International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume-1, Issue-III ISSN (Online): 2454- 1966

Privacy Protection for Framework Secure Data Encrypted Using OSN

R.KRISHNAMOORTHY, V.SABAPATHI, V.ARUNA

PG Scholar, M.Tech Scholar, Assistant Professor,
Department of CSE,
Nandha Engineering college, Veltech Dr.RR Dr.SR Technical University,

E-Mail: krishcse@gmail.com, sabapathi2000@gmail.com, aruname10@gmail.com.

December – 2015

www.istpublications.com

Privacy Protection for Framework Secure Data Encrypted Using OSN

R.KRISHNAMOORTHY, V.SABAPATHI, V.ARUNA

PG Scholar, M.Tech Scholar, Assistant Professor,
Department of CSE,
Nandha Engineering college, Veltech Dr.RR Dr.SR Technical University,

E-Mail: krishcse@gmail.com, sabapathi2000@gmail.com, aruname10@gmail.com.

ABSTRACT

A secure data sharing scheme in OSNs based on cipher text policy attribute based proxy re-encryption and secret sharing. This system presents a multiparty access control model, which enables the disseminator to update the access policy of cipher text if their attributes gratify the existing access policy. Also provide check ability on the outputs returned from the OSNs service earner to guarantee the exactness of part decrypted cipher text. The refuge and routine analysis results indicate that the proposed scheme is secure and efficient in OSNs. The key policy attribute are used for unfolding encrypting data and policy employed in user`s key, and the cipher text policy is the access structure on the cipher text and the access structure can also be present-day in either monotonic or non-monotonic. Privately achieve this protection through a new approach to building secure Systems: building practical systems that compute on encrypted data, without access to the decryption key. In this setting, individually designed and built a database system (CryptDB), a web application platform (Mylar), and two mobile systems, as well as developed new cryptographic schemes for them.

Key Words: Role-Based Access Control, Two-Party Computation, Attribute Secret Key, EASIER**,** access policy, proxy re-encryption, key policy attribute.

1. INTRODUCTION

Information security as defined by the standards published by the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC),is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. Data security includes the broad areas of information security management the topic of this book, computer and data security, and network security. To protect information and its related systems, organizations must implement such tools as policy, awareness, training and education, and technology. The NSTISSC model of information security evolved from a concept developed by the computer security industry known as the C.I.A. triangle. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value for its use in organizations: confidentiality, integrity, and availability.

Our main Objective is to improve the security in Online Social Networks**.**The primary goals of the proposed scheme are to data privacy and access control with regard to the private data stored on potentially untrusted storage sites. A new secure data sharing scheme in OSNs based on ciphertext-policy attribute based proxy re-encryption and secret sharing.First of all, Personally Encrypt the data using AES public key encryption scheme before sharing of data. After sharing of data, the data provider should be encrypt the data based on Attribute based proxy-re-encryption.The Attribute based encryption is based on location of users.Analyze and measure the computation cost for data encryption, data decryption and policy evaluation in our scheme.To protectinformation, users encrypt different pieces of data suchas profile information, wall posts, etc. with attribute policies.Only the contacts with keys having enough attributesto satisfy a policy can decrypt the data.

There are two tasks for encryption in building the private online social network. The first is to restrict the information available to applications as precisely as possible, so that individual organizations are not entrusted with large volumes of personal information. Although it is tempting to focus only on the exchange of information with friends, some applications may benefit from limited access to a user's profile, location, or messages, while carefully avoiding broad exposure. The second task is to restrict the information shared with friends" to what might be appropriate. Privately quote friends" here because the type of social link might be more than, less than, or different from friend. Family, neighbor, co-worker, boss, teammate, and other relations might define a connection in the social network. That connection is often simply termed friend", regardless of the actual, online relationship. A user's decision to accept one of these pseudo-friends into their neighborhood and avoid discussing certain topics or exclude them and avoid the bents of social networking represents a dilemma that can be avoided, if users may exibly classify their friends.

This design a platform-independent solution for users to share their location in a private fashion over LSSs. Our solution does not require any changes to the infrastructure and can operate with any third-party LSS. Individually propose a secure data sharing scheme supporting fine-grained and multiparty access control based on cipher text-policy attribute-based proxy re-encryption (CP-ABPRE)and secret sharing. The user first encrypts the data with random data encryption key using symmetric encryption algorithm, and then encrypts the data encryption key with access policy, and finally outsources the ciphertext. The disseminators can further customize new access policy if their attributes satisfy the existing access policy.

Privately to Present a partial decryption construction in which the computation overhead of user is largely reduced by delegating most of the decryption operations to the OSNs service provider and also provide check ability on the results returned from the OSNs service provider to guarantee the correctness of partial decrypted ciphertext. This design an efficient immediate attribute revocation method for CP-ABE scheme that achieves both forward and backward secrecy.
Moreover, the OSNs service provider only updates the ciphertext associated with revoked attribute and the personalized attribute key of non-revoked users. Thus our attribute revocation method incurs less computation cost. Without help to iimplement our solution as a prototype application for mobile phones codenamed PrivL (Private Locations. It uses encryption to protect user's location from third-party servers while still allowing them to share it with friends. It can also make use of distributed Hash tables (DHTs) to provide ephemeral data storage.

2. RELATED WORKS

In this section to discuss about OSNs and Information security. In general, there are two types of security mechanisms that have been designed to address the insider threat. The first is to prevent illicit activity by modeling access rules for the system and its users. The second is to detect illicit activity post hoc by reviewing patterns of user behavior. In this section, personally review prior research in these areas and relate them to the needs and challenges of CIS. Our own selves recognize that information leakage may transpire when information is shared between organizations.

EASiER [9] is an architecture that supports fine-grained access control policies and dynamic group membership by using CP-ABE scheme. In addition, EASiER is able to revoke a user without issuing new keys to other users or re-encrypting existing ciphertexts by using a proxy.

Yu *et al.* [10] employed KP-ABE (Key Policy Attribute based Encryption [11]) to enforce access policies based on data attributes.

Their scheme allows data owners to delegate most of the computation tasks involved in fine -grained data access control to untrusted cloud servers without disclosing the underlying data contents by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption.
Persona [14] enables access control by employing a combination of traditional public key cryptography and attribute-based encryption scheme. The combination of classical public- key schemes and ABE schemes has the drawback of increased key management complexity. The above attribute- based access control methods enable flexible access policies for the users. However, they treated media content as a single monolithic object, ignoring the structure of the content. Hence, these schemes are not suitable for access control to scalable multimedia content.

Jahid S, Mittal P et al. EASiER: Encryption based Access Control in Social Networks with Efficient Revocation A promising approach to mitigate the privacy risks in Online Social Networks (OSNs) is to shift access control enforcement from the OSN provider to the user by means of encryption.However, this creates the challenge of key management to support complex policies involved in OSNs and dynamic groups. To address this propose EASiER, an architecturethat supports fine-grained access control policiesand dynamic group membership by using attribute-based encryption.The primary goal of EASiER is to protect accidental orintentional information leak in OSN through encryption,specifically ABE, chosen for its expressiveness. Unlike traditional OSNs, which generally support one type of relationshipsuch as friend, EASiER users define relationships by assigning attributes and keys to each other. To protect information, users encrypt different pieces of data suchas profile information, wall posts, etc. with attribute policies.Only the contacts with keys having enough attributesto satisfy a policy can decrypt the data. For instance, user A defines the attributes (friend, colleague,neighbor), generates keys k1, k2, and k3 for the combinationof attributes 'colleague', 'friend, neighbor', and 'colleague,neighbor' respectively, and assigns these keys to u1, u2, andu3 respectively. She encrypts her data with the policy 'colleague or (friend and neighbor)'.

HUR J et al.[ ] The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users key. So overcome this problem to propose escrow problem which means a written agreement delivered to a third party and Attribute-based encryption (ABE) is a promising Cryptographic approach fine-grained data access control which is provides a way of defining access policies based on different attributes of the requester, environment, or the data object. The KGC can decrypt every cipher text addressedto specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the datasharing systems.

SYSTEM AND MODELS

1. PRELIMINARIES

Table 1 presents the notations used throughout the paper in this section.

1. Bilinear Maps

The present a few facts related to groups with efficiently computable bilinear maps.

Let G_0 and G_1 be two multiplicative cyclic groups of prime order p. Let g be a generator of G0 and e be a bilinear map, *e*: $G_0 \times G_0 \rightarrow G_1$. The bilinear map *e* has the following properties:

1. Bilinearity: for all $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$. (1)

2. Non-degeneracy: $e(g, g) \neq 1$. Individually say that G0 is a bilinear group if the group operation in G0 and the bilinear map *e*: $G_0 \times G_0 \rightarrow G_1$ are both efficiently computable. Notice that the map *e* is symmetric since,

$$e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a) \quad (2)$$

2. The Decisional Bilinear Diffie-Hellman (BDH) Assumption

Let $a, b, c, z \in \mathbb{Z}_p$ be chosen at random and *g* be a generator of G_1. The decisional BDH assumption [8, 34] is that no probabilistic polynomial-time algorithm *B* can distinguish the tuple $(A = g^a, B = g^b, C = g^c, e(g, g)^{abc})$ from the tuple $(A = g^a, B = g^b, C = g^c, e(g, g)^z)$ with more than a negligible advantage. The advantage of *B* is

$$\left| \Pr[\mathcal{B}(A, B, C, e(g, g)^{abc}) = 0] - \Pr[\mathcal{B}(A, B, C, e(g, g)^z)] = 0 \right| \quad (3)$$

Where the probability is taken over the random choice of the generator *g*, the random choice of *a; b; c; z* in Z*p*, and the random bits consumed by *B*.

TABLE 1. NOTATIONS

Notation	Description
K	security parameter
PK	system public key
MK	master secret key
AS	attribute set
ASK	attribute secret keys
UK	user secret keys
AK	personalized attribute key
DEK	data encryption key

RK	re-encryption key
T	access policy
Enck	symmetric encryption with key *k*
Deck	symmetric decryption with key *k*

3. Ciphertext-Policy Attribute-Based Encryption with User Revocation

In this section to define the CP-ABE with user revocation capability scheme. The scheme consists of the following six algorithms:

Setup. The setup algorithm is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public key PK and a master key MK.

AttrKeyGen (MK; Λ; U). The attribute key generation algorithm takes as input the master key MK, a set of attributes Λ⊆*L*, and a set of user indices U⊆U. It outputsa set of private attribute keys SK for each user in U thatidentifies with the attributes set.

KEKGen(U). The key encrypting key (KEK) generation algorithm takes as input a set of user indices U⊆U, andoutputs KEKs for each user in U, which will be used toencryptattribute group keys $K_{\curlywedge_i}$ for each $G_i \in \mathcal{G}$.

Encrypt (PK; M; A). The encryption algorithm is a randomized algorithm that takes as input the public parameter PK, a message M, and an access structure A over the universe ofattributes. It outputs a ciphertext CT such that only a userwho possesses a set of attributes that satisfies the accessstructure will be able to decrypt the message.

ReEncrypt (CT; G). The re-encryption algorithm is a randomized algorithm that takes as input the ciphertext CT including an access structure A, and a set of attribute groups G. If the attribute groups appear in A, it re-encrypts CT for the attributes; else, returns ⊥. Specifically, it outputsa re-encrypted ciphertext CT' such that only a user who possesses a set of attributes that satisfies the access structure and has a valid membership for each of them at the same time will be able to decrypt the message.

Decrypt (CT0; SK; K_). The decryption algorithm takes as input the ciphertext CT' which contains an access structure A, a private key SK, and a set of attribute group keys Kʌ for a set of attributes Λ. The decryption can be done if f Λ satisfies A and Kʌ is not revoked for any $\curlywedge \in A$.

4. PROPOSED SCHEME AND PERFORMANCE ANALYSIS

1. PROPOSED SYSTEM

Provide check ability on the results returned from the OSNs service provider to guarantee the correctness of partial decrypted ciphertext. Design an efficient attribute revocation method that achieves both forward and backward secrecy. The security and performance analysis results have shown that our scheme is secure and efficient. Key Generation and ABE Algorithm is used to both forward and backward secrecy technique. Thus, unauthorized access from the OSNs service provider to the plaintext of the encrypted data should be prevented. In our proposed system initially the data will be encryption format then it will decrypt twice.

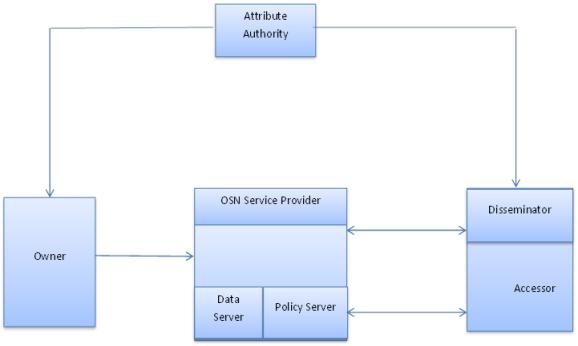

Fig 1. Proposed block diagram.

If the data will be decrypted then it will go to the Re-encrypted format privately get the original information. It proposes a secure data sharing scheme in online social networks based on ciphertext-policy attribute- based proxy re-encryption and secret sharing. Attribute-based encryption (ABE) is the important technique adopted to protect data security and achieve fine-grained access control in data sharing systems [1]. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among decryption keys and cipher texts.

The service provider OSNs accomplishes the users and stores the encrypted data and guidelines from the owners.The associated aspects are data security, multiparty access control, partial decryption, and attribute cancelation.Analyze and measure the computation cost for data encryption, data decryption and policy evaluation in our scheme.The primary goals of the proposed scheme are to data privacy and access control [3] with regard to the private data stored on potentially untrusted storage sites.

Described group-based access policies and the mechanisms needed to provide decryption and authentication byboth groups and individuals. Personally have demonstrated the versatility of these operations in an OSN design called Persona,which provides privacy to users and the facility for creatingapplications like those that exist in current OSNs.

The main advantages in highly secured data transfer with advanced encryption technique the other person cannot decrypt it easily. Next Encryption system which provides more security for our data. An authorized recipient can easily decrypt the message with the key. Finally Large computational resources.

2. PERFORMANCE EVALUATION

Individually compare the computation efficiency of both encryption and decryption gives the comparison of encryption time on the owner versus the number of attributes. Our scheme first encrypts the data based on CP-ABE, which protects the data from the malicious users and semi-trusted OSNs service provider. Privately compare our scheme with current data sharing in OSNs.

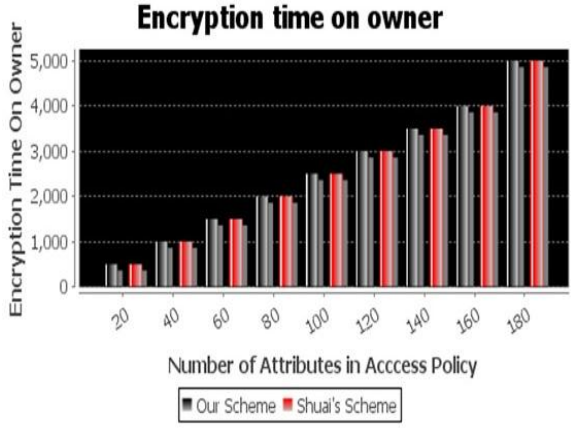

Fig 2. The Example for Encryption time on owner

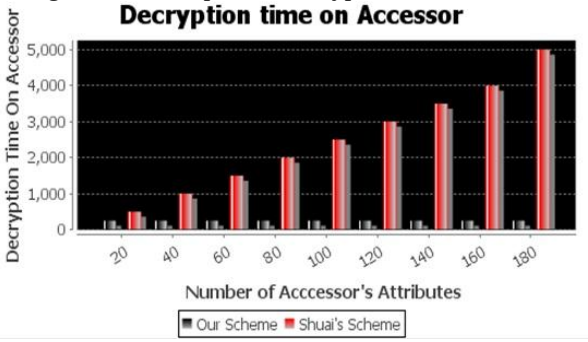

Fig 3. The Example for Decryption time on Accessor.

The compared aspects are data security, multiparty access control, partial decryption, and attribute revocation. analyze and measure the computation cost for data encryption, data decryption and policy evaluation in our scheme. The cryptographic operation was implemented using the pairing based cryptography.

Schemes	**Data confidentiality**	**Multi party access control**	**Partial decryption**	**Attribute revocation**
Shehab's scheme	ABE	Yes, access policy	Yes	Yes, backward and forward secrecy
Hu's scheme	ABE	Yes, ACL	No	No
Bethen's scheme	ABE	Cipher text-Policy	No	No
Dien's scheme	PRE	No	No	No
Wu 's scheme	ABE	No	No	No
Guo's scheme	ABE	No	No	No
Wan's scheme	ABE	No	No	No
Proposed scheme	ABE	Yes	Cipher text	Yes, backward and forward secrecy

5. RESULT DISCUSSION

The security and efficiency are important challenging issues in the data sharing systems. In this paper, our own selves first propose a secure data sharing scheme supporting multiparty access control based on CP-ABPRE and secret sharing in OSNs. Our scheme allows users to outsource encrypted data to the OSNs service provider for sharing [13], and allows the disseminators to further customize the access policy of the ciphertext if their attributes satisfy the existing access policy. Further, privately to present a partial decryption construction in which the computation overhead of user is largely reduced by delegating most of the decryption operations to the OSNs service provider [16].

Individually also provide check ability on the results returned from the OSNs service provider to guarantee the correctness of partial decrypted ciphertext[20]. Finally, also design an efficient attribute revocation method that achieves both forward and backward secrecy. The security and performance analysis results have shown that our scheme is secure and efficient.

6. CONCLUSION AND FUTURE WORK

It achieves more secure and fine grained data access control in the data sharing system. Personally demonstrated that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system. Privacy controls provided by existing OSNs are not sufficient since they rely on trusting the OSNs with data from which they can profit. It has shown how ABE and traditional public key cryptography can be combined to provide the flexible, user-defined access control needed in OSNs. personally have described group-based access policies and the mechanisms needed to provide decryption and authentication by both groups and individuals. It achieves the more privacy of using Attribute based proxy re-encryption of data for secure sharing of sensitive information. A secure data sharing scheme supporting multiparty access control based on CP-ABPRE and secret sharing in OSNs. The partial decryption creation in which the multiplication overhead of user is largely concentrated by delegating most of the decryption operations to the OSNs service provider.

Privately present a partial decryption construction in which the computation overhead of user is largely reduced by delegating most of the decryption operations to the OSNs service provider. individually also provide check ability on the results returned from the OSNs service provider to guarantee the correctness of partial decrypted ciphertext. Finally, private design an efficient attribute revocation method that achieves both forward and backward secrecy. The security and performance analysis results have shown that our scheme is secure and efficient. Future Work Blowfish is a block cipher designed by Bruce Schneier, author of Applied Cryptography.

REFERENCES

[1] SHEHAB M, SQUICCIARINI A, AHN G, et al. Access control for online social networks third party applications, Computers and Security,2012, 31(8): 897-911.

[2] RAJI F, MIRI A, JAZI M. CP2: Cryptographic privacy protection framework for online social networks, Computers and Electrical Engineering, 2013, 39(7): 2282-2298.

[3] WAN Zhiguo, LIU June, DENG R H. HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing, IEEE Transactions on Information Forensics and Security, 2012, 7(2): 743-754.

[4] WU Yongdong, WEI Zhuo, DENG R H. Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks, IEEE Transactions on Multimedia, 2013, 15(4):778-788.

[5] SHUAI Huimin, ZHU Wentao. Masque: Access Control for Interactive Sharing of Encrypted Data in Social Networks, Proceedings of6th International Conference on Network and System Security (NSS'2012): November 21-23,2012. Wuyishan, Fujian, China, 2012: 503-515.

[6] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-Policy Attribute-Based Encryption Proceedings of 2007 IEEE Symposium on Security and Privacy (SP'07): May 20-23, 2007. Berkeley,CA, USA, 2007: 321-334.

[7] HUR J. Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid. IEEE Transactions on Parallel and Distributed Systems,2013, 24(11): 2171-2180.

[8] HU Hongxin, AHN G. Multiparty Authorization Framework for Data Sharing in Online Social Networks Proceedings of 25th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'2011): July 11-13,2011. Richmond, VA, USA, 2011: 29-43.

[9] HUR J, NOH D. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems, IEEE Transactions on Parallel andDistributed Systems, 2011, 22(7): 1214-1221.

[10] TRAN D, NGUYEN H, ZHA Wei, et al. TowardsSecurity in Sharing Data on Cloud-Based SocialNetworks, Proceedings of 8th InternationalConference on Information, Communicationsand Signal Processing (ICICS'2011): December13-16, 2011. Singapore, Singapore, 2011: 1-5.

[11] DIEN N, HWANG J, YOO M. A New Frameworkfor Secure Sharing Data on Cloud-Based SocialNetworks, Proceedings of 2012 InternationalConference on ICT Convergence: "GlobalOpen Innovation Summit for Smart ICT Convergence"(ICTC'2012): October 15-17, 2012. JejuIsland, Korea, 2012: 333-335.

[12] BADEN R, BENDER A, SPRING N. Persona:An Online Social Network with User-DefinedPrivacy, Proceedings of ACM SIGCOMM2009 Conference on Data Communication (SIGCOMM'2009): August 17-21, 2009. Barcelona,Spain, 2009: 135-146.

[13] JAHID S, MITTAL P, BORISOV N. EASiER: Encryption-based Access Control in Social Networkswith Efficient Revocation, Proceedings ofthe 6th International Symposium on Information,Computer and Communications Security(ASIACCS'2011): March 22-24, 2011. HongKong, China, 2011: 411-415.

[14] GUO Linke, ZHANG Chi, YUE Hao, et al. A privacy-preserving social-assisted mobile contentdissemination scheme in DTNs, Proceedingsof the IEEE INFOCOM 2013: April 14-19, 2013.Turin, Italy, 2013: 2301-2309

[15] SHUAI Huimin, ZHU Wentao, LIU Xin. Publishingand Sharing Encrypted Data with PotentialFriends in Online Social Networks, Securityand Communication Networks, 2013.

[16] HU Hongxin, AHN G, JORGENSEN J. MultipartyAccess Control for Online Social Networks:Model and Mechanisms, IEEE Transactions onKnowledge and Data Engineering, 2013, 25(7):1614-1627.

[17] ZHOU Zhibin, HUANG Dijiang. Efficient andSecure Data Storage Operations for MobileCloud Computing, Proceedings of the 20128th International Conference on Network andService Management: October 22-26, 2012, LasVegas, NV, USA, 2012: 37-45.

[18] HUR J, KANG K. Dependable and Secure Computingin Medical Information Systems, Computer Communications, 2012, 36(1): 20-28.

[19] WU Qiuxin, ZHANG Miao. Adaptively Secure Attribute-Based Encryption Supporting AttributeRevocation, China Communications, 2012,9(9): 22-40.

[20] HUR J. Improving Security and Efficiency in Attribute-Based Data Sharing, IEEE Transactionson Knowledge and Data Engineering, 2013,25(10): 2271-2282.