CLUSTER KEY MANAGEMENT PROTOCOL IN HYBRID CLOUD USING MACHINE LEARNING

M. Karthick
Department of Computer Science, Hindustan College of Arts and Science, India

Abstract

The GKMP is an emergent protocol for protected group networking systems, such as video conference, video on demand etc. GKMP offers keys in groups for development and delivery. It is not a central main manager's interference. GKMP incorporates region-based cluster and the formation of regional cluster protocols in order to enhance the protection of multicast ecosystems (CP). A digital signature technology is used to handle the security issue effectively. This paper also reflects on the use of this intelligent protection algorithm in the distributed environment in the GKMP community controller. The analogy with traditional technologies reveals that the algorithm proposed is far superior by having better protection and decreased overhead in multicast settings. This CP system improves GKMP scalability in cloud surroundings.

Keywords:

Clusters, Group Controller, Digital Signature, Group Key Management

1. INTRODUCTION

The development and marketing of the Internet presents a wide range of situations where bandwidth and sending costs are significantly saved by community contact using multicast. Examples include news and inventory quotes, recording, teleconferences, app upgrades, video on request and more. Stable multicast sessions can be introduced by implementing encryption schemes. Messages are encrypted using a selected key, known as the Session Key or Data Encryption Key in the sense of community communication (DEK). The original message will only restore those understanding the DEK. The issue of transmitting data safely to authorised group members thus reduces the number of DEKs among the authorised group members to safe establishment. Moreover, membership changes can include refreshment of the community key. This key refresher mechanism stops a joining member, even if he or she has registered earlier messages in their crypted keys, from decoding messages that have been exchanged.

In networking systems such as multi-party distribution, video conferencing, etc., IP multicast plays an important function. The primary challenge in IP networking is the protection of data sharing over classes [4]. As it includes multiple diverse members the key downside associated with this correspondence with the Community is the introduction of security protocols [2]. This participants may quit or rejoin dynamically, so it becomes very difficult to address safety issues [9]-[11]. Several safety measures, such as access control, integrity control, authentication and confidentiality are important for enhancing community communication security [1].

This paper provides the best way to secure the privacy of users, i.e. encrypt data stored in the cloud world. In general, the authenticated user can access encrypted data in the cloud using a community key management protocol or an algorithm [3]. Proxy re-encryption technique is used to counterfeit dynamism problems and a large-scale semi-confident cloud environment. The proxy re-encoding is performed over a cloud server, which re-encodes the community key. This re-encryption helps users to decrypt the community key and use a private key [4].

The role of public membership is modified locally by means of rekeying, and the key is constant over the whole cycle. We also developed the Hyper Sphere hypothesis to deal with this complex aspect of the cloud world, but the size of the key is easily expanded when re-kept. The private key functionality is introduced by hashing, and XNOR offers a convenient and efficient way to minimise cloud key size.

2. RELATED WORKS

The GKMP problem is a big concern that many researchers have highlighted to address so that effective network community connectivity is possible. Fault tolerance is a big downside to delays and node loss in asynchronous networks [8]. Detection of errors and methods of corrections leads to frequent contact with classes of error messages. The layout of a logical ring structure with messages to detect contact faults in community is confined to this overhead [5].

GKMP is known to be an ad hoc network resource consuming protocol and lacks stability. Protection is restricted in these networks by main public networks without the use of a central network [6]. The keys are structured so that the participants adjust dynamically. Community keys in the protocol routing must be energy efficient, so it will be wisest to use a distributed key. The author [7] proposes a stable, optimised connection routing protocol which effectively distributes and manages the group keys. This protocol reduces the number of unwanted users accessing the network and efficiently handles incidents such as node connection and merger. This technology reduces the energy and control messages consumed during the cryptography process.

The proposed framework to strengthen security and enhance users' authentication during the update. In addition to this rekeying process, the automated backbone medium can boost protection and energy efficiency. For a particular group, the use of Group Controllers (GC) with theory of hyperspace is introduced. Here, an individual member of the group represents a hyper sphere and the central point is regarded as a standard group key.

3. METHODOLOGY

Based on the available parameters the GKMP scheme is updated and the paper then deals explicitly with the re-encryption scheme. The CP is uniquely configured for cloud distribution. The previous study focused specifically on a centralised environment which maintains higher integrity, which can be checked by means of public records. The whole clustering mechanism suits the HS theory well, so with the aid of ECDSA [12] XNOR functional algorithm the protection scheme deployed over GKMP is achieved. During the entering or leaving process, the ECDSA Algorithm is applied to HS.

The aim is to apply the ECDSA technique by reducing the key length and also by using the XNOR feature to minimise key duration. The digital signature technique cannot be directly applied through the connection and exit node. The size of the key is therefore reduced and the security is increased only if a digital signature technique is applied and the protocol behaves differently according to the digital signature procedure. The CP scheme, i.e. the formulation of the HS theory, offers a straightforward path for the resolution of the problem. The cluster-based HS theory, as defined in the last part, is used for the CP algorithm in the cloud sense. The new re-encryption method is based mathematically on an enhanced proxy re-encryption technique.

A cooperative generation of two protocol entities is the main generation term used by GKMP. There are many main algorithms for use in GKMP which can be used (i.e., RSA, Diffie-Hellman, elliptic curves). Many of them use asymmetric key technology to transmit information between two individuals in order to create a single encryption key. Besides protocols like GKMP, hierarchical tree-based and flat-tabling structures can be used for unified community key management systems.

In [2] the proposed group rekey approach uses the Chinese Remainder theorem to construct a stable lock to lock the group decryption key. Since the lock is common to all of the valid members, the decryption key transmission efficiency is $O(1)$. This system, however, has problems with the scalability.

There is an agency called the Central Authority (CA) in central group key management schemes which maintains a dynamically changing group of members by carrying out operations that include but not limited to allocating uniquely secret keys to members, maintaining the common Data Encryption Key among members and ensuring and holding group confidentiality in the Each member of the group has a unique identity. For e.g., this designation can be the identity of the member itself in the case of the ID-based systems.

GKM consists of initially setting up a community key at an abstract level and management it throughout the group's lifespan. We mean operations undertaken by the CA by management to maintain the group desired protection assets. The CA broadcasts in centralised schemes a chip text that the community members decode in order to acquire the key, streamlined to protect the key transport. A standalone rudimentary cryptographic that achieves this is a central encapsulation system with multiple receivers.

4. PERFORMANCE ANALYSIS

The key aim of this research is to improve cloud protection via the GKMP protocol. We implemented the HS principle with an updated ECDSA algorithm over GKMP.

Initially, 10 nodes is checked for the results and the algorithm is tested for the amount of time between nodes. The St is also measured without CP and success to reach the network took much longer than with CP. It also requires more time.

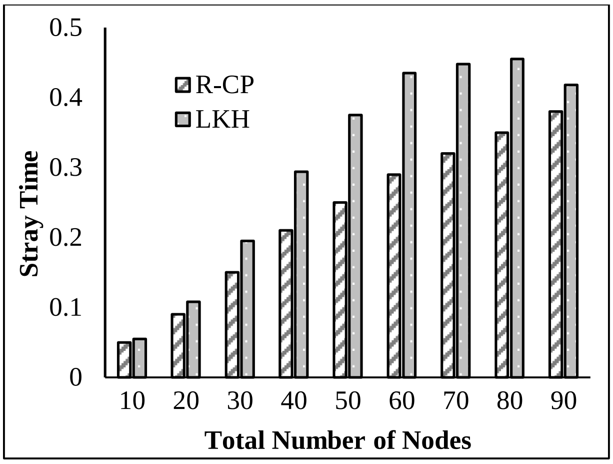

Fig.1. Delay over Cluster Nodes

The connectivity of clusters is considered significant during the initialization process. However, the degree of motility immediately varies between specified speeds when the first member is joined. The findings have shown that the connectivity rate declines steadily as clusters grow at a steady speed of 15 m/s and vice versa.

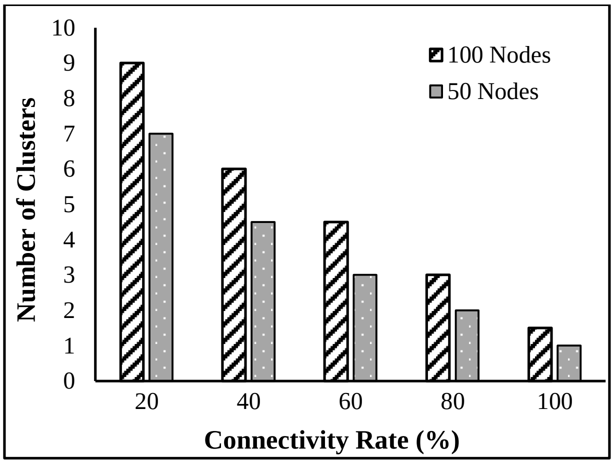

Fig.2. Total clusters connected

It is known that the machine times of the CP method are comparable to other strategies in terms of tree height. The traditional schemes differ with increasing nodes in the tree. This indicates that the scheme is stronger than other schemes in terms of computing time.

5. CONCLUSION

This CP methodology is a consistent approach to the issue of protection and overhead. The principle of the hyper-sphere implementation of clusters performed great. The use of the digital encryption technique has strengthened authentication and protection capabilities during the key agreement and re-keeping period. The reduced key size and the authentication of messages through hidden media showed how effective research is. This should be allowed. It then reduces overhead and improves easy, powerful cloud-based security technologies. The suggested CP scheme could be used for the enhancement of network architecture scalability in other protocols in IoT and big data environments.

REFERENCES

[1] Bing Wang, Yao Zheng, Wenjing Lou and Y. Thomas Hou, "DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking", *Computer Networks*, Vol. 81, No. C, pp. 308-319, 2015.

[2] Joseph Idziorek and Mark Tannian, "Exploiting Cloud Utility Models for Profit and Ruin", *Proceedings of IEEE International Conference on Cloud Computing*, pp. 33-40, 2011.

[3] J. Idziorek, M. Tannian and D. Jacobson, "Detecting Fraudulent use of Cloud Resources", *Proceedings of 3rd ACM Workshop on Cloud Computing Security*, pp. 61-72, 2011

[4] Joseph Idziorek and Mark Tannian, "Exploiting Cloud Utility Models for Profit and Ruin", *Proceedings of IEEE International Conference on Cloud Computing*, pp. 33-40, 2011.

[5] Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom and Tai-Myoung Chung, "Multi-Level Intrusion Detection System and Log Management in Cloud Computing", *Proceedings of International Conference Advanced Communication Technology*, pp. 552-555, 2011.

[6] L.A. Nivedita and K. Sravani, "Effective Service Security Schemes in Cloud Computing", *International Journal of Computational Engineering Research*, Vol. 3, No. 2, pp. 2250-3005, 2012.

[7] K. Goyal and P. Supriya, "Security Concerns in the World of Cloud Computing", *International Journal of Advanced Research in Computer Science*, Vol. 4, No. 4, pp. 976-997, 2013.

[8] Tao Xiang, Jia Hu and Jianglin Sun, "Outsourcing Chaotic Selective Image Encryption to the Cloud with Steganography", *Digital Signal Processing*, Vol. 43, pp. 28-37, 2015.

[9] P. Puzio, R. Molva, M. Onen and S. Loureiro, "Perfect Dedup: Secure Data Deduplication", *Proceedings of International Conference on Data Privacy Management, and Security Assurance*, pp. 150-166, 2015.

[10] P. Priyadharsini, P. Dhamodran. And M.S. Kavitha, "A Survey on De-Duplication in Cloud Computing", *International Journal of Computer Science and Mobile Computing*, Vol. 3, No. 11, pp. 149-155, 2014.

[11] G.U. Devi and G. Supriya, "Encryption of Big Data in Cloud using De-duplication Technique", *Research Journal of Pharmaceutical Biological and Chemical Sciences*, Vol. 8, No. 3, pp. 1103-1108, 2017.

[12] R. Shobana, K.S. Shalini, S. Leelavathy and V. Sridevi, "DeDuplication of Data in Cloud", *International Journal of Chemical Sciences*, Vol. 14, No. 4, pp. 2933-2938, 2016.