A Survey - Data Privacy through Different Methods

Kamran Shaukat Dar
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Imran Javed
University of the Punjab, PUCIT, Lahore, Pakistan.

Syed Asad Ammar
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Syed Konain Abbas
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Sohail Asghar
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

M.Abu Bakar
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Usman Shaukat
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Abstract– Data protection now-a-days has become of much importance. We store our data at different places. Everyone on internet has some kind of data which he/she wants to share/store. For this purpose security is much needed. In this paper we have given survey of different data privacy methods applicable on different kinds of data like spatial data, cloud computing, temporal data etc. Survey of different methods has been covered like IPsec, PGP (Pretty Good Privacy), IBE (Identity Based Encryption), PIR (Private Information Retrieval), DES (Digital Encryption Standard) and AES (Advanced Encryption Standards).

Index Terms – Survey on data privacy, IP sec, PGP, DES, AES

1. INTRODUCTION

In this paper; we have surveyed the different methods of data protection applied on different kinds of data. Everyone on internet has some kind of data which he/she wants to share/store. For this purpose utmost security is needed, so without use of lock up techniques or methods we can't lock up our data. People have some secrets which they only want to share with specific person and they don't want that this data spreads out unwillingly. For this sharing/storing purpose, they use internet mostly. Cloud computing is one of the practices; people use to store their data over the network. Users use many other kinds of technique as well to save their data. Many methods are being used for guarding the privacy. If a person sends data over internet then he/she wants that his/her data must be safe in all respects and all irrelevant and unauthorized accesses must be overruled. We will discuss different methods of data privacy applied on different kinds of data; like IPsec, PGP (Pretty Good Privacy), DES (Digital Encryption Standard).

2. RELATED WORK

In this paper we have surveyed the different methods of data protection on different kind of data; Sub topics will be written in order as given below:

- Privacy on Cloud Computing
- Privacy Issues in Cloud Storage
- Different Methods to Solve Privacy Issues
- Spatial Data
- IPsec
- Cryptography
- PGP (Pretty Good Privacy):
- DES (Digital Encryption Standard):

- Triple Digital Encryption Standard:

2.1. Privacy on Cloud Computing

In cloud computing, a user can store his/her data on network. If there will be privacy then user can freely store his data and also communicate with other users. User will only use this if there is a guaranty that data will remain secure and will stay private. The security in Cloud is very important. It has been a great challenge to store and manage data and its usage in cloud computing environment. Cloud computing has been defined to accommodate a huge number of users. IBE, PIR or PKI symmetric standard and asymmetric cryptography methods are used for security in cloud computing but these are all not enough for cent per cent security.

2.2. Privacy Issues in Cloud Storage

When one has the data saved on cloud, when one needs to access his/her own data or one wants to send or manipulate his/her data; some issues/problems are faced; like unhallowed access, less control of user on it and when one transfers data from one point to another point on cloud such problems also arise.

3. METHODS TO SOLVE PRIVACY ISSUE

There are some methods in cloud computing which we use to solve the privacy problems. PKI, IBE and PIR; these are some procedures which are used to maintain the privacy:

3.1 PKI (Public Key Infrastructure)

PKI is used to provide privacy for cloud data .This is good for privacy in cloud computing. PKI is the set of hardware, software, and people and polices which are made to manage, distribute, access, store and revoke digital certificate. PKI bind the public key with the user identity by the CA. In every CA domain; User identity must be distinct and must be unique. The third verification party can only get access on the base of this CA.

But there are some of the problems; which arise and can't be handled with the PKI:

- Storing Private Keys in Modular and Mobile Systems.
- Certificate Authority Solitary.
- Providing Lock Up attestation and Approval.
- Managing revocation.

In order solve these problems; the following technique; based on Identity Based Cryptography is used:

3.2 IBE (Identity Based Encryption)

Public key can be generated by any party in the identity base system. PKG; which is a third party solution and it gives private key. To work with the PKG; one must make public key at first, which retains the master private keys. If user has master key then he/she can calculate public key which corresponds ID by combining MK with unique value. If user wants to get private key; firstly he/she uses the ID which connects with the PKG, which uses the master key to produce private key identity as a result party can encrypt the messages. For decryption of the message user have private key from the PKG.

3.3 PIR (Private Information Retrieval)

Private Information Retrieval (PIR) is a protocol that permits a client to retrieve an item of a database without the owner of that database being able to find which element was taken. While this problem accept a trivial solution - Sending the whole database to the client permit the client to query with perfect privacy - there are method to decrease the communication complexity of this problem, which can be critical for large databases. PIR is for the server to send whole copy of the database to the user. This is the only valid protocol that gives the user information, theoretic privacy for their query in a single-server setting. This problem was introduced in 1995.

3.4 Spatial Data

Obfuscation and k-anonymity are the privacy method built to lock up the location base service. There are two phases in this one is to get the true location of the user and the second is to modify this and minimize the class of location information. This procedure is time consuming.

The global positioning system is increasing rapidly. Numbers of users are also increasing very fast. For this we need privacy and the privacy is very important now-a-days for every kind of data. Location base services are of widely use now-a-days. Everyone uses this service on their mobile and on other devices. To use this service user put their important information in this. Many algorithms are being used now-a-days to lock up the information

Location Obfuscation:

Location Obfuscation is one of the algorithms which is used to lock up the location of the user .The purpose of Location Obfuscation is to hide the location of the user by minimizing the importance of location information. If the area will be lost then it will difficult for attacker to attack the exact location of the user.

Spatial - Temporal Structures

It is used for indexing the present and next location of the moving entity. There are two mostly used methods: PR Tree and TRP Tree. PR is good for the entity with spatial limit.

The position of the moving entity at future time p ($p >= pc$) in TRP Tree can found by applying the linear function $t(p) =$

t(p0) + v(p –p0) where p0 is the starting point and the pc is the current time and v is the velocity.

Access Mode for Privacy Preserving

Many key designs have been made or built to carry out profile and mover entity. SSTP Trees have also been built same; as the TPR. But every lead contains extra knowledge of a profile jumping vector to hold the profile conditions.

Each tag of the SSTP consists of both TPR to hold the spatial temporal attributes and profile jumping path to hold profile conditions. This technique can only allow or refuse the route demand of core, but does not relate about obfuscating spatial temporal data.

3.5. IPsec

IPsec is one of the open source protocol which is used to lock up the internet protocol delivery by encrypting and validating the sessions. IPsec is use to protect the data which passes between couple of hosts and also between the pair of security gateways. For the security of communication on the internet; IPsec is used; which uses the cryptographic security service.

The communication which happens over the network must be protected because there is some kind of data that must be saved and hidden. Many of companies use this to lock up their data.

There is some of service details which a company doesn't want to share with others must be protected from their opposite party.

IPsec is a security which is being used in Internet layer while there are some of the techniques which are operated in the upper layer such as lock up shell etc.

Attestation Header

There are some of the headers; which are the part of IPsec protocol. These are very important and they are also used when there is an attack; and protect the internet protocol.

The AH designed to provide the integrity is shown below:

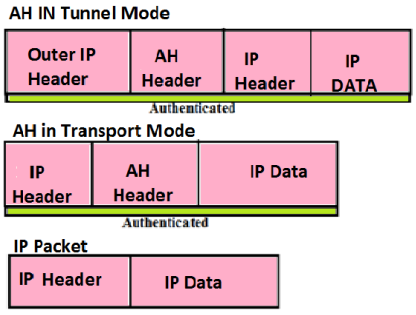

Figure 1: Attestation Header

Encapsulating Security

One of the other parts of IPsec protocol is Encapsulating Security Payload (ESP). Accuracy, stability and secrecy of the packets in IPsec is given by ESP. ESP does not provide the stability and accuracy for the packets when it is in transport shown in Figure 2.

The IPsec design calls the idea of a safety group as the basis for making security task into IP. It is only the pack of algorithms and parameters. Therefore in average bi-directional traffic the flows are locked up by a couple of safety relations. IPsec can be applied in different modes.

3.6 Cryptography

Cryptography is the technique that uses mathematics to encrypt and decrypt data. In cryptography we can store information and also you can transmit it over the internet and only the recipient can read this.

We use this to lock up our data shown in Figure 3.

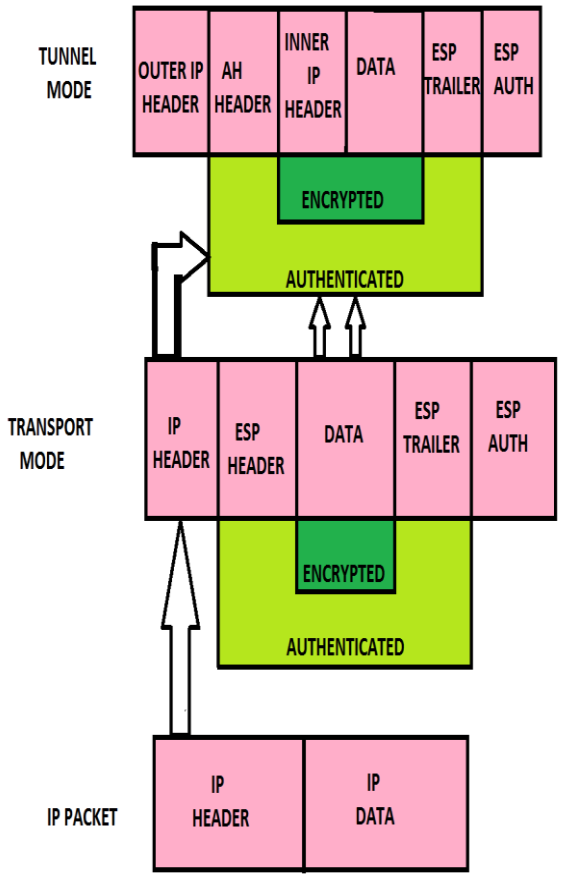

Figure 2: Encapsulating Security

Data that can be read and also can be understood without any kind of action is known as plaintext. The way which is use to spot the plaintext to hide its substances is called encryption. Cipher text is used to encrypt the plaintext result into unreadable.

If you use this no one can get access to your data and also no others can get access and also can't read your files. PGP is one of the type of cryptography.

It can be week and also be can be strong. Strength can be measured in time. Cipher text is the result of strong cryptography which is very difficult to possess. The use of cryptographic algorithm is in encryption and decryption.

Conventional cryptography

We use encryption to save our data from others who have no authority to get access to the important data and the data which is very sensitive. Cryptanalysis is also use to breakdown the lock up connection.

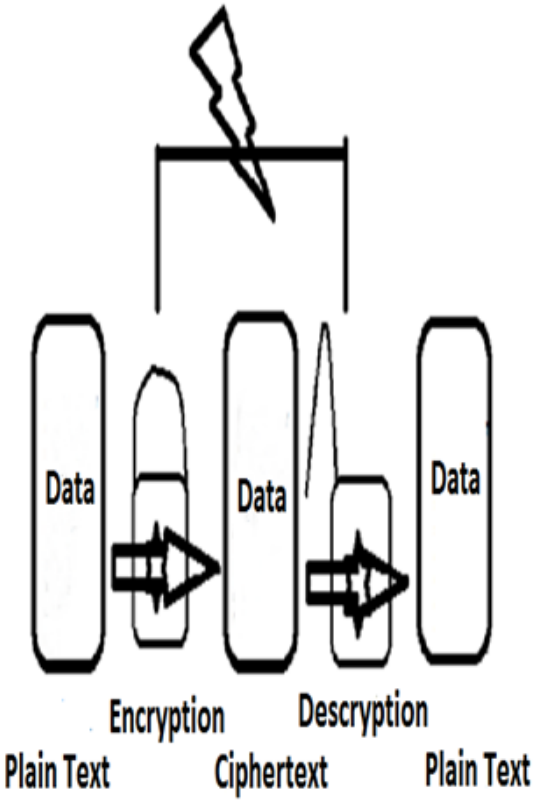

Figure 3: Cryptanalysis

One of the other types of cryptographic is conventional cryptography and also it is known as secret key. One of the type of conventional cryptographic is (DES).

The conventional cryptography is the key between the encryption and decryption. If we want to send some kind of information to other we will use this method to send our information in such a way that no one can get access to it.

If we are sending some kind of sensitive information then we will use this. We will give some key value to some specific word which we will tell the receiver and by using that he can get easily access to the data and third party can easily access it. Although this is very week but this is the one of the example of conventional cryptography. The speed of conventional is also very good and most use it is in encrypting data which is going nowhere. Due to the lock up key it is quite expensive.

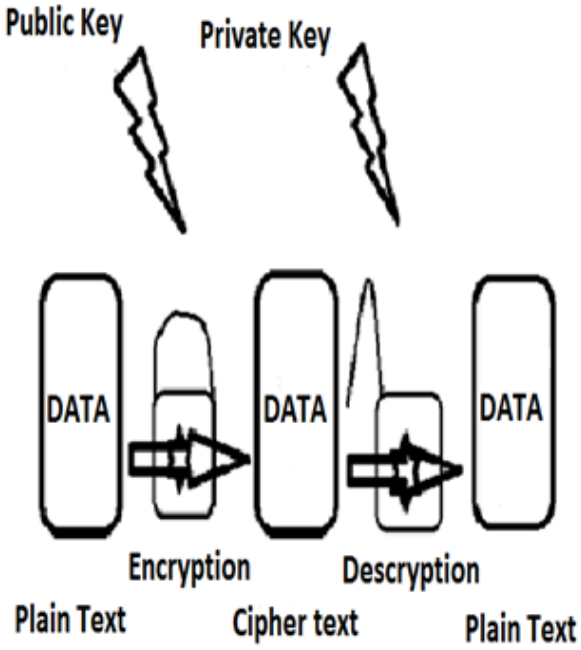

Figure 4: Public Key Cryptography

If two persons want to communicate with each other so they must have key and they have to hide that from others. If the sender and the receiver place or area is not same so they must have a lock up connection, an email or any kind of source which they are using must be lock up. There is one problem in this which is key distribution. The problem of key distribution can be overcome by using PK cryptography.

Public Key Cryptography

The PKC was introduced in 1975. PKR use couple of keys for encryption. For the encryption of the data PK is use and for the decryption we use the private key. While sending your information from sender top user you provide your public key and the private key will be in secret.

If someone has the public key he can only encrypt the data but he can't decrypt the data. He receiver can only decrypt data if he has the private key. One of reason of it usage is that people can send their information secretly shown in Figure 4.

3.6 PGP (Pretty Good Privacy)

Pretty good privacy is data encryption and decryption that present the cryptographic privacy and the verification for data delivery. PGP is used for the security purpose. It is also used to lock up the email communication. The usage of PGP is in encrypting and decrypting the texts. The standard which is use for the PGP is Open PGP.

Some of the function of conventional cryptography and Public key are gather by PGP. Whenever a user encrypts data by using PGP; PGP firstly compressed that data due to this the time is save, the space of disk is save and also increase the cryptographic security. PGP generates the session key which is the one-time-only session key. Some numbers are generated when you move your mouse and also when we type keystrokes theses are created randomly.

For the encryption of the data this key work efficiently and then will be the generation of cipher text. The session key and also the public key work together and the key along with the cipher text is send to the receiver. While in the decryption the receiver copy of PGP use the private key to get the session key and uses to decrypt the cipher text.

Keys play a very important role in the cryptography algorithm. Keys are the very large numbers. If the length of key will be high its mean that the encryption is more lock up.

Digital signature

If a sender adds 1 to his or her secret key encrypted text then the message will with digital signature. By use of this user can check the validation of the message while it is coming from the sender from which he wants and also he can check the integrity of it.

3.7 DES (Digital encryption standard)

NIST publish a symmetric key block chipper called DES. It was publish in 1975 as a draft of FISP. There are two permutations which are used in encryption method; starting and final permutations. And there are 16 Festal round in the structure of DES. Security of DES is good.

It uses some fast subroutines. It is easy to study which proves that many of attacks will fail. If any of irrelevant party want access to the data it will fail. DES simple and it is easy to implement.

Des take some input string as plaintext and after passing through 16 rounds it convert it into the Cipher Text whose length is same as the input length. The block is of 64bits. A key is used in DES. Decryption only can be done when a user has a key through this he/she can encrypt.

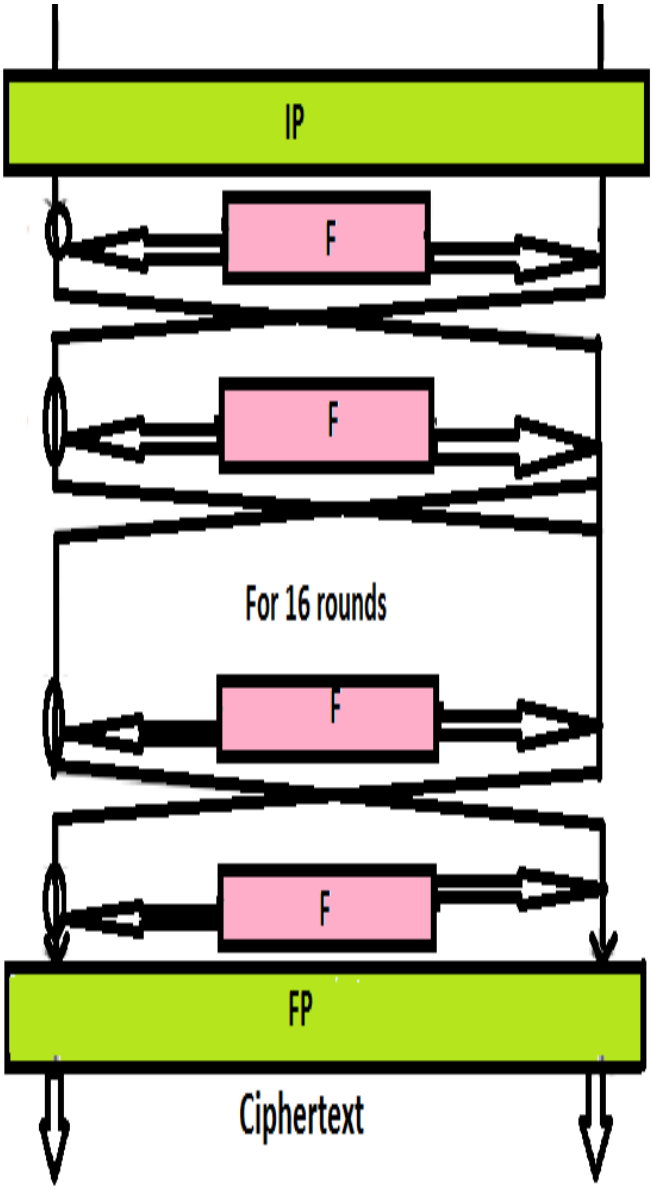

Figure 5: Digital Encryption Standard

The key is of 64 bits but 56 bits are used by the algorithm. The block is of 64bits. A key is used in DES. Decryption only can be done when a user has a key through this he/she can encrypt. The key is of 64 bits but 56 bits are used by the algorithm.

The 64 key is divided into two parts of 32 bits before the main round. There is some crossing happen which is called the Festal scheme. The festal shape makes sure that the encryption and decryption are same method. There is only

difference which that when we are decrypting then the sub keys are in reverse order shown in Figure 5.

DES has some standard. There will be some of attacks which will break down the DES. Some of the attacks are Brute force. There is another attack which is called the Davies attack which will break DES with the complexity 2^56.

Brute force is also an attack which destroys it. Brute force checks the all keys until the require key founds. There are some are attacks which are much worse than of Brute force.

- Differential Cryptanalysis
- Linear Cryptanalysis
- Improved Davies' attack

3.8 Triple Digital Encryption Standard

Triple DES depends on the DES algorithm. It also has the advantage of proven reliability and a longer key length that remove many of the attacks that can be used to decrease the amount of time it takes to break DES. But this will not safe or lock up the data for longer time.

Now-a-days AES is use at the place of DES. Triple DES is very efficient. Many of the security system refer this system. The Triple DES key takes 3 keys and each key have length of 64 bit.

The Triple DES breaks the user key into three parts. In this data will be encrypted in first, then decrypted in second key and will again encrypted in third key. The speed of Triple DES is not much but it is more efficient if you will use it in good manner and if you will manage it good.

There are some of the Triple DES modes which are working same as the some modes of DES. The some of the modes of triple des are Triple ECB and Triple CBC.

Drawbacks:

Its performance is not much good because there in effective codes for DES/3DES and its security is not much good because for this we need a large blocks.

Advanced Encryption Standards (AES)

It was issue in 1997 by US NIST and in 2000 it was names as AES. AES is much faster and efficient then of Triple DES [19]. Security is also much good than of Triple des and also its cost is not much. AES is spelled out by the NIST. AES is using in many companies and organizations. Many of security software are using AES shown in Figure 6.

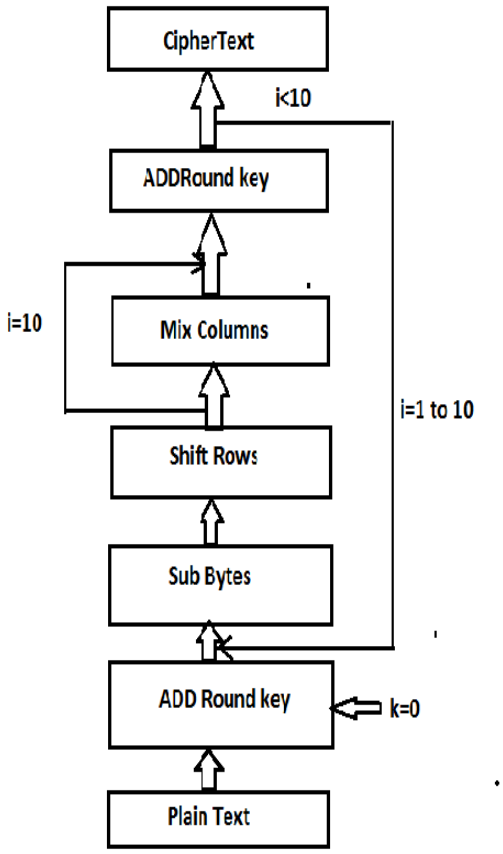

Figure 6: Advanced Encryption Standard

4. CONCLUSION

In this paper, we have presented the survey of different methods of data privacy applicable on different kinds of data. Firstly; we discussed the cloud computing privacy issues and for this purpose we used PKI, IBE, PIR methods and then spatial data privacy. We have used Obfuscation or k-anonymity method. IPsec is an open source protocol which is used to lock up the internet protocol delivery by encrypting and validating the sessions. Cryptography is the technique that uses mathematics to encrypt and decrypt data. In cryptography we can store information and also we can transmit it over the internet and only the recipient can read this. Pretty Good Privacy (PGP) is data encryption and decryption technique that presents the cryptographic privacy and the verification for data delivery. It is also used to lock up the email communication. PGP is also used for the security purposes. The usage of PGP is mostly in encrypting and decrypting the texts. Security of DES is good. It uses subroutines. There are two permutations which are used in encryption method with starting and final permutation. There are 16 Festal round in the structure of DES. It is used to lock up almost all types of data. Triple DES is based on the DES

algorithm. The Triple des key will take 3 keys data will be encrypted in first, then decrypted in 2nd and will again encrypted in 3rd key. Its performance is not good enough because there are ineffective codes for DES/3DES and its security is not much good because for this we need a large blocks. AES is much faster and efficient than Triple DES. Its security is also much good than that of Triple DES and it is less expensive as well. Many companies and organizations are using AES method. Many of security software are also using AES, because it is the most efficient method than other methods.

REFERENCES

[1] AlSudiari, Mohammed AT, and T. G. K. Vasista. "Cloud computing and privacy regulations: an exploratory study on issues and implications." *Advanced Computing: An International Journal (ACIJ)* 3.2 (2012).

[2] Ardagna, Claudio Agostino, et al. "Location privacy protection through obfuscation-based techniques." *Data and Applications Security XXI*. Springer Berlin Heidelberg, 2007. 47-60.

[3] Mokbel, Mohamed F. "Privacy in Location-based Services: State-of-the-art and Research Directions." *Mobile Data Management, 2007 International Conference on*. IEEE, 2007.

[4] Jafarian, Jafar Haadi, et al. "Protecting location privacy through a graph-based location representation and a robust obfuscation technique." *Information Security and Cryptology–ICISC 2008*. Springer Berlin Heidelberg, 2009. 116-133..

[5] Pearson, Siani. "Privacy, security and trust in cloud computing." *Privacy and Security for Cloud Computing*. Springer London, 2013. 3-42.

[6] Ardagna, Claudio, et al. "An obfuscation-based approach for protecting location privacy." *Dependable and Secure Computing, IEEE Transactions on* 8.1 (2011): 13-27.

[7] Mokbel, Mohamed F., Thanaa M. Ghanem, and Walid G. Aref. "Spatio-temporal access methods." *IEEE Data Eng. Bull.* 26.2 (2003): 40-49.

[8] Cai, Mengchu, and Peter Revesz. "Parametric R-tree: An index structure for moving objects." *Proc. of the COMAD*. 2000.

[9] Atluri, Vijayalakshmi, and Heechang Shin. "Efficient security policy enforcement in a location based service environment." *Data and Applications Security XXI*. Springer Berlin Heidelberg, 2007. 61-76.

[10] PKI reborn in cloud by Jaimee Brown and Peter Robinson RSA, The Security Division of EMC found at: http://365.rsaconference.com/servlet/JiveServlet/previewBody/3037-102-1-4074/NMS-301 %20-%20PKI%20Reborn%20in%20the%20 Cloud.pdf

[11] Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." *Advances in Cryptology—CRYPTO 2001*. Springer Berlin Heidelberg, 2001.