Survey Paper on Object Oriented Cryptographic Security for Runtime Entities

Prof. Supriya Sarkar, Sohina Hasan

Department of Computer Engineering, Department of Computer Engineering, SKNSITS, Lonavala, India

Abstract— *With the advent of complex systems the need for large data storage with less space utility & high performance have become the vital features. Another important concern of the data is the security which is assured via the cryptographic techniques implemented at all levels of data storage. In this survey paper we introduce the concept of security between two hierarchical data accesses and propose the concept of hierarchical cryptography between data of different classes of different hierarchies.*

Keywords— Hierarchical inheritance, cryptree, cryptographic file system, Elliptical curve, Dual level key management, Chinese Remainder Theorem, cipher text policy attribute based encryption, Two level based Encryption construction.

I. INTRODUCTION

We have a lot of emerging trends for providing security to the data at different levels in the system. The data is usually organized as: (i) hierarchically (i.e. in the form of classes where each class extracts data from the other class. (ii) In the form of Grid (which emphasizes on large scale resource sharing & multi institutional collaboration). (iii) Multilevel access of data, (iv) data access in file system & storage area network, (v) general access & (vi) cloud computing (i.e. access of data from remote login).

All the data access & storage units are dealing with the problems of attacks which can be characterized as: (a) Passive Attacks: which consist of eavesdropping Or traffic analysis. (b) Active Attacks: which deal with masquerading, replaying modification, denial of service(DOS) attack.

During storage of data the data is static while during runtime the data has to be updated on and off depending upon the need. The access of data & its updating should be provided to only authentic users such that the key factors like confidentiality & integrity are maintained. In order to maintain such factors we use the technique of cryptography where we encrypt the data into cipher text & then on use decrypt it back to plain text. We also overcome the issue of general access in hierarchy via the Chinese Remainder Theorem.

Coming back to the aspect of Cryptography; it deals with key generation to decode the text. Depending upon the need either a single key is generated or dual keys are generated. We have two types of keys in cryptographic techniques. They are

(i) Symmetric Key: It is the same key used for both encryption of plaintext & decryption of cipher text.
(ii) Asymmetric Key: It uses two different keys namely public key & private key for encryption & decryption of text.

At hierarchical level when we extract information then depending upon the access specifier the data under the class is extracted & only authorized user has to be provided access for it. We generate a single key to encrypt data of a same class whereas on any update via the authorized user the key also will have to b updated. All the more here in section 1 we will emphasize more on the cryptography for the classes existing between different hierarchies which will require the data exchange via there objects. Section 2 gives literature survey followed by existing systems, conclusions & references in section 3, 4 & 5 respectively.

II. LITERATURE SURVEY

The literature survey contains study of different schemes available in cryptographic hierarchical access control for dynamic structures.

2.1 Dual key management scheme for secure grid : It is the mechanism using an innovative concept of Access Control Polynomial(ACP) & one way functions. The first level provides a flexible & secure group communication technology while the second level offers hierarchical access control.

2.2 Elliptical Curve cryptography: Elliptical curves are named so as they appear to be similar to the equation defining the roots of an ellipse. They are equations containing two variables & coefficients where the elements are in finite field. The elliptical equation is in the form of $y^2 = x^3 + ax + b$. The coefficients a, b should satisfy the condition $4a^3 - 27b^2 \neq 0$ so that there are no repeated factors.

For given values of a & b, the elliptical curve consists of positive & negative values of y for each value of x. A special point which acts as an identity is used. The following addition rules are used in elliptical curve arithmetic.

2.3 Cryptree: A cryptree is a cryptographic data structure consisting of keys & cryptographic links. It can be seen as directed graph with keys as vertices & cryptographic links as edges. Due to this tree structure cryptrees can be used efficiently manage the keys of nested folders in cryptographic file system, typically by making the links of the cryptographic tree publicly available.

2.4 Chinese Remainder Theorem(CRT): It works on 2 categories: data based solution and key based solution. Assume a data item is to be shared with k shares. In the data based solution, this data item is first encrypted by k shares' public keys respectively; then these k individual cipher text are combined by CRT . As a result, the final share cipher text is k times bigger than the data item. In the key based solution, the data item is first encrypted by a symmetric key to produce a data cipher text. Next, this symmetric key is encrypted by k shares' public keys respectively. Finally, these k individual cipher text are combined by CRT to produce a symmetric key share cipher text. The Data cipher text & the symmetric key share cipher text are concatenated & shared with those k shares.

2.5 File Encryption Integrity Protection Through Hash Trees: To compute the hash trees, a file is divided into 4kB blocks, a corresponding to Linux page size. We recall the construction of a k-ary Merkel tree using a hash function H(): Every leaf node stores the output of H applied to a data page of length b bytes, & every internal node stores the hash value computed on the concatenation of the hash values in its children. As the maximum file size in SAN.FS is fixed the maximum depth of the hash tree can be computed in advance, given the degree k. A high degree k results in a flat tree structure & has therefore similar unfavorable properties as using a single hash value for the whole life.

2.6 Dynamic Exterior Attacks: When an illegal user wishes to access the security key through the related public information when a new class joins the hierarchy.

2.7 Cipher text policy Attribute-based Encryption(CP-ABE): it is a public key cryptography primitive for one-to-many communications in cloud. In this algorithm, a user's private key is associated with a set of attributes, encrypts the file with an access tree. The access tree is organized in a way that its interior nodes are threshold gates & its leaf nodes are associated with user attributes. The user is able to decrypt if and only if that his attributes satisfy the access tree.

2.7.1 Proxy Re-Encryption: It is a semi trusted proxy in which the given proxy re-encryption key translates cipher texts under public key into cipher text under public key & vice versa.

2.8 Two Level Encryption Based Construction (TLEBC): It uses two level graphs. In two level partially ordered hierarchy, where each level contains the same number of classes & there are no edges between classes at the same level. Also in TLEBC dynamic updates to the hierarchy can be accomplished by means of only local updates to the public information only means of only local updates to the public information only.

S. No	Title	Year	Method Used	Algorithm Implemented	Problem/ Drawback
1.	A Cryptographic Solution For General Access Control	2005	Chinese Remainder Theorem (CRT) & hierarchical Encryption	CRT based on database solution and key based solution by : (i) fast modular exponentiation algorithm (ii) Garner's algorithm	It is too complex and lengthy. Security issues are a prominent problem with this algorithm. It lacks user/programmer friendly interface.
2.	Dual-Level Key Management for secure grid communication in dynamic & hierarchical	2006	Dual key management mechanism using access control polynomial one-way function .	First level provides a flexible & secure group communication & second level offer hierarchical access control.	Due to high dynamic nature of grid computing updates of group keys efficiently & effectively becomes a challenging problem.

	groups					
3.	Multilevel Access Control in a MANET for A Defense Messaging system using Elliptical Curve Cryptography	2009	Elliptic Curve Cryptography	Steps of elliptical Cryptography are: (i) Decide on the elliptical curve E, the elliptical curve should not have two coefficients a, b such that $4a^3-27b^2 \neq 0$ & a prime number p. (ii) For the elliptical curve equation apply values of x from 1 to p-1 & generate y values (iii) find the quadratic residues to avoid repetition in mod values & then collect all points on the elliptical curve	Management of traffic over the network & network congestion issues.	
4.	Cryptree: A folder tree structure for cryptographic file systems.	__	Data encapsulation under a Cryptree .	Hierarchical access via both types of cryptrees. (i) General Cryptree (ii) Read Access Cryptree	Cryptree does not provide proper information.	Medium
5.	Cryptographic Security for a high performance Distributed File System	2010	Key Management is integrated with the meta data service of the SAN file system.	File Encryption & integrity protection through hash trees.	(i) Hash tree implementation should include more sophisticated locking mechanism. (ii) Recovery issues.	High
6.	An Efficient & Secure key Management Scheme for hierarchical Access Control Based on ECC	2011	Efficient key management & derivation based on elliptical curve cryptosystem.	The product of the algorithm proposed by Jeng Wang Scheme is proned to dynamic exterior attacks.	No cryptographic solution is given to over come dynamic exterior attack.	Low
7.	Survey Paper on a Dynamic Cryptographic Access Control Scheme in Cloud Storage Services.	2014	Cipher text policy attribute based Encryption.(CPABE)	(i) Proxy Re-encryption Algorithm (PRE) (ii) Lazy Re-encryption Algorithm	Data security is at risk	Low

8.	Cryptographic hierarchical Access Control For Dynamic Structures.	2016	Hierarchical key assignment scheme with dynamic updates.	Construction based on symmetric encryption schemes.	(i) Protected data could be accessed i.e. it can be seen by unauthorized user since key decryption is not to reliable here. (ii) Cannot be used for different classes of different hierarchies.	

III. CONCLUSION

In this paper we propose the model from the knowledge gained by the literature survey of various survey papers the data should go triple encryption where data is organized under cryptees. Then the cryptographic key for every class function should be enveloped under hash functions. And at the end all this data should again be Encrypted using 128 bit AES algorithm.

ACKNOWLEDGEMENT

This paper has been completed with the help of Prof. Supriya Sarkar. I thank her for her help, support & guidance. I also thank the anonymous reviewers for their useful comments.

REFERENCES

[1] William Stalings, "Cryptography & network Security principles & practices", Third edition, pearson education.2001

[2] M. Atallah, K.Frikken,& M. Blanton, "Dynamic & Efficient Key Management For Access Hierarchies," CERIAS Tech report 2006-02, Center for education & research in, information Assurance & security, Purdue University.

[3] X. Zou, B. Ramamurthy, & S. Magliveras, "Chinese remainder theorem based hierarchical access controller secure group communications." Lecture notes in computer Science (LNCS), 2229:381.385, Nov. 2001

[4] A. Azagury, R. Canettii, M. Factor, S. Halevi, E.Henis D. Naor, N. Rinetzky, O. Rodeh, & J.Sataran, "A two layered approach for securing an object store network, " in Proc. 1st International IEEE Security in storage Workshop (SISW 2002), 2002.

[5] B. Gassend, G. E. Suh, D. Clarke, M. van Dijk, & S.Devdas, "Caches & hash trees for efficient memory integrity verification, " in Proc. 9th Intl. Symposium on high Performance Computer Architecture(HPCA '03), 2003.

[6] R. Pletka & C.Cachin, "Cryptographic security for a high- performance distributed file system," Research Report RZ 3661, IBM Research, Sept. 2006.

[7] C. C. Chang, I. C. Lin, H. M. Tsai, & H. H. Wang. "A key assignment Scheme for controlling Access in Partially Ordered User Hierarchies". In Proceedings of 18th International Conference On Advanced Information Networking & Applications(AINA'04), volume 2, pages 376-379, 2004.

[8] H. M. Tsai & C. C. Chang. "A Cryptographic implementation for dynamic access control in a user hierarchy." Computers & Security, 14(2): 159-166, 1995.

[9] Laxminath Tripathy & Nayan Rajan Paul " An Efficient and secure Key Management Scheme for Hierarchical Access Control Based on ECC" .

[10] Roman Pletka & Christian Cachin "Cryptographic Security for a high-Performance Distributed File System".

[11] Prof. D. N. Rewadkar(H.O.D) & Juhi M. Shah "Survey Paper on a Dynamic Cryptographic Access Control Scheme in Cloud Storage Services" Juhi M Shah et al, Int. J. Computer Technology & Applications, Vol5(3), 1309-1315

[12] Bethencourt, A. Sahai, B. Wwters, "Ciphertext-policy attribute based encryption" IEEE Symposium on security and Privacy. Berkeley, California, USA, pp. 321-334, 2007.

[13] Rui Zhang, Pei Shuai Chen "A Dynamic Cryptographic Access Control Scheme in cloud Storage Services"

[14] Yibing Kong, Jennifer Seberry, Jansuz R. Getta, & Ping yu, " A Cryptographic Solution For General Access Control" School of Information Technology & Computer Science, University of Wollongong, NSW, Australia

[15] Rivest, R. L, Shamir, A., Adleman, L. A method for obtaining Digital Signatures & Public key

Cryptosystems. Communications of the ACM, Vol. 21, no. 2. ACM Press(1978) 120-126

[16] Dominik Grolimund, Luzius Meisser, Stefan Schmid, Roger Wattenhofer, "Cryptree: A Folder Tree Structure for Cryptographic File Systems" ethz.ch Computer Engineering & Networks Laboratory(TIK), ETH Zurich, CH-8092 Zurich

[17] H. Chien, Y. Chung, . Tian. A Novel Key Management Scheme for dynamic Access Control in a user Hierarchy, IEEE COMPSAC, 2004.

[18] J. Nafeesa Begum, K.Kumar, Dr. V. Sumathy "Multilevel Access Control in a MANET for a Defense Messaging system using Elliptical Curve Cryptography"

[19] Xukai Zou, Yuan-Shun Dai, Xiang Ran, "Dual- level Key Management for secure grid communication in dynamic & hierarchical groups. Department of computer & Information Science, Purdue University School of Science, Indiana University, Purdue University, Indianapolis, 46202, USA.

[20] Arpana Mahajan & prof. Yask Patel, "Enhancing PHR Services in cloud computing: Patient Centric & fine Grained data Access using ABE".

[21] Jason Crampton, Keith Martin & Peter Wild, "On Key Assignment for Hierarchical Access Control", Information security Group Royal Holloway, University of London, UK.

[22] Minu George, Dr. C. Suresh Gnanandhas, Saranya. K, "A Survey on Attribute Based Encryption Scheme in Cloud Computing" Department of CSE, Vivekanandha College Of Engineering for Women, Tamil Nadu, India

[23] "Cryptographic Hierarchical Access Control for Dynamic Structures" by Arcangelo Castiglione, Alfredo De Santis, Member, IEEE, Barbara Masucci, Francesco Palmieri, Aniello Castiglione, Member, IEEE, and Xinyi Huang