International Journal of Computational Research and Development (IJCRD)
Impact Factor: 4.775, ISSN (Online): 2456 - 3137
(www.dvpublication.com) Volume 2, Issue 1, 2017

SECURING DATA IN MOBILE CLOUD COMPUTING USING CUBICAL TECHNIQUE FOR KEY MANAGEMENT

A. T. Ravi* & N. Gowri Priya**

* Associate Professor, Department of Computer Science and Engineering, SSM College of Engineering, Komarapalayam, Tamilnadu

** Assistant Professor, Department of MCA, SSM College of Engineering, Komarapalayam, Tamilnadu

Cite This Article: A. T. Ravi & N. Gowri Priya, "Securing Data in Mobile Cloud Computing Using Cubical Technique for Key Management", International Journal of Computational Research and Development, Volume 2, Issue 1, Page Number 55-58, 2017.

Abstract:

Traffic interception is one of the important and major problems in the present era. Whenever we are developing algorithms for construction of more security for the data there is an equal or more chances for the malicious users to develop algorithms to destruct the data or network. We need to be more cautious of the problems when we are using third party for data and key storage. Present days we need to store data and key values are to be stored in third party servers called cloud servers. When we are using mobile devices for data transfer and key transfer we need to send them in secure manner. When mobile devices are moving from one place to another place they need to travel in sensitive networks. During handover management attackers may gain their access by impersonation. Attacker may have every chance to take advantage of stealing access credentials of actual user. When we are sending data in network some malicious users may see or modify the data. Cryptanalysis may be the problem. In order to avoid the problem we need to store key/data in cloud server in secured way by splitting the key and applying Homomorphism Algorithm which may depend on third party for key/data storage. In order to store them in secure manner we are using Cubical Technique by distributing the key in multiple clouds.

Key Words: Cryptanalysis, Homomorphism Algorithm & Cubical Technique

1. Introduction:

Mobile device users are increasing rapidly. Almost 95% of people in the earth using mobile devices. People are using basic phones and also smart phones. Smart phone users are also increasing rapidly. In very near future almost all the people using mobile phone are smart phone users. Facilities in smart phone not only communicating by telephonic conversation and also for SMS, MMS messaging, social network utilization like face book, twitter, LinkedIn etc. Gaming is also one of the important features in smart phones. We can also use smart phones for internet browsing. Present day's smart phone replaces laptops and pc's. We can also use Google and other search engines in our smart phones. International market for smart phones is increased with increasing facilities. So many apps are developed using android phones and became more popular. By increasing demand for smart phones increases the security problems. Whenever we are using mobile smart phones because of the movement of the phone we can enter from one network to another network rapidly. These rapid mobility causes loss in signal and security many times. We may travel some sensitive areas may cause so many security issues. We are going to learn some security problems. Before knowing security problem we need to learn about the mobile technology briefly. We are using large data with mobiles. Some data may be sensitive. We are saving our data in the cloud servers. In order to retain mobile data in cloud servers securely we need to take lot of measures. We also take care about the data to be communicating securely. And finally correct person has to take the data without impersonation. We need to work a lot for privacy and protection of data from attackers is a serious need. Virtualization of cloud servers also creates vulnerability in communication channels.

Figure 1.1: Mobile Cloud Computing Advantages

2. Related Work:

Whenever we are using public/private keys, keys are to be stored in cloud servers. We need to take lot of care for their preservation. The public/private key may be disclosed by malicious user due to cryptanalysis.

Then the key is distributed among multiple servers [3] and homomorphism algorithm is applied for the key to preserve it privately. In this algorithm we are using more servers instead of a single server to preserve our key by using encryption technique we need to encrypt the entire key at client side and cut the entire key into different parts and apply homomorphism algorithm on each part. Then send each part to the cloud servers. So the cryptanalyst cannot estimate which key is from which part. He doesn't know the start and finish of the key. He cannot estimate the pattern of the key. He cannot integrate the keys. So this is a best technique used for key privacy not disclosing to attacker. For privacy preserving of data or resource [3] the data owner has to take lot of care about the important data not to be disclosed when it saves in the cloud servers. A hybrid data security model for the cloud storage and communications will be implemented by combining various techniques together to achieve the data security goal. The techniques included in the combination would be data encryption with secure key exchange [4]. If the data saved in cloud servers the cloud server compromise may disclose our data. Or the malicious attacker (man in the middle) can crypt analyzes the data from owner. We need to develop new algorithms for the improvement of security when we are in unsecured area. A system for strong authorization for access but the authentication is not that much strong. Cubical technique is the plain text may obtained by anybody who knows how to solve the cube, especially with the 2*2*2 cube used in their experiment [7].

3. Proposed Work:

We are proposing begin with the implementation of strong authentication. In this respect we propose composite key for storage in cloud servers. Homomorphism algorithm is implemented to encrypted secret key from key owner [3], digital certificates are provided to key requesters for key grant. Resource protection from malicious attackers, Authentication is to be safer. The users want to connect the cloud servers for requesting keys in a secured way. For example by using SSL network the data travels in a safer mode. When a user wants to utilize the resource he/she needs to take permission from resource owner. This permission is in token format. The purpose of this procedure is to make the data and resource in secured way and not to disclosed to the outside environment. Here our main work is to distribute the composite key to be encrypted first and then splitting it into multiple parts and apply homomorphic algorithm, then sends each piece to each cloud server using cubical technique which makes our key very authenticate & secure. When intruder sees the pattern of the keys he cannot understand them and cannot break them.

Figure 3.1: Cloud Servers

Homomorphic Algorithm: This algorithm is used on cipher text to keep the cipher text more secured when the data or information is more sensitive. When more attacks are happening or predict to happen then this algorithm is used. This algorithm is very simple to use. This is used to prevent the data from insecure networks to avoid cryptanalysis. Homomorphic algorithms are very much useful in cloud computing especially we are using mobile data which is very sensitive to network used mainly for confidentiality of data.

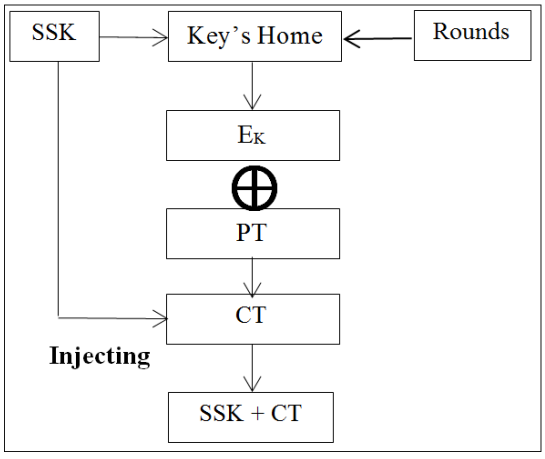

Figure 3.2: Encryption Process

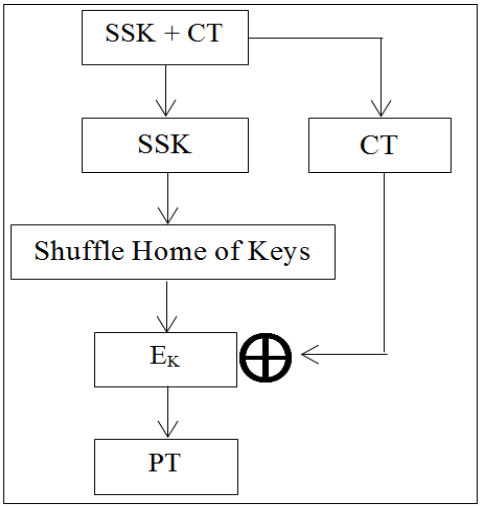

Figure 3.3: Decryption Process

Homomorphic algorithms are also used for other systems like electronic voting systems, also for collision resolution techniques etc. When the key owner sends encrypted key directly to store it in cloud server then the chance of interception is high. Cryptanalyst may analyze the key when the owner sends it through the network. When the network is sensitive then there is a chance of crypt analyzing the data/key. When only single key is used for cloud server to store by key owner there will be problem of Cryptanalysis of the key by the analyst.

Key to be Distributed in Cloud Servers: Data owner/key owner must take care about key as well as data to be securely stored in cloud servers. The problem of key disclosure is minimized by using cubical technique. Key is going to retained by multiple cloud servers for more security. Then the data is also stored in cloud servers by using distributed system when needed. Otherwise data is stored in one cloud server only by applying encryption algorithm on the data. Each key requester can take the permission from key owner and get the key from cloud servers distributed among them. Then the key owner sends algorithms for integration of distributed data which is collected from cloud servers and apply decryption algorithm send by key owner in secured way gives the key value. Here we need three algorithms one for homomorphic algorithm used by the owner, integration algorithm to combine encrypted key and finally secret key decryption for decrypting the key and for distributing the keys with the help of Cubical technique.

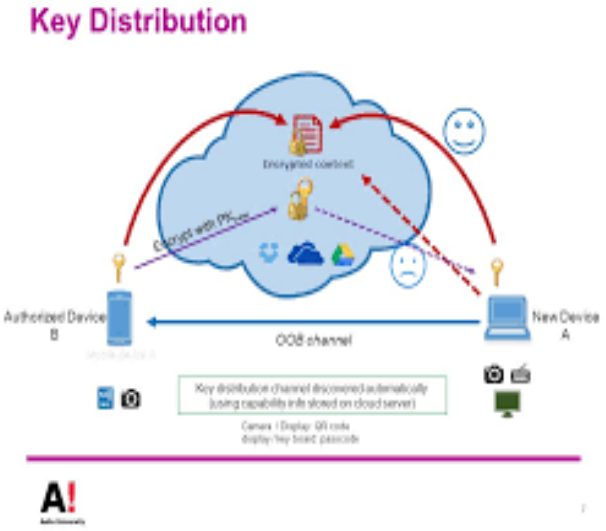

Figure 3.4: Key Distribution in Cloud Servers

Cubical Technique in Key Distribution: Key shuffling is done with the help of Cubical technique for more security process. Data should be encrypted using Integration algorithm and decrypted. The key is splitted into various parts using homomorphic algorithm to avoid hacking the key. With the help of Cubical technique, the key is distributed to the cloud server with the Cubical value. The algorithm uses the cube to generate the key in a specific way that is completely different from the other current algorithms. Cube 8*8*8 has a 3.6×10^{217} possible number of permutations. The key will not be exchanged. The secret shared key will be exchanged instead.

4. Future Work:

We can develop more protected algorithms for key storage and safely deliver to the correct person without the leakage. Impersonation and key stealing should be eliminated. Key preserving is good here but improvement is needed for distribute the key to the users in more secured way. Data is also stored in secured way in cloud servers for the network interception and server compromise. Improvement in response timing & performance should be monitored.

5. Conclusions:

Today most of the people are using cloud servers as a third party for authentication as well as data store. So people are taking services with less cost and effort from cloud servers. At the same time there are lot of security threats are encountered. We need to do lot of work to minimize the security threats in this regards and we need to concentrate in the performance timing while distributing the Key to multiple clouds.

6. References:

1. http://www.ijifr.com/pdfsave/25-08-2015925V2-E12-037.pdf
2. http://ijcttjournal.org/Volume9/number-4/IJCTT-V9P140.pdf
3. D. Hardt, The OAuth 2.0 Authorization Framework, Ed. Microsoft. July 31, 2012. <http://tools.ietf.org /html/draft-ietf-oauth-v2-31> (accessed 10.01.14).
4. Satpreet Kaur, Mandeep Singh, A Novel Cryptographic Key Distribution Scheme For Cloud Platforms, [IJCA], 2015, 22-25.
5. S. Xiao, W. Gong, Mobility can help: protect user identity with dynamic credential, in: The Eleventh International Conference on Mobile Data Management (MDM), 2010, pp. 378–380.
6. M. Leandro, T. Nascimento, D. Santos, M. Westphall, C. Westphall, Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth, in: The Eleventh international Conference on Network (ICN), 2012, pp. 88–93.
7. Ali M Alshahrani and Prof. Stuart Walker, Computer Science and Electronic Engineering, University of Essex, Wivenhoe Park, Colchester, Essex, UK, C04 3SQ, New approach in Symmetric Block Cipher Security using a new Cubical Technique [IJCSIT],2015, pp. 69-75.