Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9490-9495, 2017
ISSN: 1816-949X

Data Security Using Odd-Even Threshold Cryptography in Cloud Computing

D. Kosare and D. Naidu
Department of Computer Science Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India

Abstract: The malicious insider may be an employees, user or cloud service provider. In cloud environment, data owner may store diplomatic data of their organization in cloud storage. The cloud service provider should guarantee integrity, security, access control and confidentiality about the stored data at cloud. The malicious insiders can conduct burglary on sensitive data at cloud storage. Most of the organizations pay no attention the insider attack because it is harder to detect and mitigate. This is a major emerging problem in organizations. In order to tackle these issues we proposed odd-even threshold cryptography scheme at users side in which data owner divides users in groups and further groups are divide into two user groups (i.e., odd and even user groups) and gives single key to each user groups for decryption of data. Distributed parallel processing is applied on two groups (i.e., odd and even user groups) for simultaneously performing two decryption processes. The main features of this scheme is that data are prohibiting from malicious insider attack, also, reduce the number of security key and decryption process time.

Key words: Cloud computing, malicious insider attacks, decryption, prohibiting, emerging, time

INTRODUCTION

Cloud computing is a computing model, distributed on large scale in which small area of computing resources is available to users through the internet and it also provides storage and computing services at a very low cost, so it has gain popularity in various organizations and institutions. The storage of terabyte data, generated by everyday is the biggest requirement of an IT industry. Thus, to meet this requirement it requires many of hardware, software and network infrastructures. Cloud computing solve this problem in cost effective manner. It has completely changed the structure not only IT industry but some other sectors like education, healthcare sector. Cloud computing is growing very rapidly because of their features like resource capability, network infrastructure, storage capability, cost effective, quick access of information. The main characteristics of cloud computing are: remotely hosted, ubiquitous, resiliency, on-demand self service, rapid elasticity, broad network access, full managed by the provider. On other side all data is virtual and cloud is as open services and they make use of public network for their application and services which are questionable regarding security issues. Data security is a prime obstacle in the way of cloud computing. People are still fearing to exploit the cloud computing. Some people believe that cloud is not a safe place and once you send your data to the cloud, you lose complete authority over it. They are more or less right. Data of data owners are taken care and stored at external servers. So, confidentiality integrity and access of data become unprotected. Since, external servers are operated by commercial service providers, data owner can't trust on them as they can use data for their profits and can destroy businesses of data owner. Data owner even can't trust on users as they may be mischievous. Data confidentiality may violet through collusion attack of mischievous users and service providers. Some approaches are given to ensure these security requirements but they are lacked in some ways such as violation of data confidentiality due to collusion attack and heavy computation (due to large no keys).

To address these issues based paper propose a scheme that uses odd-even threshold cryptography scheme in which data owner divides users in groups and further groups are divide into two user groups (i.e., odd and even user groups) and gives single key to each user groups for decryption of data. Distributed parallel processing is applied on two groups (i.e., odd and even user groups) for simultaneously performing two decryption processes. This scheme not only provides the strong data confidentiality but also reduces the number of keys. Proposed scheme is more secure and reduces number of keys.

Literature review: Data confidentiality and access control are two major security requirements in cloud computing. Sometimes, more importance is given to security of data thus, forgetting the performance of system. For instance, we sometimes use too many keys for data security. As the

Corresponding Author: D. Kosare, Department of Computer Science Engineering,
Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India

keys are confidential there is a need to secure and maintain keys which itself is a additional work. Thus, it affects the performance of the system. So, reducing number of keys become more essential. This problem is solved by introducing scheme that provide not only data security but at the same time maintain the performance. An overall related works is presented here.

Yong and Zhen (2007) presented a scheme is the group-key scheme. In this study group-key agreement scheme is used. This scheme construct the session key by sharing equally contributed information from every group member and permit group members to agree on a session key to secure their communication. There is a single key similar to each group of users for decryption process and all users of the group know that key. Here, number of keys is reduced but there is a problem of collusion attack of CSP and a user because a single malicious user can break whole data of the group to CSP. We know that CSP party is not trust worthy. It can make use of data owner's data for its commercial profits.

Sanka *et al*. (2010) presented a exhausted to achieve data confidentiality. In this study, symmetric key and capability list scheme tried to achieve data confidentiality and access control. In this scheme, data are encrypted by symmetric keys and symmetric keys are known only to data owner and corresponding data users. CSP is use as storage Medium for the encrypted data. Since, the stored data are encrypted; CSP is unable to see it. Data are further encrypted by one time secrete session-key shared between CSP and user by the Diffie-Hellman protocol to protect data from outsiders during the transmission between CSP and user. This scheme no doubt provides the whole data security but there is associated a key corresponding to each user and users may be large in number in some applications. So, number of keys increases. These in turn increase the maintenance as well as security concern of key. So, as to secure the data we sometimes make use of so many keys. This extra work affect the system's performance, so, it is recommendable to reduce number of keys.

Sathishkumar and Ramesh (2016) presented a flooding based protocol. Black hole attack is a serious security problem to be solved for active delivery of packets of data in Mobile Ad-Hoc networks. In this problem, a malicious node uses routing protocol to promote itself as having the shortest path to the node whose packets it wants to snatch.

Sagar and Kumar (2015) tried to achieve data authentication.in this study threshold cryptography scheme is used. In threshold cryptography, basically there are three entities: data owner, cloud service provider and many users associated with data owner. Users are divided in groups on some basis such as location, project and department and corresponding to each group, there is a single key for encryption and decryption of data. Parts of the key are distributed among the each user in the group. Data can be decrypted when at least threshold number of users will present. This scheme not only provides data confidentiality but also reduces the number of keys. This scheme is best for preventing data security from collusion attack of malicious users and service providers and also maintains the system performance. But this technique takes more time for decryption process.

Harit *et al*. (2012), they explains threshold signature which can evict the misbehaving node from vehicular ad hoc network by maintaining the properties of public key infrastructure architecture.

Bennani *et al*. (2010), they put forward the idea of using the cloud for decoupling the management of local, user-specific encryption keys from the one of role-specific protection keys, obtaining simple key management and revocation schemes.

Chachapara and Bhadlawala (2013) tried to convey about cloud where they have focused on adding new functionality for cloud providers that is secure sharing.

Shi *et al*. (2011) tried to acheive cost effective parallel processing would become a required skill. This paper reports a resource planning study using a method derived from classical program time complexity analysis, we call timing models. Basically this will help in improving time efficiency of proposed model.

MATERIALS AND METHODS

Cloud computing: In today's world most companies want to store and retrieve data and cloud computing helps to make their job more flexible and easy. Also, the cost of storing huge amount of data will be minimal compared to storing the data physically or in an external device. Besides the benefits of cloud computing there are certain disadvantage which cloud faces are regarding the security issues because to maintain data privacy, confidentiality and integrity. Moreover, as cloud service provider has a complete control on the infrastructure, so, security risk like manipulating or stealing of code by service provider exist.

Figure 1 explains us how data is accessed from the cloud and how an unauthorized entity can access our private content. So, how to prevent private data from unauthorized users and insider attack. One of the best solutions for preventing private data from unauthorized user is to divide the secret among the employees. So, he/she can't alone access the private data.

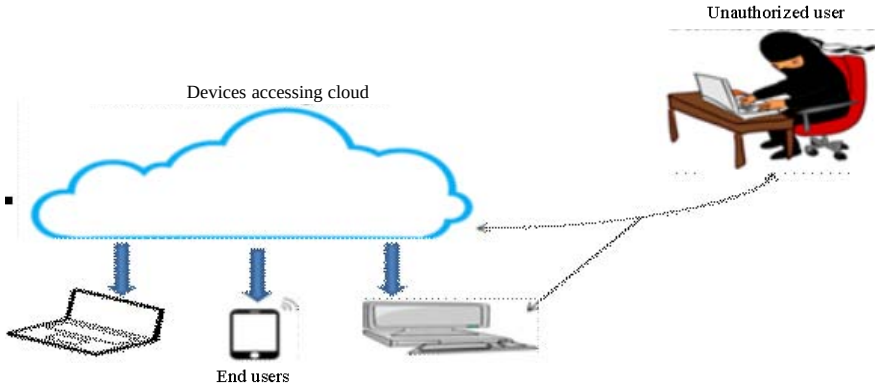

Fig. 1: Security barrier in cloud computing

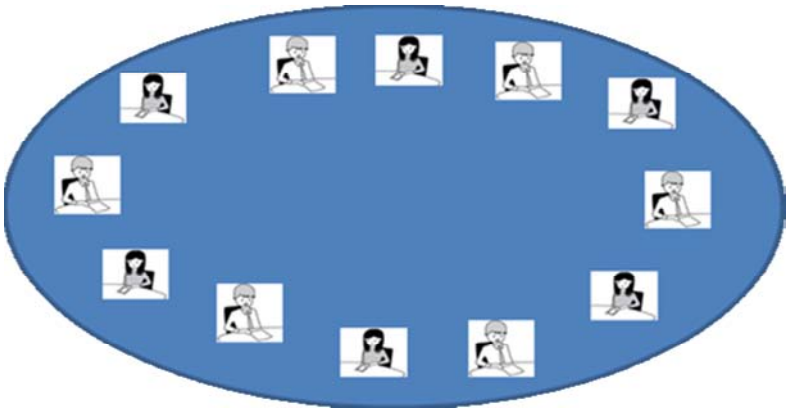

Fig. 2: Organization of 12 employees

Consider below example: In one organization, there are 12 employees are working on a secret project. They wish to lock up the documents in a drawer so that the drawer can be opened if and only if six or more of the employees are present. Figure 2 describes the example of organization.

So, the question is what is the smallest no, of locks needed? And what is the smallest number of keys to the locks each employee must carry? If you choose any 6 employees and for any chosen 6 employees you keep a dedicated lock. So that, means the number of locks which are needed or the number of ways how you can actually choose 6 from 12:

$$\text{Minimum number of locks} = 12C6\frac{12!}{6!\times 6!} = 924$$

Smallest number of keys to the locks each employee must:

$$\text{Carry} = 11C5 = \frac{11!}{5!\times 6!} = 462$$

Therefore, you see that even for a small employee which has got 12 employee and we want a scheme where 6 employees if they combine, they can understand or deduce the secret. But this kind of scheme requires very large number of locks and keys. Hence, the objective of developing an efficient secret sharing scheme is to find out a mechanism, through which you can actually divide the secret amongst n employee. Such that, out of them, if t employee where t<n, if they combine, they should be able to find out the secret but the scheme should be efficient which means that the number of locks or the number of key should be small that means ,the computational it should be as minimum as possible.

RESULTS AND DISCUSSION

Proposed scheme: There are some drawbacks of the existing system. These drawbacks are overcome in the proposed system by using the concepts of odd-even threshold cryptography on user side. To understand proposed scheme better we take an example of real life scenario.

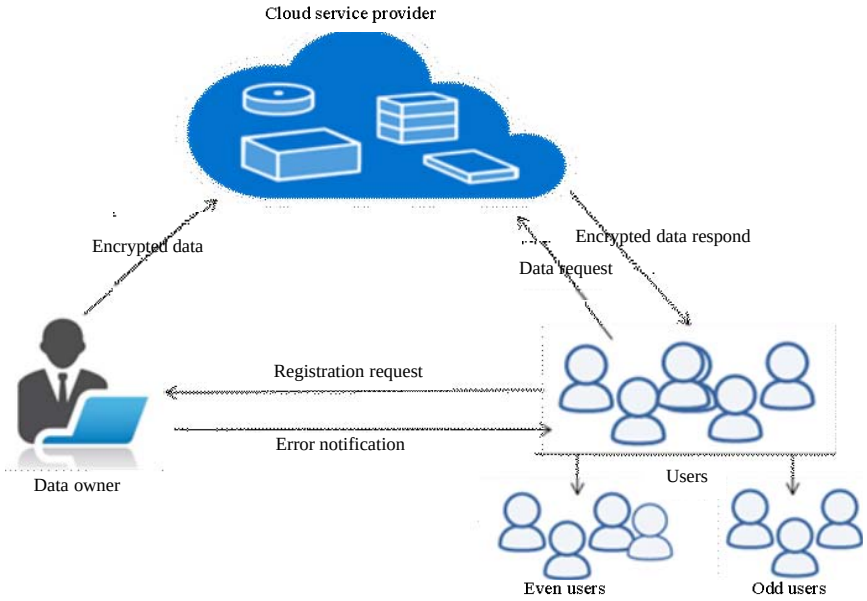

Fig. 3: System architecture

In Fig. 3, there are three entities that is Data Owner (DO), users and Cloud Service Provider (CSP). Data Owner (DO) may be a software industry who stores its data on to the Cloud Service Provider (CSP) and the users may be its employees who view their data from the CSP. Data owner divides users in groups on some basis such as designation basis and further groups are divide into two user groups (i.e., odd and even user groups) and gives single key to each user groups for decryption of data. At the beginning, DO register all the users. During registration users send their personal information to DO. DO then encrypts the original file by using AES algorithm and send those encrypted file to CSP. Confidentiality and authentication are guaranteed between DO and CSP, by this encryption. After receiving encrypted file from DO, the CSP stores encrypted file in its storage. User then send request for file to CSP. CSP then check whether the user is authentic or not. If user is authentic then CSP send the requested file to the user. After getting encrypted file from CSP. Then user main concern how to decrypt the file because he/she does not decrypt file alone. At user side, we use odd-even threshold cryptography scheme for file decryption process. In this scheme, data owner divide users into groups and those groups are further divided into odd-even user groups and gives single key to each user groups for decryption of data.

At a time only two users (i.e., odd user and even user) can access the same file of one group. So, collusion attacks are not arising. By using polynomial technique we divide the secret key into n parts and using lagrange polynomial technique we reconstruct the secret key. Hence, unauthorized user can not access private data from the cloud because he/she must take part of the secret key from remaining users of the same group. And also, it reduces decryption process time by dividing users into two groups.

Odd-even threshold cryptography: Goal of this scheme; divide a secret D into n pieces $D_1, ..., D_n$ in way that:

- Knowledge of any t or more D_i pieces make D easily computable
- Knowledge of any t-1 or fewer D_i pieces leaves D completely undetermined (i.e., all possible value of D are equally likely)

There are five important components in odd-even threshold cryptography.

Secret: Secret is a secret message or number that you want to share with other securely.

Share: Share is a piece of secret. Secret is divided into pieces and each piece is called share. It is computed from given secret, you need to get certain number of shares.

Threshold: Threshold is the number of shares you need at least in order to recover your secret. You can restore your secret only when you have more than or equal to the number of threshold.

Polynomial: Using polynomial equation, we generate shares. Suppose your threshold value is 4 (t = 4), then always take polynomial degree is t-1 means 3:

Table 1: Odd and even users groups

Odd users group		Even users group	
Users	Part of secret key (share)	Users	Part of secret key (share)
1	59377	2	59432
3	59513	4	59620
5	59753	6	59912
7	60097	8	60308

$$a(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$

Lagrange interpolation: Using lagrange interpolation formula, we reconstruct the original secret key which is shares among the group of users:

$$L(x) = \sum_{j=0}^{t} y_j l_j$$

$$l_j = \prod_{\substack{0 \le m \le t \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

Mathematical derivation of odd-even threshold cryptography: Let Data Owner select n = 8 (a group of 8 users) and t = 3:

$$x_i = i, 1 \le i \le 8$$

Let select secret s = 59348. The data owner chooses two secret coefficient a_2 = 13 and a1 = 16 are used to produce the polynomial. The coefficient a_0 = 59348 is the secret. Therefore, by using polynomial we generate shares and part of secret key. Here, t = 3. So, polynomial highest degree is t-1, i.e., 2.

Generate share:

$$a(x) 13x^2 + 16x + 59348$$

Eight shares and eight part of secret key are obtained from the polynomial: (1, 59377); (2, 59432); (3, 59513); (4, 59620); (5, 59753); (6, 59912); (7, 60097); (8, 60308). So, that, each users can get eight different part of the secret key. Now, these users are divided into two groups, i.e., (Table 1).

To reconstruct the secret: In order to reconstruct the secret S, t users will be enough from both groups (i.e., odd and even group). Here, t = 3. So, we take any 3 users from odd group, i.e. (3, 59513); (5, 59753); (7, 60097). It is possible to construct α (x) by using Lagrange's polynomial and the value of S can also be derived. Let us consider (x_0, y_0) = (3. 59513); (x_1, y_1) = (5, 59753); (x_2, y_2) = (7, 60097). Lagrange's polynomials can be computed as:

For odd user group:

$$l_0 = \frac{x-x_1}{x_0-x_1}.\frac{x-x_2}{x_0-x_2} = \frac{x-5}{3-5}.\frac{x-7}{3-7} = \frac{1}{8}x^2 - 1\frac{1}{2}x + 4\frac{3}{8}$$

$$l_1 = \frac{x-x_0}{x_1-x_0}.\frac{x-x_2}{x_1-x_2} = \frac{x-3}{5-3}.\frac{x-7}{5-7} = \frac{1}{4}x^2 - 2\frac{1}{2}x - 5\frac{1}{4}$$

$$l_2 = \frac{x-x_0}{x_2-x_0}.\frac{x-x_2}{x_2-x_2} = \frac{x-3}{3-7}.\frac{x-5}{7-5} = \frac{1}{8}x^2 - x + 1\frac{7}{8}$$

$$L(x) = \sum_{j=0}^{2} y_j l_j(x)$$

$$L(x) = 59513.\left(\frac{1}{8}x^2 - 1\frac{1}{2}x4\frac{3}{8}\right) + 59753$$

$$\left(-\frac{1}{4}x^2 + 2\frac{1}{2} - 5\frac{1}{4}\right) + 60097.\left(\frac{1}{8}x^2 - x + 1\frac{7}{8}\right)$$

$$= 13x^2 + 16x + 59348$$

For even user group: Let us consider for even user (x_0, y_0) = (2, 59432); (x_1, y_1) = (4, 59620); (x_2, y_2) = (6, 59912).

$$l_0 = \frac{x-x_1}{x_0-x_1}.\frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4}.\frac{x-6}{2-6} = \frac{1}{8}x^2 - 1\frac{1}{4}x + 3$$

$$l_1 = \frac{x-x_0}{x_1-x_0}.\frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2}.\frac{x-2}{4-6} = \frac{1}{4}x^2 - 2x - 3$$

$$l_2 = \frac{x-x_0}{x_2-x_0}.\frac{x-x_2}{x_2-x_2} = \frac{x-2}{6-2}.\frac{x-4}{6-4} = \frac{1}{8}x^2 - \frac{3}{4}x + 1$$

$$L(x) = \sum_{j=0}^{2} y_j l_j(x)$$

$$L(x) = 59432.\left(\frac{1}{8}x^2 - 1\frac{1}{4} + 3\right) + 59620.$$

$$\left(-\frac{1}{4}x^2 + 2x - 3\right) + 59912.\left(\frac{1}{8}x^2 - \frac{3}{4}x + 1\right)$$

$$= 13x^2 + 16x + 59348$$

Remember that the secret is the free coefficient which means that S = 59344.

CONCLUSION

In this study, we discussed the need for security from unauthorized users in cloud computing environment and a new approach for preventing private data from unauthorized users. There have a lot of work already been done for providing security to clouds and users side. Also provide authenticated user and services but in this study a novel approach based on threshold cryptography using odd and even concept have been given for a strong and more secure protocol. This approach is also useful for time efficiency. The proposed scheme is useful for those applications where works are done in team and group

such as in software industries. You may think proposed scheme has limited applications but it is not as such. It is applicable all where you can group users on some basis and can apply odd-even threshold cryptography technique. Such as software and hardware industries institutes, banks, university and medicals fields.

RECOMMENDATION

In future another framework can also be used to provide more security to cloud environment.

REFERENCES

Bennani, N., E. Damiani and S. Cimato, 2010. Toward cloud-based key management for outsourced databases. Proceedings of the IEEE 34th Annual Workshops on Computer Software and Applications (COMPSACW'10), July 19-23, 2010, IEEE, Seoul, Korea, ISBN:978-1-4244-8089-0, pp: 232-236.

Chachapara, K. and S. Bhadlawala, 2013. Secure sharing with cryptography in cloud computing. Proceedings of the 2013 Nirma University International Conference on Engineering (NUiCONE'13), November 28-30, 2013, IEEE, Ahmedabad, India, ISBN:978-1-4799-0725-0, pp: 1-3.

Harit, S.K., S.K. Saini, N. Tyagi and K.K. Mishra, 2012. RSA Threshold signature based node eviction in vehicular aad hoc network. Inf. Technol. J., 11: 980-988.

Sagar, V. and K. Kumar, 2015. A symmetric key cryptography using genetic algorithm and error back propagation neural network. Proceedings of the 2nd International Conference on Computing for Sustainable Global Development (INDIACom'15), March 11-13, 2015, IEEE, New Delhi, India, ISBN:978-9-3805-4415-1, pp: 1386-1391.

Sanka, S., C. Hota and M. Rajarajan, 2010. Secure data access in cloud computing. Proceedings of the 2010 IEEE 4th International Conference on Internet Multimedia Services Architecture and Application (IMSAA'10), December 15-17, 2010, IEEE, Bangalore, India, ISBN:978-1-4244-7930-6, pp: 1-6.

Sathishkumar, R. and C. Ramesh, 2016. A modified method for preventing black-hole attack in mobile Ad Hoc networks. J. Eng. Appl. Sci., 11: 182-191.

Shi, J.Y., M. Taifi and A. Khreishah, 2011. Resource planning for parallel processing in the cloud. Proceedings of the 2011 IEEE 13th International Conference on High Performance Computing and Communications (HPCC'11), September 2-4, 2011, IEEE, Banff, Alberta, Canada, ISBN: 978-1-4577-1564-8, pp: 828-833.

Yong, Z.H. and H. Zhen, 2007. An efficient authenticated group key agreement protocol. Proceedings of the 41st Annual IEEE International Carnahan Conference on Security Technology, October 8-11, 2007, IEEE, Ottawa, Canada, ISBN:978-1-4244-1129-0, pp: 250-254.