Journal of Engineering and Applied Sciences 11 (3): 384-389, 2016
ISSN: 1816-949X
© Medwell Journals, 2016

Enhance Data Transferred Security in Cloud Using Combination of Dynamic Eventual Batch Rekeying with DHKE and AES Encryption Algorithm

[1,4]Sura Khalil Abd, [1]S.A.R Al-Haddad, [1]Fazirulhisyam Hashim,
[2]Azizol B HJ Abdullah and [3]Salman Yussof
[1]Department of Computer and Communication System Engineering,
University Putra Malaysia, UPM, Selangor, Malaysia
[2]Department of Computer Science and Information Technology, Selangor, Malaysia
[3]College of Engineering, University of Diyala, Diyala, Iraq

Abstract: In this study, we present an enhancement of data transferred security mechanism in the cloud. We suggest providing a secret key that is exchanged securely between cloud server and cloud group members. This secret key is used to encrypt data transferred using symmetric encryption. Furthermore, batch rekeying method will be applied to develop a rekeying technique for securing group communication in cloud applications. The proposed rekeying technique will be designed to have the following properties: improve system efficiency by reducing the percentage of wasted computing resources and reducing the number of message signing, eliminate out-of-synchronization problem and ensure forward and backward secrecy.

Key words: Message, group, secret, cloud, batch

INTRODUCTION

Privacy and data confidentiality are the most critical open security issues in cloud, recently. Cloud users have some concerns when they trust service providers to store their sensitive information. Where the information are located, who have the right to control it and if significant data can be accessed and utilized illegitimately are all questions that increase users concerns (Aceto *et al*., 2013). Commonly used security mechanism to access data is username and password pair. This pair guarantees only valid users can access data but can't guarantee securing data when it stored in cloud and flows through the network (Seo *et al*., 2014). Moreover, users sometimes create easy theft opportunities by using simple password rather than complex hard-to-crack one. Another risk faced by data storedin cloud is accidental data loss. This is possible as most cloud storage applications allowusers to share sensitive information, opening the door to common errorssuch as accidentally sending the document link to wrong person or modifying data by cloud service providers. Therefore, while data is being transferred on network, the foremost requirement is data security and the major threat is data hacking (Tari, 2014).

In cloud computing, multicast has been used successfully to afford an efficacious, optimum effort delivery service from a sender to large group of receivers. Therefore, protecting group communications considers a serious cloud issue (Sriprasadh and Pandithurai, 2013). To achieve this protection, a symmetric key, Group Key (GK), is used. GK is shared only by group members and distributed by a key server which provides GK management service. Messages can be decrypted and read only by group members as it transferred encrypted with GK (Govinda *et al*., 2013). Key is the vital part of the system; if the key is revealed to strangers, then the system would be in insecure scenario as it can be used by attackers to decrypt the transferred data. Therefore, security of key exchanged between the key server and the group members is another issue as it exchanged through unsecure communication channel (Yao and Zhao, 2014).

GK must be securely delivered to exclusively members participating in the group. This is difficult to be achieved as the group membership is very dynamic. Thus, GK should be changed and delivered to current members whenever the membership is changed. This process called rekeying. Rekeying guarantees backward secrecy if a member joins the group and forward secrecy if a member leaves. Rekeying process may waste network resources. For example, a group of nusers, initially distributing GK to all users requiresNmessages each encrypted with an individual key. The computation and communication costs are proportional to group size N. Thus, multicast

Corresponding Author: Sura Khalil Abd, Department of Computer and Communication System Engineering, University Putra Malaysia, UPM, Selangor, Malaysia

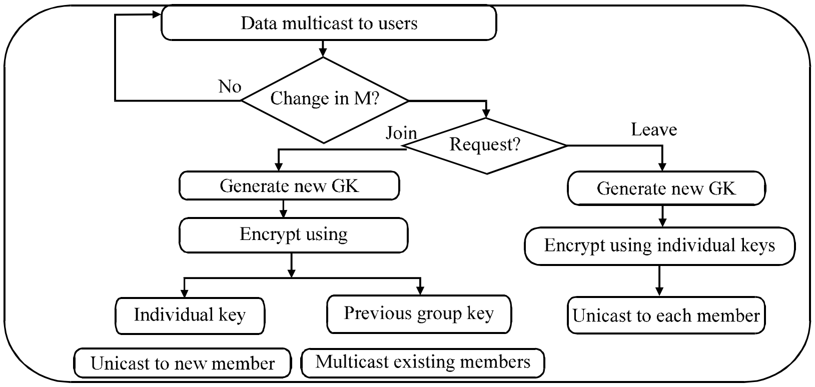

Fig. 1: Individual rekeying

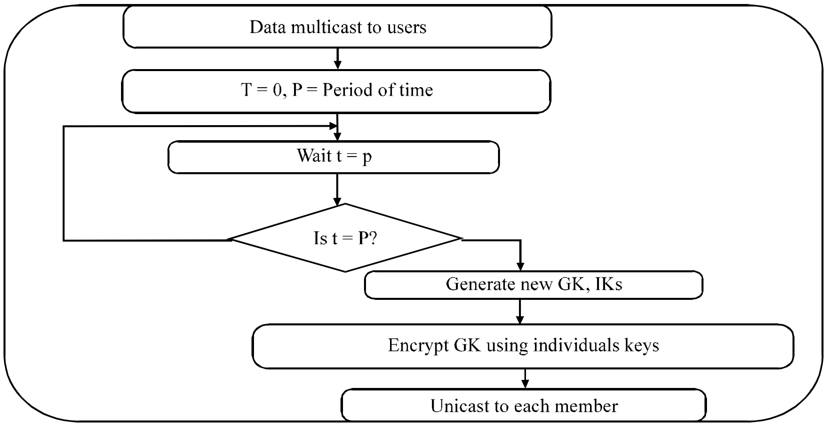

Fig. 2: Periodic rekeying

communication quality maybe affected (Li *et al*., 2012). In this study, we develop a rekeying scheme in a way that does not degrade the quality of multicast communication using batch rekeying.

Literature review: There are number of researchers who previously have showed their interest in security challenges faced by cloud computing presented proposals of improving data security in cloud (Xiao and Xiao, 2013; Dinadayalan *et al*., 2014; Tari, 2014; Tari *et al*., 2015). Besides their studies, our previous study Abd *et al*. (2014) presented new solutions in cloud security area mentioned the strength and the weaknesses for each proposed solution. In this syudy, we will discuss rekeying schemes focusing on its strengths and weaknesses points. Then, explained why batch rekeying is a better choice to be used in our proposed research.

Individual Rekeying (IR): In IR, GK is changed whenever members join or leave the group as shown in Fig. 1. In dynamic membership environment, IR may end up congesting the network as it creates numerous rekey messages whenever Membership (M) changes (Je *et al*., 2014). Two reasons make IR relatively inefficient. First, to obtain authentication, the rekey message has to be signed; otherwise, bogus rekey messages can be sent out by a compromised group member and the whole system can be messed up. Signing process will put a cumbersome load on the key server if it has to be done for every single request, especially when requests are frequent. Thus, signing operation is computationally expensive. Second, it is a squandering of server cost considering if a couple of departs register one after another. Key server will produce a new GK and auxiliary keys for these departs; nonetheless, they may temporally take place so close where the earliest group of new keys are not utilized and directly substituted by the next new group keys.

As a result, several keys may be created and handed out, never utilized in case of frequent requests (Li *et al*., 2009). Besides inefficiency, another challenge isout-of-synchronization between keys and data. A data message ciphered by an out dated GK or with a GK that has not yet been received by a user. Therefore,

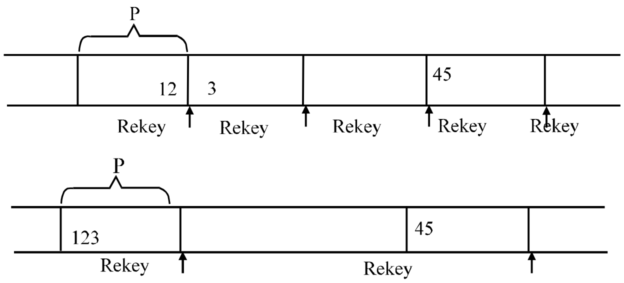

Fig. 3: Regular and eventual batch processing: a) Timestamp (regular); b) Timestamp (eventual)

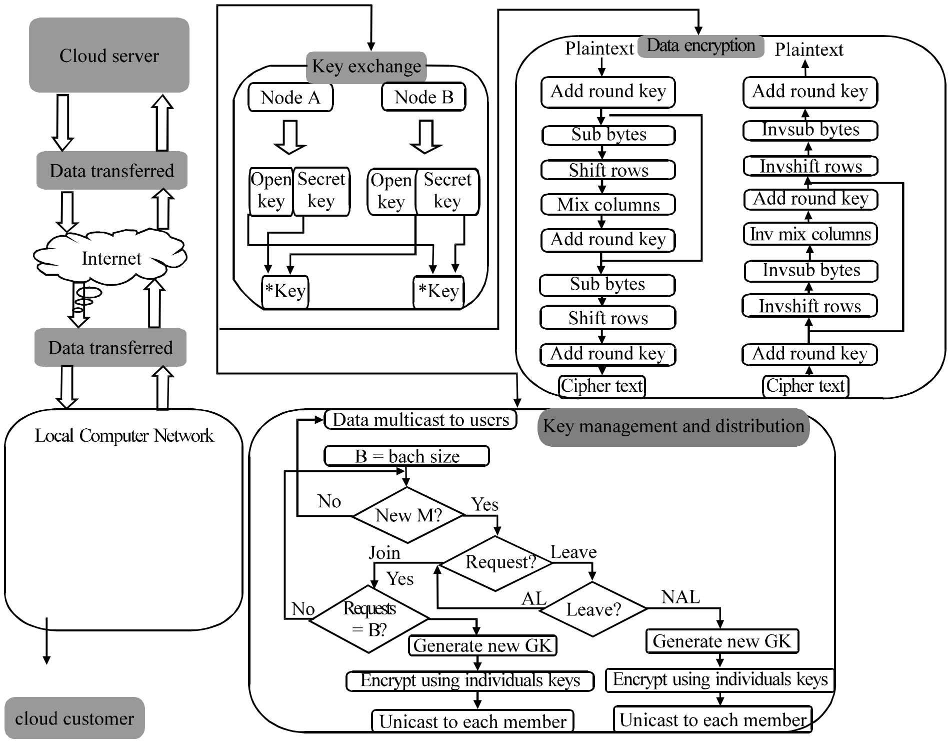

Fig. 4: System framework

users may need to keep multiple versions of GKs to decrypt the received messages, and a large buffer to keep data that cannot yet be decrypted due to unavailability of the proper group.

Periodic Rekeying (PR): In PR as shown in Fig. 2, GK is periodically changed and distributed regardless of membership change. PR in the group membership states which is very dynamic can avoid resource waste. The number of rekey messages to be signed is decreased: instead of one for each, it will be one for each period; therefore, system efficiency is improved. It also diminishes the probability of producing new keys that will not be utilized (Park *et al.*, 2014). However, it has vulnerable weak points in both the forward and backward secrecy as changing the key in this method is periodic, a new user can have the opportunity to read past communications and a departed user can read future communications. Malicious users can use these security gaps as an attack points. PR is also inappropriate in a static environment. Membership in this environment is hardly changed. As a result, resources can be wasted as PR periodically creates unnecessary rekey messages without any changing in group membership.

Batch Rekeying (BR): In this research, BR is proposed to solve previous rekeying techniques issues. In BR, arekey interval is the timeduration the key server waits to collect join and leave requests, create new keys, structure a rekey message and multicast the rekey message.The number of

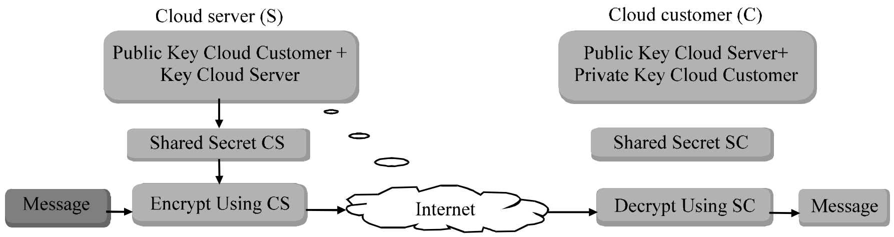

Fig. 5: Diffie-Hellman Key Exchange

rekey messages to be signed is decreased by BR to be one for a batch of requests. Therefore, it improves the efficiency of the system. It also diminishes the probability of producing new keys that will not be utilized as advantages of the possible overlap of new keys are taken for multiple rekey requests. BR alleviates out-of-sync problem as the rekey period is supposed to be bigger than the message delays; the authoritative delivery maximum delay of rekey messages and the data messages maximum delay are less than the rekey interval length (Veltri *et al*., 2013). As shown in Fig. 3, there are two schemes of batch processing member's request: Regular and Eventual BR. Regular BR processes a batch of user's requests utilizing queue to work with regular period regardless of their arriving time. Eventual BR processes a batch of user's requests during a fixed period at their arriving time (Lee *et al*., 2008).

The rekeying interval structure has two methods: static and dynamic. Static is simple, less flexible and can be defined as a fixed period of time repeated regularly regardless of members' requests. From the definition, it can be noticed that it is suitable to regular BR. Resource waste is the most important issue faced by this method. In static environment, unnecessary rekeying messages are created periodically with no change in group membership. On the other hand, rekeying will be processed when the number of requests, join or leave, reach a threshold, batch size, in dynamic method which saves resources in static environment. In general, group member's arrival and departure are completely random, collected cumulatively for a period of time and considers as a single (Vasanthi and Purusothaman, 2014).

MATERIALS AND METHODS

Our proposed reseqarch depends on cryptography techniques to secure both the key exchange process and the data transferred between the server or service center and the client in the cloud. Keys are exchanged securely between cloud server and users. Then, the shared secret key is used to encrypt data transferred using AES. Finally, to enhance security BR is utilized to change keys then multicast it to the users. As shown in Fig. 4, there are main stages t used to secure data transferred through cloud.

Key exchange: Each cloud customer should be provided with GK and IK. GK used to cipher data transferred from cloud server to customers. IK used to cipher data transferred from individual customer to cloud server. Security of key exchanged is the first stage of the proposed system. Diffie-Hellman Key Exchange (DHKE) is proposed to enable this secret exchanging. DHKE considers one of the most common techniques in computer networks to exchange keys securely between two nodes (Escala *et al*., 2015). As shown in Fig. 5, cloud server and cloud customer initiate a session to exchange their public keys. Then, each entity calculate a shared secret key using exchanged public key with its private one taking advantage of discrete log hard problems as a cryptography strength. The resulted shared secret key is used to encrypt and decrypt messages as explained next section. DHKE theoretically proven that it is secure if a proper size of keys is used.

Data encryption: The shared secret key produced from DHKE in previous section is used as a data cryptographic key using Advance Encryption Standard (AES). AES can be defined as a symmetric block cipher that can process data blocks of 128 bits utilizing cryptographic keys of 128, 192 and 256 bits such that the index attached to a bit falls in between the range $0 \leq i \leq 128$, $0 \leq i \leq 192$ or $0 \leq i \leq 256$, respectively (Rhee, 2003). All byte values of the AES are introduced by a vector notation which matches to a polynomial representation as:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum\nolimits^7_{i=1} b_ix^i$$

The full detailed explanation of AES round layers can be found by Daemen and Rijmen (2002).

RESULTS AND DISCUSSION

Key management and distribution: The third stage is managing key distribution and membership process. In our proposed research, cloud server multicast data to cloud members at once instead of send one copy for each which saves overall network bandwidth. Protected communication between members of a secure cloud group is supported by a Group Key Management (GKM) protocol. GKM ensures accessing to group data is gained only by secure group members. Hence, group data can be authenticated (Baddi and Kettani, 2013; Kori and Raghuwanshi, 2013). Thus, providing valid group members with the up-to-date cryptographic status required for secrecy and authentication. Thus, changing keys with membership changes, rekeying, is the goal of GKM. To achieve it, managing rekeying process becomes a main demand.

Eventual BR is proposed to manage keys changing. When there is a change in membership, first check if the change is a member join or leave. There are two types of leaving member: Authenticated Leave (AL) or Not Authenticated (NAL). AL is the member who decided to leave the group. NAL is the member who expelled from the group. In case leaving is NAL, then keys directly are changed to avoid backward secrecy issue. Generate new keys and unicast to each member. In case it AL, then batch size is check. If the member requests reach batch size threshold, then generate new keys and unicast to each member.

CONCLUSION

This paper concentrates on promoting cloud security by designing and developing mix cryptographic techniques to enhance security of data transferred between the service centre and the clients including integrity and confidentiality. To secure secret key exchanged between cloud and users, DHKE is suggested. Moreover, AES has been suggested to cipher the transferred data according to its speed, key size and its immunity against breakable. Furthermore, we develop a rekeying technique based on batch rekeying scheme for securing group communication in cloud applications. We proved theoretically that our proposed rekeying technique improves system efficiency by reducing the percentage of wasted computing resources, number of message signing, eliminate out-of-synchronization problem and ensure forward and backward secrecy.

ACKNOWLEDGMENTS

The research is supported by University Putra Malaysia Grant GP-IPS/2015/9462000.

REFERENCES

Abd, S.K., S.A.R. Al-Haddad, F. Hashim and A. Abdullah, 2014. A review of cloud security based on cryptographic mechanisms. Proceedings of the International Symposium on Biometrics and Security Technologies, August 26-27, 2014, Kuala Lumpur, Malaysia, pp: 106-111.

Aceto, G., A. Botta, W. De Donato and A. Pescape, 2013. Cloud monitoring: A survey. Comput. Networks, 57: 2093-2115.

Baddi, Y. and M.D.E.C. El Kettani, 2013. Key management for secure multicast communication: A survey. Proceedings of the National Security Days Meeting, April 26-27, 2013, Rabat, Morocco, pp: 1-6.

Daemen, J. and V. Rijmen, 2002. The Design of Rijndael: AES-The Advanced Encryption Standard. Springer, New York, USA., ISBN-13: 978-3540425809, Pages: 255.

Dinadayalan, P., S. Jegadeeswari and D. Gnanambigai, 2014. Data security issues in cloud environment and solutions. Proceedings of the World Congress on Computing and Communication Technologies, February 27-March 1, 2014, Trichirappalli, India, pp: 88-91.

Escala, A., G. Herold, E. Kiltz, C. Rafols and J. Villar, 2013. An algebraic framework for Diffie-Hellman assumptions. Proceedings of the 33rd Annual Cryptology Conference on Advances in Cryptology, August 18-22, 2013, Santa Barbara, CA., USA., pp: 129-147.

Gao, J., D. Hu, Y. Wang and Z. Yang, 2007. An efficient rekeying approach for secure multicast communication. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, September 21-25, 2007, Shanghai, China, pp: 1949-1953.

Govinda, K., E. Sathiyamoorthy and S. Agarwal, 2013. Secure key exchange for cloud environment using cellular automata with triple-DES and error-detection. Int. J. Eng. Technol., 5: 1004-1009.

Je, D.H., H.S. Kim, Y.H. Choi and S.W. Seo, 2014. Dynamic configuration of batch rekeying interval for secure multicast service. Proceedings of the International Conference on Computing, Networking and Communications, February 3-6, 2014, Honolulu, HI., USA., pp: 26-30.

Kori, N.K. and S. Raghuwanshi, 2013. An efficient key management approach for multicasting supported networks. Proceedings of the International Conference on Green Computing, Communication and Conservation of Energy, December 12-14, 2013, Chennai, India, pp: 905-908.

Lee, H., B. Rhee, E. Kim and S. Han, 2008. User-oriented batch processing of individual rekeying. Proceedings of the International Conference on Information Science and Security, January 10-12, 2008, Seoul, South Korea, pp: 38-43.

Li, B., J. Pan, G.P. Li, M.K. Han and Y. Fu, 2009. A secure and efficient distributed batch rekeying protocol for dynamic collaborative groups. Proceedings of the International Conference on Information Engineering and Computer Science, December 19-20, 2009, Wuhan, China, pp: 1-4.

Li, B., Y. Yang, Z. Lu, B. Yuan and T. Long, 2012. Secure distributed batch rekeying algorithm for dynamic group. Proceedings of the IEEE 14th International Conference on Communication Technology, November 9-11, 2012, Chengdu, China, pp: 664-667.

Park, Y.H., D.H. Je, M.H. Park and S.W. Seo, 2014. Efficient rekeying framework for secure multicast with diverse-subscription-period mobile users. IEEE Trans. Mobile Comput., 13: 783-796.

Rhee, M., 2003. Internet Security: Cryptographic Principles, Algorithms and Protocols. John Wiley and Sons, UK., ISBN-13: 9780470862469, pp: 107-111.

Seo, S.H., M. Nabeel, X. Ding and E. Bertino, 2014. An efficient certificateless encryption for secure data sharing in public clouds. IEEE Trans. Knowledge Data Eng., 26: 2107-2119.

Sriprasadh, K. and O. Pandithurai, 2013. A novel method to secure cloud computing through multicast key management. Proceedings of the International Conference on Information Communication and Embedded Systems, February 21-22, 2013, Chennai, India, pp: 305-311.

Tari, Z., 2014. Security and privacy in cloud computing. IEEE Cloud Comput., 1: 54-57.

Tari, Z., X. Yi, U.S. Premarathne, P. Bertok and I. Khalil, 2015. Security and privacy in cloud computing: Vision, trends and challenges. IEEE Cloud Comput., 2: 30-38.

Vasanthi, A. and T. Purusothaman, 2014. Optimizing batch rekeying interval for secure group communication based on queuing model. J. Comput. Sci., 10: 325-329.

Veltri, L., S. Cirani, G. Ferrari and S. Busanelli, 2013. Batch-based group key management with shared key derivation in the internet of things. Proceedings of the 9th International Wireless Communications and Mobile Computing Conference, July 1-5, 2013, Sardinia, pp: 1688-1693.

Xiao, Z. and Y. Xiao, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutorials, 15: 843-859.

Yao, A.C.C. and Y. Zhao, 2014. Privacy-preserving authenticated key-exchange over internet. IEEE Trans. Inform. Forensics Secur., 9: 125-140.