PRIVACY-PRESERVING MA-CPABE-NMAC SCHEME IN CLOUD ENVIRONMENTS FOR SECURE CAPTCHA DESIGN AND AUTHENTICATION IN HEALTHCARE INFORMATION SYSTEMS

Prof. Giulia Conti[1]
[1] University Of Zurich, Department Of Cybersecurity And Biomedical Cloud Systems, Zurich, Switzerland

ABSTRACT

In a cloud, the data are subjected to many forms of security and privacy issues. A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. Here, the paper propose a Multi authority based privacy-preserving CP-ABE with captcha protocol (MAPA-c) to address security and privacy issue for cloud storage. In the MAPA-c 1) CaRP are both a captcha and a graphical password scheme, which addresses a number of security problems altogether, such as online guessing attacks, relay attacks. 2)Multi access authority is achieved by MA-CP-ABE scheme which provides anonymous access request matching mechanism with security and privacy considerations; and 3) attribute based access control is adopted to realize that the user can only access its own data fields.

KEYWORDS: captcha, privacy preserving, cryptography, cloud..

1. INTRODUCTION

Cloud computing is location-independent computing, whereby shared servers provide resources, software, and data to computer and other devices on demand. Details are abstracted from consumers, who no longer have need for expertise in, or control over, the technology infrastructure "in the cloud" that supports them. Cloud computing is still considered in its infancy, there are many challenging issues waiting for tackling. The cloud suffers much from data loss, privacy, security and revocation problems.

In a cloud, critical information is placed in infrastructures of entrusted third parties, ensuring security to data and preserving privacy of user is of paramount importance. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally complex. Text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard. Machine recognition of non-character objects is far less capable than character recognition. Here, captcha is introduced as graphical passwords (CaR-RP) with both recall based and recognition based schemes to enhance the security of user. CaR-RP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Unlike other graphical passwords, images used in CaR-RP are Captcha challenges, and a new CaR-RP image code is generated for every login attempt. Using MA-ABE scheme, whichallows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority a number dk and a set of attributes. It can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. It reduces heavy computation overhead on central authority but privacy of the user is traced. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure. Here the encryptor intelligently decides who should or should not have access to the data that it encrypts. A non-monotonic access structure where the secret keys are labelled with a set of attributes including not only the positive but also the negative attributes [1]. Comparatively, ABE scheme with non-monotonic access structure can express a more complicated access policy which prevents collision attack.

2. LITERATURE REVIEW

A literature survey has been conducted and is listed as follow.

Dunning *et al.* [2] proposed an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty oriented cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed on top of secure sum data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem are used for the data mining, a

distributed solution of certain polynomials over finite fields enhances the algorithm scalability, and Markov chain representations are used to determine statistics on the required number of iterations.

Liu *et al.* [3] proposed a multi-owner data sharing secure scheme (Mona) for dynamic groups in the cloud applications. The Mona aims to realize that a user can securely share its data with other users via the entrusted cloud server, and can efficiently support dynamic group interactions. In the scheme, a new granted user can directly decrypt data files without pre-contacting with data owners, and user revocation is achieved by a revocation list without updating the secret keys of the remaining users. Access control is applied to ensure that any user in a group can anonymously utilize the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration. It indicates the storage overhead and encryption computation cost are independent with the amount of the users.

Grzonkowski*et al.* [4] proposed a zero-knowledge proof (ZKP) based authentication scheme for sharing cloud services. Based on the social home networks, a user centric approach is applied to enable the sharing of personalized content and sophisticated network-based services via TCP/IP infrastructures, in which a trusted third party is introduced for decentralized interactions.

Nabeel*et al.* [5] proposed a broadcast group key management (BGKM) to improve the weakness of symmetric key cryptosystem in public clouds, and the BGKM realizes that a user need not utilize public key cryptography, and can dynamically derive the symmetric keys during decryption. Accordingly, attribute based access control mechanism is designed to achieve that a user can decrypt the contents if and only if its identity attributes satisfy the content provider's policies. The fine-grained algorithm applies access control vector (ACV) for assigning secrets to users based on the identity attributes, and allowing the users to derive actual symmetric keys based on their secrets and other public information. The BGKM has an obvious advantage during adding/revoking users and updating access control policies.

Wang *et al.* [6] proposed a distributed storage integrity auditing mechanism, which introduces the homomorphism token and distributed erasure-coded data to enhance secure and dependable storage services in cloud computing. The scheme allows users to audit the cloud storage with lightweight communication overloads and computation cost, and the auditing result ensures strong cloud storage correctness and fast data error localization. Towards the dynamic cloud data, the scheme supports dynamic outsourced data operations. It indicates that the scheme is resilient against Byzantine failure and malicious data modification attack.

Sundareswaran *et al.* [7] established a decentralized information accountability framework to track the users' actual data usage in the cloud, and proposed an object-centred approach to enable enclosing the logging mechanism with the users' data and policies. The Java ARchives (JAR) programmable capability is leveraged to create a dynamic and mobile object, and to ensure that the users' data access will launch authentication. Additionally, distributed auditing mechanisms are also provided to strengthen user's data control, and experiments demonstrate the approach efficiency and effectiveness.

M. Chase*et al.* [8] proposed MA-ABE scheme, whichallows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. It reduces heavy computation overhead on central authority but privacy of the user is traced.

V. Goyal *et al.* [9] proposed KP-ABE, in which cipher text is associated with set of descriptive attributes, and users' keys are associated with policies. They stress that in KP-ABE, the encryptor exerts no control over who has access to the data it encrypts, except by her choice of descriptive attributes for the data. Rather, they must trust that the key-issuer issues the appropriate keys to the appropriate users. It falls short of flexibility in attribute management and scalability in dealing with multiple-levels of attribute authorities.

J. Bethencourt*et al.* [10] proposed CP-ABE, in which a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in the system, they

specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure. Here the encryptor intelligently decides who

should or should not have access to the data that it encrypts. It suffers from collusion attack which arises when users combine their attributes to obtain the attributes of the owner.

3. PRIVACY PRESERVING MA-CPABE-NMAC SCHEME

Access Structure
An access structure is employed to control users, from accessing the protected resource in systems where users need to cooperate with multiple parties [10]. For instance, the head agent may specify the following access structure for accessing this information: ((“Public Corruption Office” AND (“Knoxville” OR “San Francisco”)) OR (management-level > 5). By this, the head agent could mean that the memo should only be seen by agents who work at the public corruption offices at Knoxville or San Francisco and FBI officials very high up in the management chain.

Monotonic Access Structure
A monotonic access structure [10] is an access structure where, given a universal set P, if a subset S! Of P satisfies the access structure, all subsets S of P which contain S! Satisfy the access structure.

Threshold Access Structure
A (k, n)-threshold access structure is an access structure where, given a universal set P with |P| = n, a subset S of P satisfies the access structure if and only if it contains at least k elements in P.

Non-Monotonic Access Structure
A non-monotonic access structure [1] where the secret keys are labelled with a set of attributes including not only the positive but also the negative attributes. Comparatively, ABE scheme with non-monotonic access tructure can express a more complicated access policy.

Pseudo Random Key Generator
A PRKG [11] is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRKG's state, which includes a truly random seed. The numbers are important in practice for their speed in number generation. The common classes of suitable algorithms include Linear Congruent Generators, Lagged Fibonacci Generators, and Linear Feedback Shift Registers.

Linear Congruent Generator
LCG represents one of the oldest, easiest, fastest and best-known pseudorandom number generator algorithms.

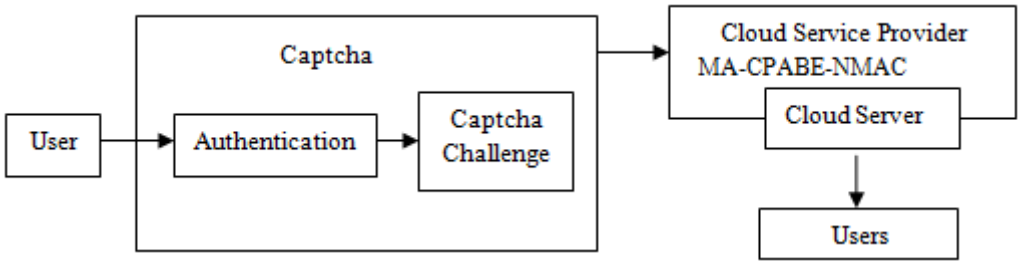

Figure 1 Block diagram of Privacy preserving MA-CPABE-NMAC scheme

The different modules in the system are listed as follows:

Authentication of anonymous user
Anonymous access request matching mechanism with security and privacy considerations is achieved here. The *Anonymous user* is used for public access (browsing) to your web Site. Anonymous access is the most common web site access control method. The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from *authorization,* which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who it claims to be, but says nothing about the access rights of the individual.

Captcha based on Hard AI Problems

A CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but are beyond the capabilities of current computer programs. Here it is a sequence of clicks on an image, which is used to derive a password. Here a new CaRP image code is generated for every login attempt.

Pseudo Random Attribute Generation
A PRKG is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRKG's state, which includes a truly random seed. The numbers are important in practice for their speed in number generation. The common classes of suitable algorithms include Linear Congruent Generators, Lagged Fibonacci Generators, and Linear Feedback Shift Registers.

Management of owner's data
An authority maintains the attributes which is framed on access structure, and each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure.

Multi-Authority - Cipher text-Policy Attribute Based Encryption
Multi-Authority – Cipher text - Policy Attribute Based Encryption is an efficient encryption which is used to preserve security and privacy of the user, to resist collusion attack, comparing to other public key encryption method and to handle expressive types of encrypted access control. Here, a decryption key and set of attributes are generated randomly based on Pseudo Random Key Generator (PRKG) using a Linear Congruent Generator (LCG) when the account is registered. Here four types of authorities are used.

Based on Multi-Authority Attribute based Encryption (MA-ABE), two attributes out of four is distributed to the user from the owner's registered attribute set. Again based on Cipher text-Policy Attribute Encryption (CP-ABE) on a Non Monotonic Access Structure.

Non-Monotonic Access Structure
A non-monotonic access structure [1] where the secret keys are labelled with a set of attributes including not only the positive but also the negative attributes. Comparatively, ABE scheme with non-monotonic access structure can express a more complicated access policy.

Pseudo Random Key Generator
A PRKG [11] is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRKG's state, which includes a truly random seed. The numbers are important in practice for their speed in number generation. The common classes of suitable algorithms include Linear Congruent Generators, Lagged Fibonacci Generators, and Linear Feedback Shift Registers.

4. CONCLUSION

Using Captcha based KP-ABE scheme privacy of owner is preserved providing data confidentiality, security, access control from unauthorized access and usability gradually increased with less time consumption and memory consumption. A CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but are beyond the capabilities of current computer programs. Here it is a sequence of clicks on an image, which is used to derive a password. Here a new CaRP image code is generated for every login attempt. Cipher text is associated with set of descriptive attributes, and users' keys are associated with policies. They stress that in KP-ABE, the encryptor exerts no control over who has access to the data it encrypts, except by their choice of descriptive attributes for the data. Rather, they must trust that the key-issuer issues the appropriate keys to the appropriate users.

REFERENCES

[1] J. Yu, P. Lu, G. Xue, and M. Li, "Towards Secure Multi- Keyword Top-k Retrieval over Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, 2013.
[2] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.
[3] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2012.
[4] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social

Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, 2011.
[5] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, 2012.
[6] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.
[7] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEETransactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.
[8] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.
[9] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.
[10] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.
[11] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," in Proceedings of Global Telecommunications Conference (GLOBECOM 2010), December 6-10, 2010.