A Survey on Attribute Based encryption Methods to Preserve Privacy in Mobile Users

M B Rajashekar
Assistant Professor, Department of CSE
GSSSIETW, Mysuru

Dr. S. Meenakshi Sundaram
Professor & Head, Department of CSE
GSSSIETW, Mysuru

***Abstract*— The potential applications of developing privacy preserving to improve performance is still an open Issue. Mobile phones are not designed for privacy and security they expose new kinds of surveillance risks are the motivational factors to develop a privacy preserving of location of the mobile users. Today's location-based services solely rely on users' devices to determine their location, e.g., using GPS. However, it allows malicious users to fake their STP information. In traditional public key cryptography. Instead both users' private keys and cipher texts will be associated with a set of attributes or a policy over attributes. A user is able to decrypt a cipher text if there is a "match" between his private key and the cipher text. It requires calculation for each key this decreases the performance.**

Keywords - CP-ABE, Privacy Preserving, STAMP, Mobile Users

I. INTRODUCTION:

In many situations, when a user encrypts sensitive data, it is imperative that she establish a specific access control policy on who can decrypt this data. For example, suppose that the FBI public corruption offices in Knoxville and San Francisco are investigating an allegation of bribery involving a San Francisco lobbyist and a Tennessee congressman. The head FBI agent may want to encrypt a sensitive memo so the attributes can access it. only personnel that have certain credentials or at-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, FBI officials very high up in the management chain, and a consultant named Charlie Eppes. As illustrated by this example, it can be crucial that the person in possession of the secret data be able to choose an access policy based on specific knowledge of the underlying data. Furthermore, this person may not know the exact identities of all other people who should be able to access the data, but rather she may only have a way to describe them in terms of descriptive attributes or credentials. Traditionally, this type of expressive access control is enforced by employing a trusted server to store data locally. The server is entrusted as a reference monitor that checks that a user presents proper certification before allowing him to access records or files. However, services are increasingly storing data in a distributed fashion across many servers. Replicating data across several locations has advantages in both performance and reliability. The drawback of this trend is that it is increasingly difficult to guarantee the security of data using traditional methods; when data is stored at several locations, the chances that one of them has been compromised increases dramatically. For these reasons we would like to require that sensitive data is stored in an encrypted form so that it will remain private even if a server is compromised. Most existing public key encryption methods allow a party to encrypt data to a particular user, but are unable to efficiently handle more expressive types of encrypted access control such as the example illustrated above.

STAMP requires low computational overhead. The contributions of this paper can be summarized as:

- A distributed STP proof generation and verification protocol (STAMP) is introduced to achieve integrity and non transferability of STP proofs. No additional trusted third parties are required except for a semi-trusted CA.
- STAMP is designed to maximize users' anonymity and location privacy. Users are given the control over the location granularity of their STP proofs.
- STAMP is collusion-resistant. The Bussard-Bagga distance bounding protocol [9] is integrated into STAMP to prevent a user from collecting proofs on behalf of another user. An entropy-based trust model is proposed to detect users mutually generating fake proofs for each other.
- STAMP uses a entropy-based trust model to guard users from prover-witness collusion. This model also encourages witnesses against selfish behavior.
- Modifications to STAMP to facilitate the utilization of stationary wireless infrastructure APs or trusted mobile users are presented.
- A security analysis is presented to prove STAMP achieves the security and privacy objectives.
- A prototype application is implemented on the Android platform. Experiments show that STAMP requires preferably low computational time and storage.

II . PRIVACY PRESERVING

Anonymity: Location privacy is an extremely important factor that needs to be taken into consideration when designing any location based systems. Revealing both identity and location information to an untrusted party poses threats to a mobile users. First, a prover should be able to hide his/her identity from a witness. In addition, it is not only the prover's anonymity that we should pay attention to, a witness's anonymity should also be preserved. Since a witness who agrees to create an STP

proof is co-located with the prover, his/her identity should not be revealed to the prover, either. Pseudonyms: Pseudonyms are often used to provide anonymity. Nevertheless, if the same pseudonym is used by a mobile user, it is possible for an adversary to link multiple locations of the same pseudonym. By profiling and analyzing the user's location trace, the adversary could reveal the identity of the user or at least significantly reduce the anonymity set. True anonymity requires unlinkability [12]. Anonymity can be effectively enhanced if a user is assigned with multiple pseudonyms, and pseudonyms are carefully chosen when communicating with another party. The APPLAUS scheme [3] adopts such an approach. However, this incurs high operational overhead because of the management of identities and their corresponding pseudonyms. It also requires a deliberate pseudonym scheduling algorithm which statistically eliminates the possibility of linking multiple pseudonyms or user profiling based on a single pseudonym. In addition, the pseudonym manager (e.g., CA) has to be completely trusted. Otherwise, it could be the single point of failure. If an adversary breaks into the pseudonym manager and obtains a copy of the pseudonym mapping, the whole system would break down. Therefore, we do not design STAMP based on pseudonyms. Instead, we use cryptographic encryption and commitment techniques to hide users' identities in the STP proof generation process. Location Granularity: An STP proof system needs to be flexible in terms of location granularity, in order to enforce location privacy and accommodate localization error. The location of a prover could be represented by different levels of granularity, for example, a city, a neighborhood, or an exact geo-coordinate point. Though a prover needs to reveal both his/her identities and STP information in order to get services from a verifier, the prover does not necessarily trust the verifier completely. When a prover tries to claim his/her location at a particular time to a verifier, he/she should not be obligated to reveal his/her most accurate location to the verifier. Depending on the requested service, a prover should have control over the granularity of his/her location that is revealed to the verifier.

III. THE STAMP SCHEME

A. Preliminaries 1) Location Granularity Levels: We assume there are granularity levels for each location, which can be denoted by , where represents the finest location granularity (e.g., an exact Geo coordinate), and represents the most coarse location granularity (e.g., a city). Hereafter, we refer to location granularity level as location level for short. When a location level is known, we assume it is easy to obtain a corresponding higher location level where . The semantic representation of location levels are assumed to be standardized throughout the system. 2) Cryptographic Building Blocks: STAMP uses the concept of commitments to ensure the privacy of provers. A commitment scheme allows one to commit to a message while keeping it hidden to others, with the ability to reveal the committed value later. The original message cannot be changed after it is committed to. A commitment to a message can be denoted as where is a nonce used to randomize the commitment so that the receiver cannot reconstruct , and the commitment can later be verified when the sender reveals both and . A number of commitment schemes [14]–[16] have been proposed and commonly used. Our system does not require a specific commitment scheme. Any scheme which is perfect binding and computational hiding can be used. In our implementation, we used [14], which is based on one-way hashing. One-way hash functions have the similar binding and hiding properties as commitment schemes.

IV. PROTOCOL

1) Overview: Our protocol consists of two primary phases: STP proof generation and STP claim and verification. Fig. 2 gives an overview of the two phases and the major communication steps involved. When a prover collects STP proofs from his/her co-located mobile devices, we say an STP proof collection event is started by the prover. An STP proof generation phase is the process of the prover getting an STP proof from one witness. Therefore, an STP proof collection event may consist of multiple STP proof generations. The prover finally stores the STP proofs he/she collected in the mobile device. When a prover encounters a verifier (the frequency of such encounters is specific to the application scenarios) and he/she intends to make a claim about his/her past STP to the verifier, the STP claim and verification phase takes place between the prover and the verifier. A part of the verification job has to be done by CA. Therefore, communication between the verifier and CA happens in the middle of the STP claim and verification phase. In Fig. 2, the two arrowed lines in red color represent the latter two stages of the Bussard-Bagga protocol. These stages require multiple interactions between the two involved parties, and thereby are represented by doubly arrowed lines. The preparation stage of the Bussard-Bagga protocol does not need to be executed for every STP proof generation and thus is not shown. Users could run the preparation stage before each STP proof collection event or pre-compute and store several sets of the bit commitments and primitives, and randomly choose one set of them when needed. Subsequently, we present the details of the STAMP protoco them when needed. Subsequently, we present the details of the STAMP protocol

V. LITERATURE REVIEW

In 2009, M. Chase and S.S.M. Chow presented a distributed KP-ABE scheme that solves the key escrow problem in a multi-authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this kind of fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with the other authorities in the system to generate a user's secret key. This results is communication overhead on the system setup phase and on any rekeying

phase, and requires each user to store additional auxiliary key components besides the attributes keys, where N is the number of authorities in the system [2].

In 2009, Recently, S.S.M. Chow proposed an anonymous private key generation protocol in identity-based literature such that the KGC can issue a private key to an authenticated user without knowing the list of users' identities. It seems that this anonymous private key generation protocol works
properly in ABE systems when we treat an attribute as an identity in this construction. However, found that this cannot be adapted to ABE systems due to mainly two reasons. First, in Chow's protocol, identities of users are not public anymore, at least to the KGC, because the KGC can generate users' secret keys otherwise. Second, since the collusion attack between users is the main security threat in ABE [3].

In 2008, Bethencourt, V. Kumar and Boldyreva proposed first key revocation mechanisms in CP-ABE and KP-ABE
settings, respectively. These schemes enable an attribute key revocation by encrypting the message to the attribute set with its validation time. These attribute-revocable ABE schemes have the security degradation problem in terms of the backward and forward secrecy. They revoke attribute itself using timed rekeying mechanism, which is realized by setting expiration time on each attribute. In ABE systems, it is a considerable scenario that membership may change
frequently in the attribute group. Then, a new user might be able to access the previous data encrypted before his joining
until the data are reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). On the other hand, a revoked user would still be able to access

VI. ADVANTAGES

- Target a wider range of applications.
- STAMP is based on a distributed architecture.
- STAMP requires only a single semi-trusted third party which can be embedded in a Certificate Authority (CA).
- We design our system with an objective of protecting users' anonymity and location privacy.
- No parties other than verifiers could see both a user's identity and STP information (verifiers need both identity and STP information in order to perform verification and provide services).
- STAMP requires low computational overhead.
- A security analysis is presented to prove STAMP achieves the security and privacy objectives.

REFERENCES

[1] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in Proc. ACM HotMobile, 2009, Art. no. 3.
[2] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in Proc. ACM GIS, 2010, pp. 23–32.
[3] Z. Zhu and G. Cao, "Towards privacy-preserving and colluding-resistance in location proof updating system," IEEE Trans. Mobile Comput.,vol. 12, no. 1, pp. 51–64, Jan. 2011.
[4] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in Proc. ACM WiSe, 2003, pp. 1–10.
[5] R. Hasan and R. Burns, "Where have you been? secure location provenance for mobile devices," CoRR 2011.
[6] B. Davis, H. Chen, and M. Franklin, "Privacy preserving alibi systems," in Proc. ACM ASIACCS, 2012, pp. 34–35.
[7] I. Krontiris, F. Freiling, and T. Dimitriou, "Location privacy in urban sensing networks: Research challenges and directions," IEEE Wireless Commun., vol. 17, no. 5, pp. 30–35, Oct. 2010.
[8] Y.Desmedt,"Major security problems with the'unforgeable'(feige)fiat-shamir proofs of identity and how to overcome them," in Proc. SecuriCom, 1988, pp. 15–17.
[9] L.BussardandW.Bagga,"Distance-bounding proof of knowledge to avoid real-time attacks,"in Security and Privacy in the Age of Ubiquitous Computing. New York,NY, USA:Springer,2005.
[10] Y. S. Sneda, G. Mahadevan, M. Prakash, "A Personalized Product Based Recommendation System Using Web Usage Mining and Semantic Web", International Journal of Computer Theory and Engineering, Vol. 4, No. 2, April 2012.
[11] J.Reid,J.Nieto,T.Tang,andB.Senadji,"Detectingrelayattackswith timing-basedprotocols,"inProc.ACMASIACCS,2007,pp.204–213.
[12] C. Kim, G. Avoine, F. Koeune, F. Standaert, and O. Pereira, "The Swiss-knifeRFIDdistanceboundingprotocol,"inProc.ICISC,2009, pp. 98–115.
[13] D. Singelee and B. Preneel, "Location verification using secure distanceboundingprotocols,"inProc.IEEEMASS,2005
[14] H. Han et al., "Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments," in Proc. IEEE INFOCOM, Apr. 2014, pp. 727–735.
[15] W. Hill, L. Stead, M. Rosenstein, and G. Furnas, "Recommending and Evaluating Choices in a Virtual Community of Use," Proc. Conf. Human Factors in Computing Systems, 1995.
[16] P. Resnick, N. Iakovou, M. Sushak, P. Bergstrom, and J. Riedl, "GroupLens: An Open Architecture for Collaborative Filtering of Netnews," Proc. 1994 Computer Supported Cooperative Work Conf., 1994.
[17] U. Shardanand and P. Maes, "Social Information Filtering: Algorithms for Automating 'Word of Mouth'," Proc. Conf. Human Factors in Computing Systems, 1995.
[18] R. Baeza-Yates and B. Ribeiro-Neto, Modern Information Retrieval. Addison-Wesley, 1999.
[19] N. Belkin and B. Croft, "Information Filtering and Information Retrieval," Comm. ACM, vol. 35, no. 12, pp. 29-37, 1992.
[20] J. Delgado and N. Ishii, "Memory-Based Weighted-Majority Prediction for Recommender Systems," Proc. ACM SIGIR '99 Workshop Recommender Systems: Algorithms and Evaluation, 1999. [21] D. Billsus and M. Pazzani, "Learning Collaborative Information Filters," Proc. International Conf. Machine Learning, 1998.
[21] J.S. Breese, D. Heckerman, and C. Kadie, "Empirical Analysis of Predictive Algorithms for Collaborative Filtering," Proc. 14th Conf. Uncertainty in Artificial Intelligence, July 1998.
[22] B. Mobasher, R. Cooley, J. Srivastava "Automatic Personalization Based on Web Usage Mining", Communications of the ACM, Volume 43 Issue 8, Aug. 2000.
[23] S.K. Shinde, U.V. Kulkarni, "A New Approach for on Line Recommender System in Web Usage Mining", International Conference on Advanced Computer Theory and Engineering, 2008. ICACTE '08, pp. 973- 977, 2008.
[24] M. Jalali, N. Mustapha, N.B. Sulaiman, A. Mamat, "A Web Usage Mining Approach Based on LCS Algorithm in Online Predicting Recommendation Systems", 12th International Conference on Information Visualisation, pp. 302-307, 2008.
[25] X. Sui, S. Wang, Z. Li, "Research on the model of Integration with Semantic Web and Agent Personalized Recommendation System", International Conference on Computer Supported Cooperative Work in Design, pp. 233 - 237, 2009.
[26] Y. S. Sneda, G. Mahadevan, M. Prakash, "A Personalized Product Based Recommendation System Using Web Usage Mining and Semantic Web", International Journal of Computer Theory and Engineering, Vol. 4, No. 2, April 2012.