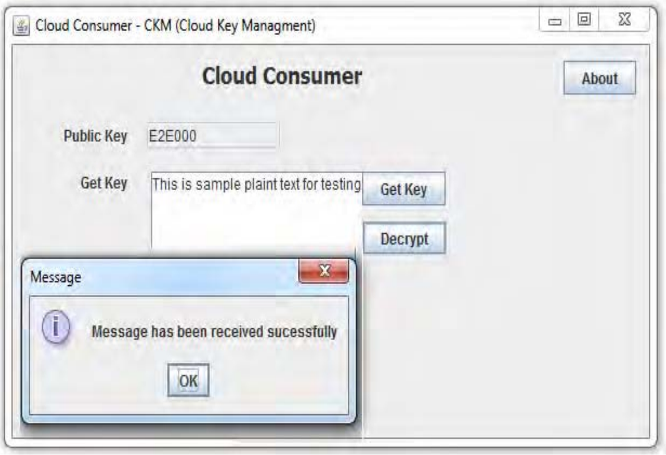
Cloud Consumer - CKM (Cloud Key Managment)

Cloud Consumer

Public Key: E2E000

Get Key: 7DBD8EE63B40B94D98D4CD83568F3CB1 723CF522B1BBA0B5A7948149BC540FA

Fig 7. Shows the Key generated using CA



Cloud Consumer - CKM (Cloud Key Managment)

Cloud Consumer

Public Key: E2E000

Get Key: This is sample plaint text for testing

Message

Message has been received sucessfully

Fig 7. Decryption using CA

## VII. CONCLUSION

Nowadays security in the cloud environment is the open issue. Even though we have strengthened the key size and powerful security algorithms, it is hard to communicate in the case of public/private cloud. Presently, all the data communications are migrating to cloud based computing. In that case, a private/public cloud can generate the key in a secure manner using this methodology. In addition to that, the system checks the error-detection in the receiver's end.In future, this methodology could be enhanced with different algorithms such AES, Blowfish and so on. The key size could be extended to higher size using CA (Cellular Automata) as well as the data could be compressed using CA and sent over the network. However, the same ideology could be implemented as web-service so that it could be used in different platform. Rather than using existing security algorithm some of the CA rules are inheritably random, this could be used for encryption and decryption of data in a light-weight manner.

## REFERENCES

[1] Benkiniouar, M. and Benmohamed, M. "Cellular automata for cryptography "'Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on', 2004, pp. 423- 424.

[2] Gage, D., Mcgarry, B., Ken, D. and Adviser, S. F. "Cellular Automata : Is Rule 30 Random?", SUSQUEHANNA UNIVERSITY.

[3] Harn, L., Mehta, M. and Hsin, W.-J. "Integrating Diffie-Hellman key exchange into the digital signature algorithm DSA)," *Communications Letters, IEEE* (8:3), 2004, pp. 198 – 200.

[4] Jing, X. and jun, Z. J. "A Brief Survey on the Security Model of Cloud Computing, "'Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010 Ninth International Symposium on', 2010, pp. 475-478.

[5] Rimal, B. P., Choi, E. and Lumb, I. "A Taxonomy and Survey of Cloud Computing Systems," *Networked Computing and Advanced Information Management, International Conference on* (0), 2009, pp. 44-51.

[6] Schiff, J. L. *Cellular Automata: A Discrete View of the World (Wiley Series in Discrete Mathematics & Optimization).*

[7] Wolfram, S. *A new kind of science*, Wolfram Media Inc., Champaign, Ilinois, US, United States, 2002.