View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by International Journal of Innovative Technology and Research (IJITR)

Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

Applying Policy Hiding Cryptograhic Scheme in DOSN

Harshitha M
4th sem, M.Tech (CNE)
Shree Devi Institute of Technology,
Mangalore, India.

Abstract-- Security concerns in online social networking service have number of proposals for decentralized online social networks (DOSN). This removes the central provider and giving the control over their data who can access it. This project use the cryptographic scheme. In existing DOSN cryptographic primitives that hide the data but reveal the access policies. The project analyze Predicate encryption (PE) is cryptographic primitives that to provide access control of encrypted data using attribute based policies. We use bloom filter means that decreasing decryption time and indicate objects that can be decrypted by a particular user. This is best suitable for performance efficiency.

Keywords— Prediction encryption, Diffie hallman, Elgamal encryption & decryption, Bloom filters Introduction

INTRODUCTION

Centralized online social network collects and store the information in cloud but suffer from privacy leak when transfer of data to third parties for advertisement purposes [1].

Decentralized architecture (DOSN), which user have control over their data and who can access it and this requires cryptographic means to protect data. General purpose cryptographic in DOSN use attribute based encryption (ABE) [2] to protect confidentiality and privacy. Access control mechanism should be privacy preserving. Privacy preserving means user should be able to decrypt only the object for which they satisfied the access policy; encrypted objects should not to reveal users who have access to these object; the quantity, size, and type of objects should be unknown to the user unless he can decrypt them.

In existing DOSN are not privacy-preserving, ABE-based DOSN systems could be provide privacy by using a privacy-preserving of this cryptographic primitive[3], but efficiency would be lost because of the quadratic growth of the ciphertext size in the number of attributes. BE-based systems could use anonymous BE, ANOBE [4], but then long ciphertexts make it inefficient.

In proposed PE scheme ciphertext size, encryption and decryption time are linear in size. We proposes a univariate polynomial construction for access policies to increase the performance of the scheme. Hiding access policies in PE also prevents legitimate users from knowing whether they will be able to decrypt a ciphertext. We address this by using Bloom filters.

The purpose of this project, every encrypted or un-encrypted object stored in the profile, each user data controlled by cryptographic scheme, Profile owner create decrypted key for each of his friends. An object is encrypted under some access policy. Only the user whose decryption key satisfies the access policy of an object can decrypt the object. A digital signature scheme (independent from the encryption scheme) is used for message authentication purposes. Each user is assumed to have a private key for signing messages that he posts.

RELATED WORK

There are many research on decentralized network, Privacy, access mechanism, storage are the main concern on cloud.

Safebook [5] online social network applications severely suffer from various security and privacy exposures. This article suggests a new approach to tackle these security and privacy problems with a special emphasis on the privacy of users with respect to the application provider in addition to defense against intruders or malicious users. In order to ensure users' privacy in the face of potential privacy violations by the provider, the suggested approach adopts a decentralized architecture relying on cooperation among a number of independent parties that are also the users of the online social network application. The second strong point of the suggested approach is to capitalize on the trust relationships that are part of social networks in real life in order to cope with the problem of building trusted and privacy-preserving mechanisms as part of the online application. The combination of these design principles is Safebook, a decentralized and privacy-preserving online social network application. Based on the two design principles, decentralization and exploiting real-life trust, various mechanisms for privacy and security are integrated into Safebook in order to provide data storage and data management functions that preserve users' privacy, data integrity, and availability. Preliminary evaluations of Safebook show that a realistic compromise between privacy and performance is feasible.

Secure and dependable storage services in cloud computing: Cloud storage enables users to remotely store their data and enjoy the on demand high quality cloud applications without the burden of local hardware and software management. We propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append.

Fuzzy Keyword Search Over Encrypted Data Using Cloud Computing[7]: In this paper, for the first time we formalize and solve the problem of supporting efficient yet privacy preserving fuzzy search for achieving effective utilization of remotely stored encrypted data in Cloud Computing. We used

All Copyrights Reserved by R.V. College of Engineering, Bangalore, Karnataka

an advanced technique (i.e., wild card-based technique) to construct the storage efficient fuzzy keyword sets by using edit distance technique. With the help of symbol based tri search scheme we enhance searching efficiency. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search.

Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds[8]: decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

DESIGN & IMPLEMENTATION

The design of proposed system use PE scheme with attributes that hides access policies. This scheme achieve privacy, high performance and functionality in the DOSN process flow in the diagram shown in Fig 1.

The Fig: 2 shows the component diagram, how sender and receiver access information by using encryption and decryption method.

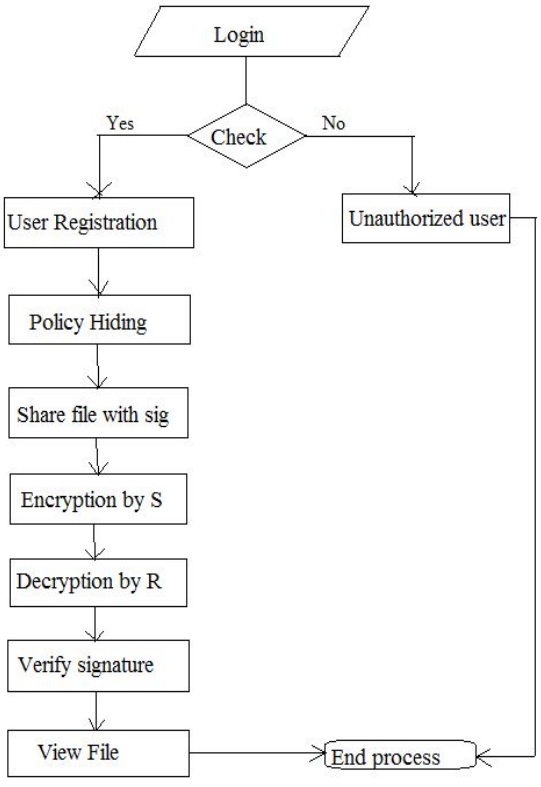

Fig 1: Data flow diagram

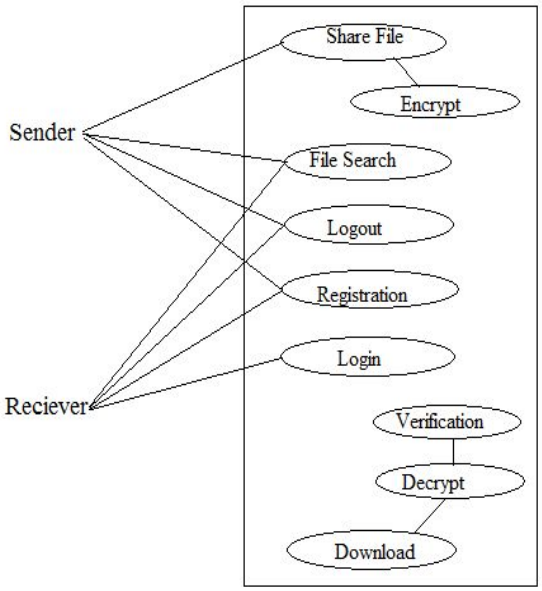

Fig: 2 Component diagram

A. Predicate Encryption

Predicate encryption (PE) is a cryptographic primitives, which use attribute to provide control of encrypted data. When creating a ciphertext, the encryptor specifies an access policy and only those users whose keys satisfy the policy can decrypt. The decryption keys are generated by the encryptor using a master secrete.

$$H_f\ (P_T + K) = C_T$$

H_f: Hash function.

P_T: Plain text.

K : Public key

C_T: Cipher text

The above function explain that every attributes are define in hash function H_f. Each plain text P_T has public key K to generate the cipher text C_T.

B. Bloom Filters

Bloom filters is space efficient data structure that represents elements in the set. DOSN contains multiple object objects encrypted for different users. It is impossible for a user to determine if an object is encrypted for him without trying to decrypt it since the ciphertexts do not reveal access policies. The user could use a trial-and-error approach (sequentially trying to decrypt objects) for rendering the profile, but this becomes prohibitively expensive with the large number of objects. Therefore, we utilize Bloom filters to speed up rendering and to show users in a privacy-preserving manner whether they can decrypt objects.

Bloom filter have two operation: add (x) and query (x), where x is element. Add(x) operation is add the elements with hash function. Query(x) operation is repeats hashing and then checks if the particular bit are set to 1

All Copyrights Reserved by R.V. College of Engineering, Bangalore, Karnataka

Bloom filter, encrypted object has the following format:

CT, PEenc (PK, K, AP), S, BF (H(S||kID1),…H(S||kIDn),R1,...Rpn),SGN (1)

where CT - is an object encrypted with a random key K, K - a symmetric key used for AES encryption, PK- public key of the PE scheme used for encryption, AP - access policy, S - nonce, BF - Bloom filter, H - cryptographically secure hash function, kIDi - an identifier of a decryption key belonging to recipient i, Ri - random values for padding, p - padding size, SGN - signature of all the previous fields.

C. Diffie hallman Method

This algorithm provide to communicate between two parties to shared secrete between them.

Algorithm:

1. A and B agree on a p(prime)

   g (generator), p and g public.
2. A choose a secrete number a, and send to B (g^a mod p)
3. B choose a secrete number b, and send to A (g^b mod p)
4. A computes ((g^b mod p)^a mod p)
5. B computes ((g^a mod p)^b mod p)

Both A and B can use this number as their key

D. Elgamal Method

A and B have prime number p and generatot g, A choose number and compute A = g^a, B does the same and compute.

B = g^b. A's public key is A and that's private key is a, similarly B's public key is B and that's private key is b.

1) Encrypting and Decrypting message

   If B now wants to send a message m to A, he randomly picks a number k which is smaller than p. B then computes:

   $c_1 = g^k \bmod p$

   $c_2 = A^k * m \bmod p$

and sends c_1 and c_2 to A. A can use this to reconstruct the message m by computing

$c_1^{-a} * c_2 \bmod p = m$

because

$c_1^{-a} * c_2 \bmod p = (g^k)^{-a} * A^k * m = g^{-a*k} * A^k * m = (g^a)^{-k} * A^k * m = A^{-k} * A^k * m = 1 * m = m$

PERFORMANCE

Whenever have set or list and space is an issue, bloom filter may be a use full alternatives, this provide the time and space effiency

Bloom filter use hash function A hash function is a function that will take an item of data and process it to produce a value or key. For example, you could simply add up the code values for each character in a string and return the result mod some given value. A hash function always produces the same hash value from the same data but it is possible and in fact usual for two different data values to produce the same hash value. That is the hash value isn't unique to a given item of data and you can't reverse the hashing function to get the data values. The hash function is a many-one deterministic function. A good hash function also has other desirable properties such as spreading the hash values obtained as evenly as possible over the output range but for the moment let's just concentrate on the basic hash function.

Number of bits m in bloom filter depends on the false -positive probability p and number of elements n. the space efficiency [9] is calculated by

$$m = -n\frac{\ln p}{(\ln 2)^2}$$

CONCLUSION

We have proposed to apply a privacy preserving scheme to the DOSN context: predicate encryption (PE). It is too expensive to use out of the box. Therefore for PE we proposed a construction for access policies that drastically increases performance, but introduces some trade-offs: it allows encrypting for a bounded set of groups/users; this bound is a trade-off between efficiency and functionality of the scheme; the number of groups in the system is unlimited; a user has 2g different decryption keys, where g is the number of groups a user is a member of; having multiple keys leaks some information about access policies. PE is most suitable for encrypting for groups or small sets of separate identities. We designed an experiment that showed that for newsfeed assembly from all friends our scheme shows good performance and thus user experience. For schemes that do not reveal access policies and have relatively slow decryption, we proposed to use Bloom filters to indicate to users which files they can decrypt. Bloom filters are both performant and space-efficient, and thus are suitable for DOSNs.

In this paper, we focused the evaluation on performance to see if PE is even feasible under the constraints of decentralized online social networks, starting from the security and privacy properties of the original scheme. The next steps are to focus on security and privacy, as well as semantics of access policies of our modifications.

REFERENCE

[1]. Greenwald and E. MacAskill, "NSA prism program taps in to user data of apple, google and others," 2013. http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[2]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, ser. SP '07. IEEE Computer Society, 2007, pp. 321–334. [Online]. Available: http://dx.doi.org/10.1109/SP.2007.11

All Copyrights Reserved by R.V. College of Engineering, Bangalore, Karnataka

[3]. C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryp- tion keys," in Pairing-Based Cryptography Pairing 2007, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2007, vol. 4575, pp. 39–59.

[4]. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in ACNS, ser. LNCS, vol. 5037. Springer-Verlag, 2008, pp. 111–129.

[5]. L. Cutillo, R. Molva, and T. Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," Communications Magazine, IEEE, vol. 47, no. 12, pp. 94 –101, dec. 2009.

[6]. A. Kirsch and M. Mitzenmacher, "Less hashing, same performance: Building a better bloom filter," Random Struct. Algorithms, vol. 33, no. 2, pp. 187–218, Sep. 2008.

[7]. ian Wang, Cong Wang and Ning Cao, "Fuzzy Keyword Search Over Encrypted Data Using Cloud Computing" Published in INFOCOM, 2010 Proceedings IEEE on 19 march 2010.

[8]. Ruj, S; Stojmenovic, M; Nayak, A , "Decentralized Access Control with Anonymous Authentication of Data Stored in Cloud" Published in parallel and distribution system, IEEE transaction on(vol:25 issues:2) on 15 February 2013.

All Copyrights Reserved by R.V. College of Engineering, Bangalore, Karnataka