A Novel Security Approach using Location based RSA Encryption

Amitesh Kumar Gupta, Asish Srivastava, Tinesh Kumar Goyal, Kunal Gupta

***Abstract*— In evolution of system of working of computer based on the public network such as internet, Cloud computing is a novel perspective. Cloud computing is the Concept bring into operation to persuade the Daily Computing Problems, likes of computing Resource Availability unprompted by Computer users. The passable Problem attached with Cloud Computing is the security of the cloud and the proper Implementation of Cloud over the internet. In this Research Paper, we have tried to appraise Cloud Storage Methodology and Data Security in cloud by the Geo Location based RSA encryption. We renovate the security for fact influenced in hybrid cloud environment for an organization or any other distinct place dealing with Geo-Location based RSA encryption.**

***Index Terms*— Cloud computing, Cryptography, Hybrid Cloud, RSA Algorithm, Geo Location based encryption**

I. INTRODUCTION

Presently with the expansion of technology, data and information security are required more. Certain types of data are vital like clandestine information of finance, companies, and national securities. To the contrary the mass of fact or data increased regularly, users required more energetic mode to aggregate and process that data. Nowadays a novel technique introduced for this motive, the technique known as cloud computing. This new era of technology empowers firm, organizations, and other individuals. User can accumulate any type of information and data in the cloud storage. User can retrieve data from any place, at any moment, and using any computer via public or private network. [1][2][3][4]

The greatest defiance in regarding of cloud computing is "security". The numbers of researchers are doing research on cloud computing security. Cloud user does not realize where their data accumulate or other people can access that data or information, which is stored in cloud storage. [5][6][7]

Manuscript received May 06, 2014.

Amitesh Kumar Gupta, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-7532836750.

Asish Srivastava, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-9555531144.

Tinesh Kumar Goyal, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-9417170800.

Kunal Gupta, Presently he is working as an Assistant Professor in CS&E Department, Amity University, Noida, Uttar Pradesh, India. His Research area includes Computer Networks, Network Security, and Wireless Communication & RFID. +91-8860363739.

The procedure of RSA algorithm is very embracing, which is first multiply two prime numbers and perform some more computation. After that obtain two set of two numbers one of them work as private key and another work as public key. [8][9] In our proposed solution, we attach one more security layer which gives the comfort to the user that the content never accessed by the unauthorized user. In this solution user physical location and time is main factor to provide the security to the user. Geographical location based encryption is a prescript of encryption. In this technique cipher text will be decrypted at predefined location or time. If user does not satisfy the above condition then user not able to access the information or data. If anyone tried to decrypt the cipher text the process generate an error or produce garbage data. [7]

In this paper, first we have briefly illustrated cloud computing. We have also explained some of security majors encountered in cloud computing. Then we have explained "Geo Encryption" algorithm and "RSA encryption" algorithm. Finally using "Geo-Location based RSA Encryption" we have proposed a novel model for improving the security of accessing the data in cloud computing.

In this paper, a new mechanism of key generation is introduced. Our proposed solution generate key on the basis of user physical location. This Paper is written in following structure. First discuss about basics of cloud computing in II. In section III Problem statement discussed, RSA algorithm, Geo encryption in traditional cryptography which provide security in addition. In section IV we discussed our proposed model. At last in section V discusses the conclusion of the proposed model.

II. CLOUD COMPUTING

A. Definition

Cloud computing is a terminology used to illustrate a diversity of computing concepts that embrace a number of computers interconnected via a public or private network such as the Internet. Cloud computing is also follow client and server model. Client sends a request to the server and server respond to the client. Only one important point makes it to different from traditional internet system, which is only pay that amount as much you use the cloud resource. [1][2] Concretely it is an infrastructure or platform that process codes in a supervisory and extensible model. Users work on virtual environment, resource feels to the user that it was physically present on user machine but in actual resource present on elsewhere. User have to pay to the cloud provide

that much use the resources. [4][5]

B. Deployment Model of Cloud

Cloud computing have many deployment models. Some of them are discusses here. User use one of them to perform computing task. [3][5][6]

- Private Cloud:

It is an infrastructure run for an organization. It may be managed by organization or third party. In Private cloud organization have its own Data center or infrastructure. It is an on premises deployment model.

- Public Cloud:

A cloud deployment model called Public Cloud when it is access over a network and open for any user and any time. It is an off Premises deployment model.

- Community Cloud:

A cloud Infrastructure shares with more than one organization with some set of generic concern like security, jurisdiction. Community managed by itself community or third party.

- Hybrid Cloud:

Hybrid Cloud is a combination of two or more clouds. It may be combination of public, private or community cloud.

C. Service Models of Cloud

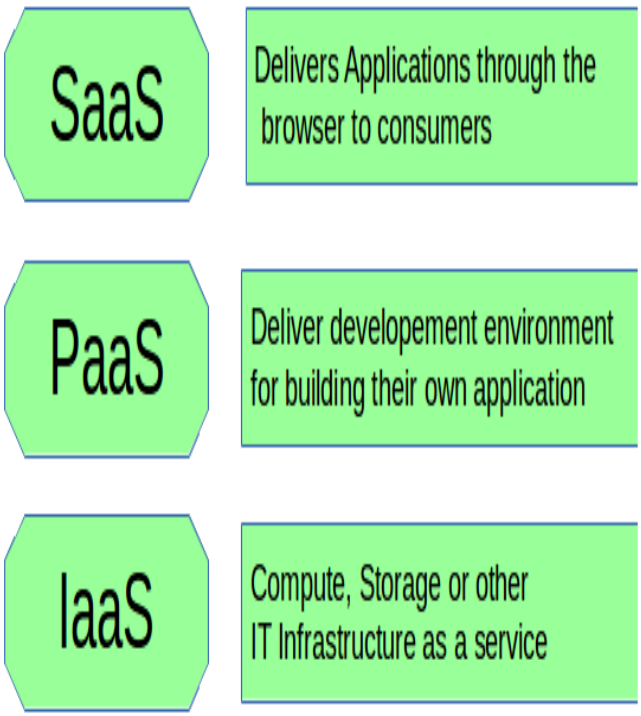

Figure 1: Cloud Service Models

III. PROBLEM STATEMENT

A. RSA Algorithm

RSA is a cryptographic algorithm which is used for encryption of plain text to cipher text and vice versa. It uses mathematical computation for generating public and private key which are used for encryption or decryption purpose. RSA is used when highly secure data transmitted over the internet. [8][9][10]

In RSA cryptosystem, user shares their public key with receiver for decrypting message. It Keep secret its private key. Private Key never shares with other user. [6][7]

RSA algorithm uses mathematical function to compute Public or Private Key. It takes two large prime numbers and multiplies and applies some additional operation on it and generates two set of keys. One key is works as public and other works as private key. [11][12]

In RSA algorithm factors which is produced after multiplying of two prime numbers. If anyone knows about the factor which is used in encryption process then the encryption can easily break.RSA encryption is strong when the factor are not disclosed. If factor are disclosed, anyone can break the encryption. [10][13]

B. RSA Scheme

In the year 1978, RSA Introduce a public key cryptographic system that is depends on the difficulty of factoring of number. RSA algorithm is difficult because no one know about the factor of number. We take an example for showing how RSA work. We take two prime number r and s. The RSA scheme is as follows:-

RSA Algorithm

To produce the keys following steps must do:

1. Choose two large prime randomly and must be secret; Prime numbers are r and s.
2. Compute the multiplication n=r *s.
3. Compute φ (n) =(r-1)*(s-1)
4. Select an integer e, 1< e< φ (n), e and n are co prime.
5. Calculate the value for d, (d*e) % φ (n) =1
6. Public key = (e, n)
7. Private Key = (d, n)

Encryption algorithm for public key

Entity E encrypts a fact F, and Entity D decrypts.

Encryption:

$$ci = f^e \pmod n$$

0≤f<n, c is cipher text

Decryption: To decrypt cipher text c to plain text. Entity D must do the following:

$$F = ci^{d} \pmod{n}$$

It decrypts the cipher text and produces the original Fact.

C. GEO-RSA CRYPTOGRAPHY

a. Location Based "Identity":-

In cryptography "identity" Components are important to us. We can use physical location of person for identity. We can also use some other information for identity such as address, phone no. and other information which helps to verify the person. We use that identity information as a key for encrypt or decrypt the information. [13][14]

b. Location Based "Access Control":-

In this approach resources allocated to user with respect to his/her physical location. User only accesses those resources which are permitted by the cloud provider to that location. Resources are encrypted with GEO-Lock. Geo-Lock is a key, which is a XOR of location identity or cloud provider RSA key. If user does not present at specific location, then user can not able to access the resource. [15]

Geo-lock is generated on the basis of receiver physical location, and Time stamp. If receiver wants to unlock the Geo-lock then user need to be present at specific location and time. The Geo-lock is a result of XOR operation with the time stamp (key_T) and location. The Geo-lock is then encrypted by RSA and transferred to the receiver.

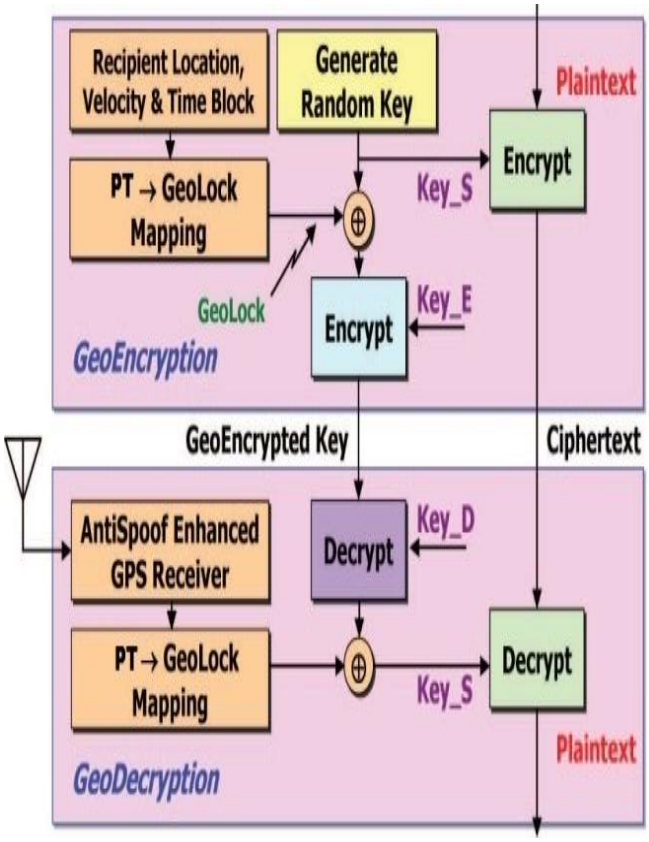

Figure 2: Geo-Location Algorithm

On the receiver (decryption) side, Geo-locks are computed using an Anti_Spoof Geo location receiver for PT input into the PT Geo-lock mapping function. If the PT values are correct, then the resultant Geo-Lock will XOR with the Geo-Locked key to provide the correct session key (Key_S).

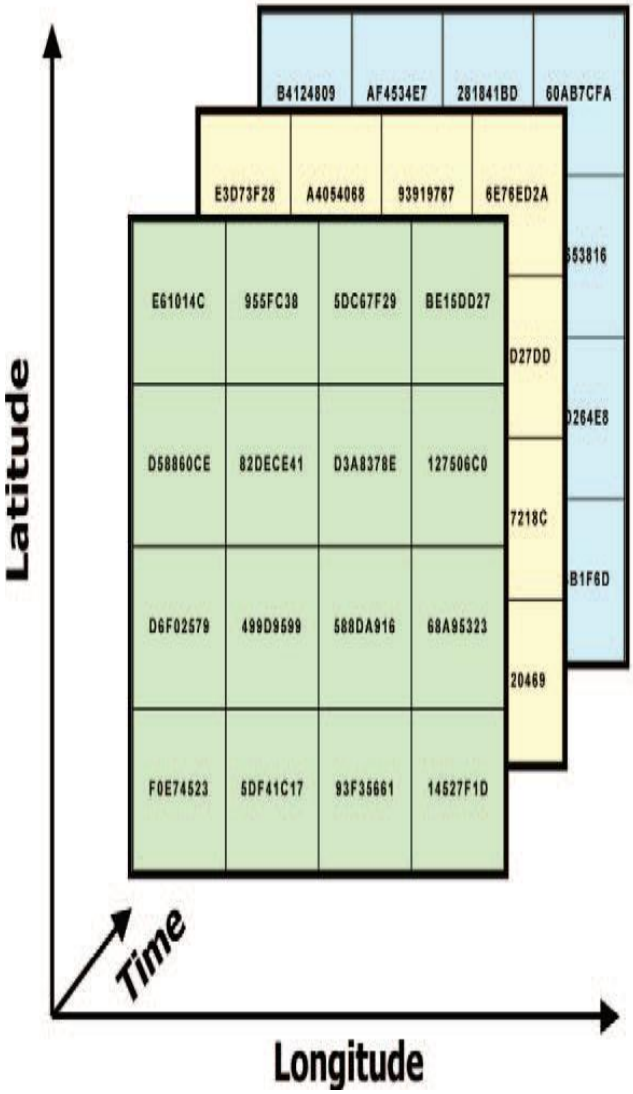

Figure 3: A PT Geo-Lock Mapping Function

In above figure shows the mapping function between Latitude tame and longitude physical constraint. Here, a grid of longitude, latitude and time values has been created, each value associated with Geo-lock. For increasing security location and time value also mapped with hash function, so one can see the encrypted value of location and time.

IV. PROPOSED MODEL

In cloud computing data security is main concern of cloud provider. Cloud is a have centralized data center which is used by many user at the same time so the data integrity and security is very important. Cloud provider applies many security mechanism for securing datacenter and resources to prevent unauthorized access. If user wants to access the resources need to verify the identity that he or she is an authorized user. In our method we apply some modification on secure key generation. We use the user physical location

or other unique information encrypted and apply RSA encryption with the session key and generate a key lock. Key lock is decrypted only user private key. This approach is more secure because user private key is known by user only. so one can access the user data or information whenever user doesn't share with other person This approach is more secure for banking sector or a company which have more crucial data. In this approach we need anti spoofed and accurate geo position system. Which is easily available in market and it is not expensive. So bank and company easily afford it. We divide the data into segment. That segment contains two fields: (1) user unique information (2) Data value. These segments placed in a table. We store data segment manually. Every segment placed in table with correspond their physical location. Physical location works as index value. With the help of index value we can easily retrieve the data segment

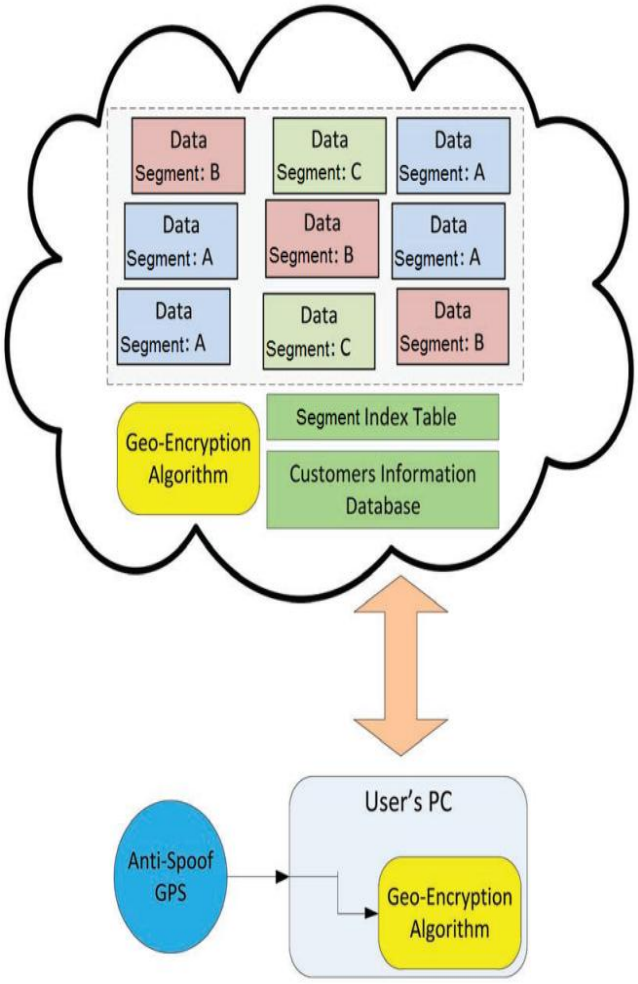

Figure 4: Proposed Model Overview

Every user have some parameter for access the data for example an Employee work in India and his longitude is 97°25' east and working duration are from 10 o'clock to 18 o'clock. Then user goes to the specific location and time duration then cloud provider give the access to the user. User need to satisfy both the parameter for access the resource. If anyone parameter mismatch then cloud service provide block the resource or terminate the user. We mentioned that this approach required anti-spoofed geo-position system. Which provide user exact location? We can apply some more restriction like that user can access the data within the room and a time frame. If any user wants to access the data from another place the valid permission required from the cloud resource provider. In our model, we provide an algorithm.

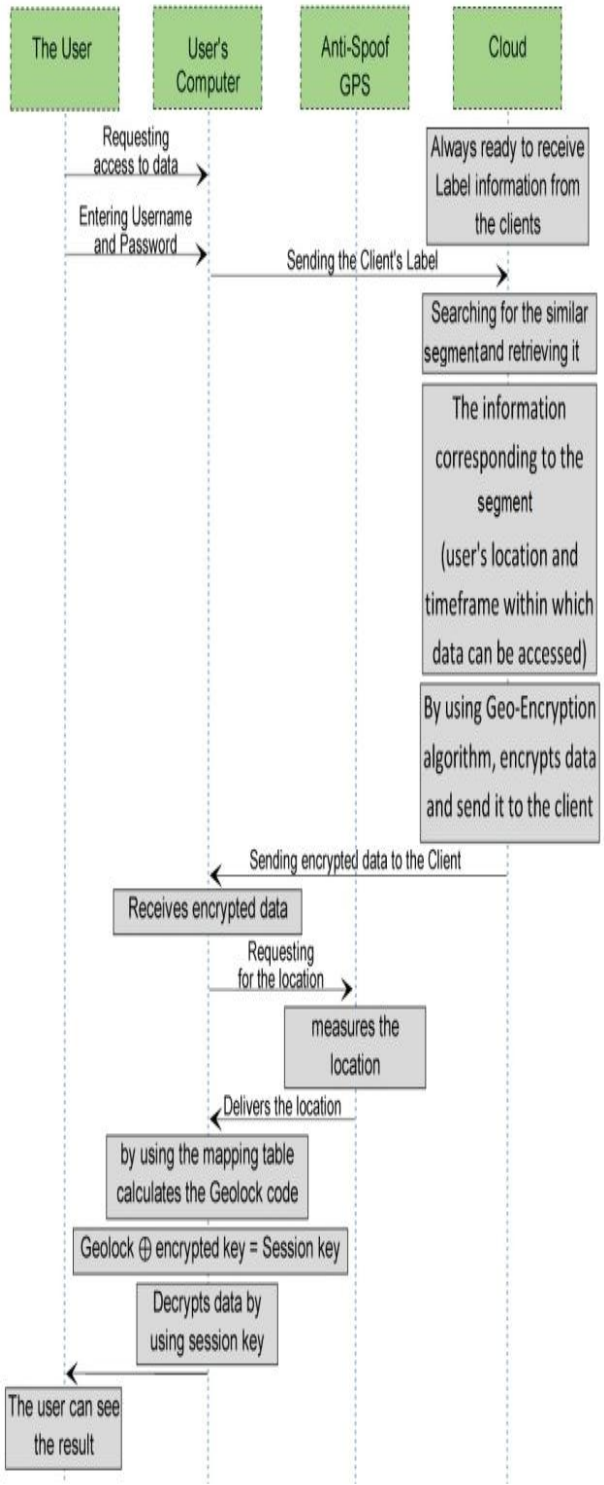

Figure 5: Proposed Model Sequence Diagram

Algorithm for Geo-RSA Encryption

1. First user sends a request segment to the cloud provider (request segment contain user location form anti-spoof GPS system and hit time stamp).
2. Cloud provider receive user request segment (segment contain user physical location and time stamp).

3. Request Segment discovered in the user information database.
4. If Information found, go to 6
5. If information not matched with database entry, discard the user request and generate appropriate message to user.
6. The knowledge about segment will be accessed (location of user and time duration in which user can access the resources).
7. User information encrypted with RSA and Geo-Encryption algorithm and send back to the user.
8. User's computer got the reply segment which contains a token for accessing the resource.
9. If toke session expires block all resource immediately.

V. CONCLUSIONS

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. The security of RSA algorithm is remains whenever the factors are not disclosed. If factor are disclosed RSA decrypt easily.

RSA algorithm security can be break if factor are disclosed. We add one layer or security which is physical position of client. If user wants to access the resource then need to be present at the physical location where the Cloud provide give the permission for accessing the resource.

One of the major challenging intension in the cloud computing is data access control. Because of the advantage of cloud computing many organization or people switch to this technology every day. Like nearly every proposed mechanism, there are defiance's as well as benefits present in this technology. Public key encryption algorithm can assure secure data access by encrypting decrypting data stored in the cloud. Therefore, it is essential to interpolate public key encryption algorithm in the data access control in hybrid cloud. In this paper, first we briefly discussed security and challenges of cloud. We also reviewed "geo encryption" and "location based encryption". Ultimately a new security stratum was compiled current security scale up using Geo-Location encryption. We can use this algorithm in various places like as organization, universities and bank's which have crucial data and have fixed physical location.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith and etc., "A view of cloud computing", Communications of the ACM, Vol. 53, No. 4, PP50-58,2010
[2] Vijay Sarathy, Purnendu Narayan and RaoMikkilineni, "Next Generation Cloud Computing Architecture: Enabling Real-Time Dynamism For Shared Distributed Physical Infrastructure," in the proceedings of 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Lariss, June 2010, pp. 48-53.
[3] Cloud computing. www.cncloudcomputing.com.
[4] G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, 1st ed. O'Reilly Media, 2009.
[5] L. Schubert, "The future of cloud computing," Euro. Commission Information Society and Media, EU, Tech. Rep.,2010.
[6] C. Lo, W. Peng, C. Chen, T. Lin, and C. Lin, "Carweb: A traffic data collection platform," in Proceedings of the 9th International Conference on Mobile Data Management. IEEE, 2008, pp. 221–222.
[7] D. Denning and P. MacDoran, "Location-based authentication: grounding cyberspace for better security," in Computer Fraud and Security, np.: Elsevier Science Ltd, 1996.
[8] L. Scott and D. Denning, "Geo-encryption: using GPS to enhance data security." GPS World, 1 Apr. 2003.
[9] Ala Al-Fuqaha, Omar Al Ibrahim, Joe Baird,"A Mobility Model for GPS-Based Encryption", IEEE GlobeCom 2005.
[10] Douglas R. Stinson "Cryptography Theory and Practice", Chapman & Hall/CRC Press, 3rd Edition,pp. 211-214, 2006
[11] Pointcheval D "New Public Key Cryptosystem Based on the Dependent-RSA Problem", in proceedings of Euorcrypt'99, LNCS 1592, Springer Verlag, pp. 239-254, 1999
[12] Rabin, M. "Digitalized signature and Public Key Functions as intractable as factorization", Technical Report, MIT/ LCS/ Tr, MIT Lab. Computer Science, Cambridge, Jan. 1979.
[13] Gurudatt Kulkarni "Cloud Security Challenges", 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA),IEEE, 2012.
[14] Logan Scott & Dorothy E. Denning, "Location Based Encryption & Its Role in Digital Cinema Distribution", Proceedings of ION GPS/GNSS 2003, pp 288-297.
[15] Gurudatt Kulkarni 1 et al, "Cloud Security Challenges", 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA),IEEE, 2012.

Amitesh Kumar Gupta Pursuing Masters of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India, Area of Interest: Computer Networks, Network Security, Cloud Computing, Data Mining and Warehousing.

Asish Srivastava Pursuing Master of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India. Area of Interest: Cloud Computing, Virtualization, Computer Networks and Network Security.

Tinesh Kumar Goyal Pursuing Master of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India, Area of Interest: Cloud Computing, Computer Networks and Software Engineering.

Kunal Gupta, Presently he is working as an Assistant Professor in CS&E Department, Amity University, Noida, Uttar Pradesh, India. His Research area includes Computer Networks, Network Security, and Wireless Communication & RFID.