Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey of Secret Sharing Algorithm for Multiparty Authentication in Cloud Computing

Rashmi Nigoti[*] , Dr. Shailendra Singh

NITTTR Bhopal

India

Abstract—Cloud computing is s major area of research because, now a day's everyone is moving toward the cloud. Cloud computing have many advantages, but also have security risks which requires a new security algorithm for multi parties. In this paper we reviews threshold cryptography, Secret Sharing Schemes (SSS) for cloud computing, and lastly suggested scenario where we are using secret sharing scheme for multi-party authentication for cloud computing. In multi-party authentication, out of n-servers k servers are authenticated and shares from these servers are selected based on some trust function which uses some parameters for calculating trust value of each server. These parameters are updated each time a client communicates to the server.

Keywords— Cloud; threshold cryptography; sharing secret scheme; multi-party authentication; trust function.

I. Introduction

This document is a template. By using cloud computing, many companies can significantly decrease their IT expenditure. There is a lot of merits of cloud computing which facilitate the companies to adopt cloud computing, in addition security is a major barrier, because employees can access data easily, alter it, and disclose the data. Sometime such activities can harm for a big and famous company. In such situation, security has a major role than in classical network. Security issues in the cloud include application security, data security, middleware security, network security, storage security and Virtualization Security. The main goal is to securely store and manage data that is not controlled by the owner of the data [2]. The most important fear about data while at rest and in transit are unauthorized access, data alteration, and theft. The protection methods include encryption, providing different access levels to enable access control to the data, and integrity check by hashing, etc.

Applications require offer access only to authenticated and authorized users, and those users have to trust that their data is out of harm's way. Security must be incorporated with every phase of an application and its deployment and development and operational architecture. There are many cryptographic algorithms which may be used for encryption, but the main issue is key management. So threshold cryptography is the best way where multiple parties are involved like cloud computing.

A. Threshold cryptography

If for decrypting an encrypted message, the number of parties greater than or equal to a threshold value come together in the decryption process such system is said to be "threshold cryptosystem". Threshold cryptography makes use of two keys public key and private key [12]. A public key is used for encrypting the message and the participating parties share the corresponding private key. Let there are n number of parties. Then such system is said to be (t, n)-threshold, if t or more than t of these parties can combined their shares for decrypting the ciphertext, but less than t parties have no meaning.

Threshold cryptography makes use of Secret sharing scheme which has two phase key distribution and key reconstruction. Threshold versions of encryption algorithms can be built for many public encryption algorithms. The natural goal of such algorithms is to be as secure as the original algorithm. Threshold versions have been defined for:

- RSA
- Pallier cryptosystem
- Damgård–Jurik cryptosystem
- ElGamal

Threshold Cryptography is the art of chopping a secret into little bits. Only by possessing more than a threshold number of bits of the secret the secret can be determined. A secret must be broken into C (N, M-1) pieces and each holder carries (N-M+1)/N parts of the whole key.

B. Secret Sharing Schemes (SSS)

In modern cryptography, the security of data is fully dependent on the security of the keys used. As most of the ciphers are public knowledge, one can easily encrypt and decrypt any message if they know the key involved. For some highly confidential data, it's not always good to have a single person in control of the key and to secure of the data. This has lead to the need for Secret Sharing Schemes, which allow keys to be distributed among a group of people, with a pre-specified number of them needing to input their share in order, to access the key.

In a secret sharing scheme, a secret ξ is divided into n shares in order to be distributed among a set of players. Each secret share is a plane, and the secret is the point at which three shares intersect. Subsequently, an authorized subset k of players collaborates to reconstruct the secret this is known as (k, n) threshold secret sharing (TSS) scheme. Secret sharing consists of two phases: sharing and recovery. In secret sharing phase dealer selects polynomial f(x) of degree t-1such that f (0) is the secret. Dealer then sends shares f(i) to players Pi and finally leaves the scheme. And In the recovery phase any set of t players can construct the secret by Langrange interpolation in the absence of dealer. In fact, distributed secure systems using threshold secret sharing can be adjusted automatically based on the resource availability of the cloud providers. Cryptographic primitive can be used to create self -organizing protocol in the cloud. It also states that distributed system can be reconfigured automatically based on the resource availability of the cloud providers by using social secret sharing scheme.

Well-known secret sharing schemes (SSS) in the literature include Shamir secret sharing based on polynomial interpolation, Blakley secret sharing based on hyper plane geometry, and Asmuth-Bloom secret sharing based on the Chinese Remainder Theorem.

C. Three well known Secret sharing schemes

1) Shamir Secret Sharing Scheme

Shamir secret sharing is based on polynomial interpolation & Lagrange interpolation formula over a finite field. It uses the fact that we can find a polynomial of degree t−1 given t data points. To generate a polynomial

$$f(x) = \sum_{i=0}^{t-1} a_i x^i$$

a_0 is set to the secret value and the coefficients $a_1$to a_{t-1} are assigned random values in the field [10]. The value f (i) is given to user i. When t or more than t but not less than t out of n users comes together, they can reconstruct the polynomial using Lagrange interpolation method and can find the secret.

For example consider, the dealer selects a secret sharing polynomial as, $f(x) = 8+9x+3x^2+2x^3$ over the field Z_{15}. Let n=5, and k= 4. The secret is S= 8. Now dealer will create the shares and distribute among n players. The corresponding shares are:

f(1) = 8 + 9(1) + 3(1)2 + 2(1)3 => 22 mod 15 => 7
f(2) = 8 + 9(2) + 3(2)2 + 2(2)3 => 54 mod 15 => 9
f(3) = 8 + 9(3) + 3(3)2 + 2(3)3 => 116 mod 15 => 11
f(4) = 8 + 9(4) + 3(4)2 + 2(4)3 => 220 mod 15 => 10
f(5) = 8 + 9(5) + 3(5)2 + 2(5)3 => 378 mod 15 => 3.

k=4, so at least four players can reconstruct the secret by Lagrange's Interpolation formula,

$$f(x) = \frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_n)} f(0) + \frac{(x-x_0)(x-x_2)\cdots(x-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_n)} f(1) + \cdots + \frac{(x-x_0)(x-x_1)\cdots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\cdots(x_n-x_{n-1})} f(n)$$

Consider first four players (1, 7), (2, 9), (3, 11), and (4, 10), the secret can be calculated as:

$$\mathbf{f(0)} = \frac{7\cdot 2\cdot 3\cdot 4}{(2-1)(3-1)(4-1)} + \frac{9\cdot 1\cdot 3\cdot 4}{(1-2)(3-2)(4-2)} + \frac{11\cdot 1\cdot 2\cdot 4}{(1-3)(2-3)(4-3)} + \frac{10\cdot 1\cdot 2\cdot 3}{(1-4)(2-4)(3-4)}$$

=> 8 mod 15 => 8(= S)

Now consider another combinations of shares as (1,7), (2, 9), (4,10), (5, 3)

$$\mathbf{f(0)} = \frac{7\cdot 2\cdot 4\cdot 5}{(2-1)(4-1)(5-1)} + \frac{9\cdot 1\cdot 4\cdot 5}{(1-2)(4-2)(5-2)} + \frac{10\cdot 1\cdot 2\cdot 5}{(1-4)(2-4)(5-4)} + \frac{3\cdot 1\cdot 2\cdot 4}{(1-5)(2-5)(4-5)}$$

=> 8 mod 15 => 8 (= S) is our secret.

2) Blakley Secret Sharing Scheme

Blakley secret sharing scheme (BSSS) has a different approach which is based on hyperplane geometry [10]: for implementation a (t,n) threshold scheme, a hyperplane equation in a t-dimensional space over a finite field such that each hyperplane passes through a certain point is given to each of the n users. The intersection points of the hyperplane gives the secret we take the secret as the first coordinate of the intersection point. When t users come together, and solve the system of equations they can reconstruct the secret. Suppose a (t, n) threshold scheme there will be n × t linear system of equations,

$$Ax = y$$

Secret values of y_i with $a_{i1}, \ldots, a_{it}$ are distributed by dealer to each player. In recovery phase players will solve the linear equations by solving a matrix of hyperplane equations. Secret will be the first coordinate of the solution.

3) Asmuth-Bloom Secret Sharing Scheme

Asmuth-Bloom's Secret Scheme makes use of Chinees remainder theorem. The Chinese remainder theorem can be explained as [7],[9]:

Let $k \geq 2$, $m_1,...,m_{k\geq 2}$, and $b_1,...,b_k \in Z$. The system of equations:

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ \vdots \\ x \equiv b_k \bmod m_k \end{cases}$$

has solutions in Z if and only if $b_i \equiv b_j \bmod (m_i,m_j)$ for all $1 \leq i, j \leq k$. Moreover, if the above system of equations have solutions in Z, then it has an unique solution in $Z[m_1,...,m_k]([m_1,...,m_k]$ which denotes the least common multiple of $m_1,...,m_k)$. for the standard version of the Chinese remainder theorem, $(m_i, m_j) = 1$, for all $1 \leq i < j \leq k$,.

As discussed in [9] Asmuth and Bloom, uses special sequences of integers. More exactly, a sequence of pair wise co-prime positive integers $r, m_1 < \cdots < m_n$ is chosen such that

$$r \cdot m_{n-k+2} \cdots m_n < m_1 \cdots m_k$$

such sequence is given, then scheme works as follows:

- The secret S is selected as a random element from the set Z_r;
- The shares Ii are selected as $I_i = (S + \gamma \cdot r) \bmod m_i$, for all $1 \leq i \leq n$, where γ is an arbitrary integer such that $S + \gamma \cdot r \in Z_{m1\cdots mk}$;
- For k distinct shares $I_{i1},...,I_{ik}$, the secret S can be reconstructed as $S = x_0 \bmod r$, where x_0 is calculated, using the standard Chinese remainder theorem(CRT), as the unique solution modulo $m_{i1} \cdots m_{ik}$ of the system :

$$\begin{cases} x \equiv I_{i_1} \bmod m_{i_1} \\ \vdots \\ x \equiv I_{i_k} \bmod m_{i_k} \end{cases}$$

The sequences used in the Asmuth-Bloom scheme can be generalized by allowing modules that are not necessarily pair wise co-prime in an obvious manner. Sorin Iftene and Ioana Boureanu [9] used sequence r, $m_1, \cdots, m_n$ such that

$$r \cdot \max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}([m_{i_1},\ldots, m_{i_{k-1}}]) < \min_{1 \leq i_1 < \cdots < i_k \leq n}([m_{i_1},\ldots, m_{i_k}])$$

By multiplying every element of an ordinary Asmuth-Bloom sequence except r with a fixed element $\delta \in Z$, $(\delta, m_1 \cdots m_n) = 1$, we will obtain a generalized Asmuth-Bloom sequence.

D. Kinds of secret sharing schemes

1) verifiable secret sharing (VSS)

Commonly, we believe that the dealer who partition the secret and allocates shares to shareholders without any mistake. All shareholders must unconditionally trust that the share which they received is valid. In 1985, Chor et al. presented a concept of verifiable secret sharing (VSS). The meaning of verifiability means that shareholders are able to verify that the shares which they received are consistent. VSS is a essential tool for many researches in cryptography, such as in secure multi-party computation [5].

2) proactive secret sharing (PSS)

It mix ups the secret-sharing technology with the periodical share update process to guarantee the overall security of a system. By using this updating mechanism, only old shares are updated from time to time without changing the original secret, so the old shares stolen by attackers become useless; therefore, to steal a t- secret, an attacker requires to attack on at least t- servers in the same time period.

3) *weighted secret sharing (WSS)*

In the weighted secret sharing schemes, a positive weight is provided to each user and the secret can only be recreated if and only if the sum of the weights provided to all participants is greater than or equal to a fixed threshold value of weight.

E. Need of security on cloud computing

- Data is the most important assets of any company, and it must be protected with as much care as any other asset. While data at rest encrypt it so that if any intruder try to access that data or if due to any configuration error unauthorized parties accessed that data, that data cannot be interpreted.
- During the transmission of data encryption is a must because that data will travel over insecure public infrastructure and is observed by any party in between. It needs strong authentication between application components so that data is transmitted only to known parties.
- Trust, Security and Privacy are on-going research issues in any development, as new security holes will appear with hackers advancing in their efforts. In particular in cloud infrastructures, additional issues arise that can be considered serious security and privacy concerns. New security governance models & processes are required that cater for the specific issues arising from the cloud model.
- Information stored at cloud can be modified or lost. So, we have to do something to secure those files or data. For this the best way is to encrypt the data or files before storing in the cloud.

F. limitations of secret sharing schemes

Common to all unconditionally secure secret sharing schemes, there are some limitations:

- The secret and each share must be of same in length.
- All secret sharing schemes uses random bits for secret distribution. To distribute a secret of arbitrary length entropy of (t-1)*length is necessary.

II. **RELATED WORK**

Md Kausar Alam, Sharmila Banu K [3] surveys many running research related paper to single cloud and multi clouds security using Shamir's Secret Sharing algorithm and addresses possible solutions and methodology. Main focus of them was use of multi clouds and data security and reduces security risks and affects the cloud computing user using Shamir's Secret sharing algorithm. They used RSA algorithm with Threshold secret sharing. Amir Herzberg, Stanislaw Jarecki, Hugo Krawczyk, and Moti Yung [6] have proposed an efficient proactive secret sharing scheme, where shares are renewed from time to time (without modifying the secret) so that information collected by the adversary in one time period is now not useful for breaking the secret because the shares are changed. Hence, the adversary ready to gain knowledge of the secret needs to crack to all k locations during the same time interval or at the same time (e.g., one day, a week, etc.). In order to maintain the integrity and availability of the secret, they suggested mechanisms to identify maliciously (or accidentally) corrupted shares, also to secretly recover the correct shares after alteration is discovered.

Kamer Kaya and Ali Aydın Selcuk [7] in his paper investigated how to realize verifiable secret sharing (VSS) schemes with the help of Chinese Remainder Theorem (CRT). Also they proposed a new VSS scheme based on the Chinese Remainder Theorem (CRT) and proved its security. And using the proposed Verifiable Secret Sharing scheme, they developed a joint random secret sharing (JRSS) protocol. Joint random secret sharing (JRSS) protocols allows a group of users to jointlygenerate and share a secret in the absence of a trusted dealer. Although there have been JRSS schemes but they are based on Shamir's Secret Sharing Scheme, so far no JRSS scheme has been proposed which is based on CRT method. Chunli Lv, Xiaoqi Jia, Jingquiang Lin, Jiwu Jing, Lijun Tian, and Mingli Sun[8] has proposed a new XOR-based (k, n) threshold secret sharing scheme, in which secret is taken as a binary string and only by XOR operation both shares creation and recovery of secret can be done. They concluded that by using more shares (≥ k) speed of recovery can be increased, and when k is nearer to n, the cost of computation is less than existing XOR-based methods in both recovery phase and distribution phase.

III. APPLICATIONS

Secret sharing schemes are best for storing information that is highly sensitive, highly confidential and highly important. For example storing missile launch codes, encryption keys, and numbered bank accounts. Each of these parts of information must be kept highly confidential, as their exposure could be disastrous; still, it is also critical that they not be lost. Secret sharing schemes allow arbitrarily high levels of confidentiality and reliability to be achieved. A secret sharing scheme can secure a secret over multiple servers and remain recoverable despite multiple server failures. Only organizations with very important and confidential secrets, such as militaries, certificate authorities, and governments, would make use of the threshold cryptography. However, in October 2012 when a number of large public websites password ciphertext compromises or stolen, than RSA Security announced that it would release software that makes the technology of threshold cryptography available to the general public.

IV. SCENARIO

In cloud computing if key is stored at a single server; the system is not reliable and fault tolerance. So to store keys at multiple servers are more reliable and fault tolerant, than single server but by storing key at multiple servers confidentiality may decrease. So before storing it key is divided into n-shares, and each share is stored at different servers. Key can be recovered from any k-shares out of those n-shares by secret sharing scheme, but before selecting those k-shares servers are authenticated to select the shares by clients and this is called multiparty authentication.

V. PROBLEM DEFINATION

As we discussed above our shares of key is stored at multiple servers if we have to reconstruct the key, we required k-shares out of those n-shares, but the questions arises from which servers the shares are selected, so our problem is that what will be the criteria for selecting those k shares out of n shares.

This problem will be solved in out next implementation paper, which will use a trust function for selecting the shares based on some parameters. The parameters may be response time of servers, failure rate of servers etc. These parameters will be updated each time the client communicates to the server.

A. Trust function

To compute the reputation of each server in a multiparty authentication trust function may be used. Mehrdad Nojoumian and Douglas R. Stinson [4] have defined trust function as:

Definition: Let $T_{ji}(p)$ be the trust value assigned by P_j to P_i in period p. Let T_i: N → R be the trust function representing the reputation of P_i:

$$T_i(p) = \frac{1}{n-1}\sum_{j\neq i} T_i^j(p)$$

Where $-1 \le T_i(p) \le +1$ and $T_i(0) = 0$. For calculating player's reputation, the average of the trust values is computed.

VI. CONCLUSIONS

There are a lot of benefits of cloud computing which facilitates the companies to adopt cloud computing, in addition security is a major barrier to the adoption of cloud computing. There are many cryptography algorithms which may be adopted for cloud computing, threshold cryptography is one of the algorithm which may be used. And threshold secret sharing schemes is also used in which a secret is divided in to n parts which is called shares and distributed (or stored) to each different player (or servers), and at the time of recovery by using k-parts secret is recovered. There are many type of secret sharing schemes which are discussed above. We are trying to use secret sharing scheme in our multi-party authentication scenario. By using this type of scenario systems reliability can be increased and the system will be more fault tolerant as it is storing different part at different location if anybody wants to steal the key, he has to attack at least k- servers at a time.

REFERENCES

[1] Jianyong Chen, Yang Wang, and Xiaomin Wang "On-Demand Security Architecture for Cloud Computing", IEEE Computer Society, JULY 2012, pp. 73-78.

[2] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham "Security Issues for cloud computing", International Journal of Information Security and Privacy, 4 (2), April-June 2010, pp. 39-51.

[3] Md Kausar Alam, Sharmila Banu K, "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013, ISSN 2250-3153.

[4] Mehrdad Nojoumian and Douglas R. Stinson "Social Secret Sharing in Cloud Computing Using a New Trust Function".

[5] Lein Harn, Changlu Lin "Strong (n,t,n) verifiable secret sharing scheme", Information Sciences, Elsevier, 2010, pp. 3059–3064.

[6] Amir Herzberg, Stanislaw Jarecki, Hugo Krawczyk, and Moti Yung "Proactive Secret Sharing Or: How to Cope With Perpetual Leakage", D. Coppersmith (Ed.): Advances in Cryptology - CRYPT0 '95, LNCS 963, Springer-Verlag Berlin Heidelberg , 1995, pp. 339-352.

[7] Kamer Kaya and Ali Aydın Selcuk "A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem", Springer-Verlag Berlin Heidelberg, 2008, pp. 414–425.

[8] Chunli Lv, Xiaoqi Jia, Jingquiang Lin, Jiwu Jing, Lijun Tian, and Mingli Sun, "Efficient Secret Sharing Schemes", CCIS 186, Springer- Verlag Berlin Heidelberg, 2011, pp. 114-121.

[9] Sorin Iftene and Ioana Boureanu, "Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem".

[10] Ilker Nadi Bozkurt, Kamer Kaya, Ali Aydin Selcuk, and Ahmet M.Giiloglu, "Threshold Crtyptography Based on Blakley Secret Sharing".

[11] Sandeep.R.Narani, "Social Secret Sharing for Resource Management in Cloud".

[12] en.wikipedia.org/wiki/Threshold_cryptosystem.