# A Novel Cryptographic Key Distribution Scheme for Cloud Platforms

Satpreet Kaur
Dept. of IT
CGC Landran, Mohali

Mandeep Singh
Dept. of IT
CGC Landran, Mohali

## ABSTRACT
The problem of secure data transmission on cloud environments is addressed in the proposed security model. The data security is quite important on cloud environments because they belongs the users. The security layer is defined or implemented between the cloud user and server end to ensure the security of data being exchanged between them. In this research, a key exchange scheme has been proposed to ensure the security of cloud platforms. The proposed model under this research project presents improved random key management architecture, which may be called efficient multi-level complex key sharing and authorizing model (EMCKS) for the cloud platforms. In particular, the proposed model allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to EMCKS and verify system output. In this research, we will develop the proposed scheme named EMCKS for corporate key management technique adaptable for the clouds by making it efficient and quicker. In addition, it also has to be improved to work with Cloud server and client nodes, which enforces the proposed scheme to create a secure environment based cloud platforms. The proposed scheme has been noticed providing hardened security than the other key management architectures as it is based on non-predictive key generation mechanism. The results have shown the effectiveness of the proposed model in terms of elapsed time.

## Keywords
Cloud security, authentication, key management, secure access, channel security

## 1. INTRODUCTION
Cloud computing meets unique constraints with minimum overheads for individual clients to fulfill their on-demand needs for Data Storage and Computing Resources. Cloud computing is very useful for those who can't afford a big computing infrastructure. Latest trends show us the growth of cloud computing due to its very economical and attractive features. Multiple applications can be run simultaneously over cloud and large amount of data can be easily outsourced over cloud that is why cloud computing is steadily getting popular between clients cause the ever increasing need for storage accounts and computing power can be achieved by cloud computing. The research literature on this topic has covered a thorough coverage with the help of earlier cloud surveys. A overview of the following topic have been provided below in field of cloud computing security and remote computational and storage security with the help of previous publications. Some common terminologies must be defined before we proceed. In early days members of the cloud computing societies have different views that which features should be part of the concept of cloud computing and which should be not, Later the proper definition was provided which divides the cloud computing into three distinct models according to the different capabilities provided to the consumer by U.S. National Institute of Standards and Technology (NIST). There are three different threats in security of cloud computing. In a variety of ways the base server access can be prevented for end user. Blocking of communication between End User and Server. Analogue and Digitally this can be done by Jamming signals and by Denial of Services (DOS) attacks that effects network between server and End User. In base station strategic nodes can be targeted by DOS attacks to block communication.

Setting incorrect routing information to make the data flow in loops r in wrong directions can be used to prevent communication between the server and the nodes connected to it. Spoofing the server and making nodes into rerouting all packets to spoofed server instead of real is one way to do it.

There are many methods to attack on cloud. Attacks of acquiescent character are privacy attacks on cloud network. Eavesdropping on opponent's servers and monitoring sensors nodes to find vital information are most common. Encrypted information can even be attacked sent by sender by analyzing traffic information in which sensor conditions can disclose enough information to the privacy attacker. Camouflage Adversaries are those in which intruder attack the opponent by affixing its node into the existing wireless network. The most important issue is the security of the cloud computing. The different kind of attacks is used to happen on the wireless network. A hacker using malicious code in sensor network changes the routing data of protocols this attack is called False routing Information. In active attack hackers puts malicious information in a particular node this nodes act like a normal node but does not forward the data packets to the other nodes which 0makes it failed node this attack is called Selective Forwarding. Masquerading attacks, Man in the middle attack or other passive attacks are one of many attacks that can be used for stealing useful information.

In cyber space to prevent several types of attacks on cloud various types of authentication schemes are available. Basically two basic key exchange mechanisms are available: Non-predictive key management and Predictive key management schemes. Key generation and verification based on mathematical formula is the base of the Predictive key exchange scheme. Higher probability of guessing attacks in many cases on such methods are found. A replica algorithm is used in guessing attack for key generation by the hacker to penetrate the cloud resources. The second mechanism is Non Predictive Key Exchange which is based on Key Table Generation which uses heavier amount of memory because it is heavier table.

## 2. DRAWBACKS IN EXISTING SYSTEM
- The existing schemes are based upon the centralized authentication models using the key exchange protocols,

which raises the threat of the invading through passive information leakage attacks.

- The existing schemes use the different key mechanisms for the servers being accessed (internally accessed server) and not accessed (externally accessed server) from the outer networks. If the internally accessed server has to provide information to the user on the internet, there would be high risk of the data being hacked

## 3. PROBLEM FORMULATION

Clouds consist of a number of server nodes which are connected to each other using fiber channels. The cloud servers are being accessed by the users in the cyber space (internet). Because the cloud server and users are connected with each other using the internet connections, hence they are highly prone to the hacking attacks during the data transportation over internet. Cloud Platforms are used to sense various environmental or other parameters which can be used to predict natural hazards, climatic changes or other types of data analysis. During the periods when the Cloud nodes are in working condition, they need secure cryptographic keys for secure propagation of the sensitive information. Efficient key management and distribution scheme play an important role for the data security in clouds. Existing cryptographic key management and distribution technique usually consume higher amount of energy and put larger computational overheads on Cloud nodes. The cryptographic keys are used on different communication levels of Cloud communications i.e. neighbor nodes, cluster heads and base stations. An effective corporate key management and distribution policy is required to maintain the security of the cloud platforms. The problems described in the base papers are related to the requirement of efficient key exchange policies for clouds. In the proposed model, we are trying to solve the key-problem of energy efficient and secure key exchange scheme.

## 4. PROPOSED SYSTEM

In this research, we have proposed a hybrid data security model for the cloud storage and communications, which 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. The proposed model has been divided into two major components: Data encryption and secure authentication using key exchange. Then the data encryption will be used to create a completely unreadable and encrypted data. A fast and robust variant of data encryption (possibly AES or Blowfish) will be used for the encryption module. The proposed in this research model will utilize the key exchange model along with the data encryption and compression used earlier in the proposed system in order to protect the user data privacy and integrity. The proposed model in this research presents improved key management architecture, called efficient multi-level complex key sharing and authorizing model (EMCKS) for the clouds, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. EMCKS protects the entire life cycle of cryptographic keys. In particular, EMCKS allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to EMCKS and verify system output. In this research, we will develop the proposed scheme named EMCKS for corporate key management technique adaptable for the clouds by making it efficient and quicker. In addition, it also has to be improved to work with Cloud server and client nodes, which mean they must use less computational power of the cloud nodes.

## 5. SCOPE OF THE STUDY

The clouds are being used by the organizations and personals for the management or storage of their accounts, finances, software source codes and various types of other data. The security of the data is very important. The possibility of the attacks on the clouds, especially on the inter-nodal communications is very high. For the purpose of security many security solutions and applications have been designed and implemented. Threat of the attacks on the security solutions always increases with it gets older. Hence, there is always a requirement of the improvements in the existing solutions or the development of the newly designed security solutions to protect the data privacy on the cloud platforms, especially during the inter-nodal communications, where the data is being exchanged between the cloud and the users. The proposed model is based on the security of the inter-nodal communications for the purpose of the cloud platform security. The proposed model is designed using the combination of secure key exchange and message encryption mechanisms.

## 6. PARAMETERS

The results of the proposed security model will be evaluated using the standard performance parameters. The proposed model will be implemented to return the following parameters:

- ***Key Generation time:*** Total time taken for the key generation process.
- ***Key Transfer time:*** Total time taken to send the key information from one to another and vice versa.
- ***Key Verification time:*** Total time taken for the key matching and decision making process is called Key Verification Time.
- ***Entropy:*** The entropy gives the statistical uniqueness of the keys in the table in the form of a uniqueness index called entropy.
- ***Network Load:*** Network Load is the amount of data (traffic) being carried by the network at a particular time. The network load varies from time to time. It is represented in bytes per second or packets per seconds**.**
- ***Throughput:*** Throughput or Network throughput is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bytes per second or packets per seconds.
- ***End to End Delay:*** The end-to-end delay is the time from the generation of a packet by the source up to the destination reception, so this is the time that a packet takes to go across the network. This time is expressed in seconds (sec).

## 7. METHODOLOGY

A detailed literature survey on the key management algorithms or methods would be conducted in the first stage of the project development. A detailed literature survey would be conducted to know the problems and requirements of the existing authentication mechanisms for the cloud platforms. The requirement and structural analysis of secure key distribution and management in cloud nodes will be studied in detail to find the merits and demerits. The new security solution would be carefully designed and reviewed to overcome the shortcomings of the existing studies. The

proposed algorithm would be implemented using the NS-2 simulation. The implementation of the proposed model will be designed to return the results in the form of various performance parameters. The implemented algorithm would be thoroughly tested and corrected. The results obtained would be analyzed and the conclusion will be formed after the detailed analysis of the results of the proposed model.

The proposed secure authentication model will use the secure key exchange model. The key generation will be using the multiple keys generation using the pseudorandom number generation (PRNG) algorithm, which uses a controlled structure to generate the numbers based on seeding input.

The hackers need to guess the seeding input, which is very difficult, hence there are less changes of the guessing attacks in the PRNG based key generation architectures. The keys will encrypted before the transmitting them to the other nodes in the cloud, which will protect the process of authentication. The secure channel will be created between the cloud nodes using the secure key sharing between them. The secure channel is the most secure solution against the replication, replay and primary user emulation attacks, but the data travelling on the secure channels can be captured using the man in the middle, masquerading or other similar passive information leakage attacks. To protect the data against such attacks, the message encryption mechanism has been integrated in the security mechanism for the inter-nodal cloud security.

# 8. CONCLUSION

The clouds are being used by the organizations and personals for the management or storage of their accounts, finances, software source codes and various types of other data. The security of the data is very important. The possibility of the attacks on the clouds, especially on the inter-nodal communications is very high. For the purpose of security many security solutions and applications have been designed and implemented. Threat of the attacks on the security solutions always increases with it gets older. Hence, there is always a requirement of the improvements in the existing solutions or the development of the newly designed security solutions to protect the data privacy on the cloud platforms, especially during the inter-nodal communications, where the data is being exchanged between the cloud and the users. The proposed model is based on the security of the inter-nodal communications for the purpose of the cloud platform security. The proposed model is designed using the combination of secure key exchange and message encryption mechanisms. The performance of the proposed model will be evaluated using the parameters like key generation time, key distribution cost, overhead, entropy, etc.

# 9. FUTURE WORK

In the future, the proposed model will be enhanced in terms of security. The enhancement will be focused upon the improvement of the authentication scheme in order to make it more complex and secure.

# 10. REFERENCES

[1] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, *"KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904*, pp. 1-18, Springer, 2013.

[2] N. Suganthi, V. Sumathy, *"Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1*, pp. 71-78, INT J COMPUT COMMUN, 2014.

[3] Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter, *"Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306*, pp. 270-289, Springer, 2013.

[4] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, *"Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory, NIST, 2013.*

[5] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, *"SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18*, pp. 1-8, IEEE, 2013.

[6] Md. Monzur Morshed, Md. Rafiqul Islam, *"CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3,* pp. 571-576, IEEE, 2013.

[7] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma *"Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".*

[8] Sonam Palden Barfunga Prativa Rai, Hiren Kumar Deva Sarma, *"Energy Efficient Cluster Based Routing Protocol for Wireless Sensor Networks", ICCCE IEEE 2012, 3-5 July 2012, Kuala Lumpur, Malaysia.*

[9] Sajal Sarkar, Raja Datta, *"A Trust Based Protocol for Energy-Efficient Routing in Self-Organized MANETs", IEEE 2012.*

[10] Said BEN ALL*, Abdellah EZZATI, Abderrahim BENI HSSANE, Moulay Lahcen HASNAOUI, *"Hierarchical Adaptive Balanced energy efficient Routing Protocol (HABRP) for heterogeneous wireless sensor networks", IEEE, 2010.*

[11] Javed, Muhammad A., and Jamil Y. Khan. "A Geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." *Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011. IEEE, 2011.*

[12] William B. Davis, *"Graphical Model Theory for Wireless Sensor Networks" (December 8, 2002). Lawrence Berkeley National Laboratory. Paper LBNL-53452.*

[13] J. Kusuma, L. Doherty, and K. Ramchandran, *"Distributed Compression for Sensor Networks, International Conference on Image Processing (ICIP), October 2001.*

[14] Dragan Petrović, Rahul C. Shah, Kannan Ramchandran, Jan Rabaey, *"Data Funneling: Routing with Aggregation and Compression for Wireless Sensor Networks", First IEEE International Workshop on Sensor Network Protocols and Applications, May 11, 2003.*

[15] Raymond Wagner, Shriram Sarvotham, Hyeokho Choi, Richard Baraniuk, *"Distributed Multiscale Data Analysis and Processing For Sensor Networks", Rice University Technical Report, February 9, 2005.*

[16] Karim Seada, Marco Zuniga, Ahmed Helmy, Bhaskar Krishnamachari, *"Energy Efficient Forwarding Strategies for Geographic Routing in Lossy Wireless Sensor Networks," ACM Sensys 2004, November 2004.*

[17] Scott Briles, Joseph Arrowood, Dakx Turcotte, Etienne Fiset, *"Hardware-In-The-Loop Demonstration of a Radio Frequency Geolocation Algorithm", Proceedings of the Mathworks International Aerospace and Defense Conference, May 24-25, 2005.*

[18] da S Araújo, H., and Raimir Holanda Filho. *"Wsn routing: An geocast approach for reducing consumption energy." In Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, pp. 1-6. IEEE, 2010.

[19] Shim, Young-Chul, and C. V. Ramamoorthy. "Monitoring and control of distributed systems." In Systems Integration, 1990. Systems Integration'90., Proceedings of the First International Conference on, pp. 672-681. IEEE, 1990.

[20] Alain Bertrand, Bomgni, and Myoupo Jean Frédéric. *"An energy-efficient clique-based geocast algorithm for dense sensor networks." Communications and Network 2010 (2010).*

[21] Qian, Yi, Kejie Lu, and Nader Moayeri. *"Performance evaluation of a secure MAC protocol for vehicular networks." Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008.*

[22] Dias, João A., et al. *"Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks."GLOBECOM Workshops (GC Wkshps), 2011 IEEE. IEEE, 2011.*

[23] Hung, Chia-Chen, Hope Chan, and EH-K. Wu. *"Mobility pattern aware routing for heterogeneous vehicular networks." Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE. IEEE, 2008.*