A Review: Cryptographically Efficient, Dynamically Strong, Securely proven Optimal and hybrid Hierarchal Access Control System

Mrs. Smita Parte,
Assistant Professor (IT) Technocrats Institute of Technology, Bhopal, MP

Dr. Durgesh Kumar Mishra,
Professor and Head (CSE), Director, Microsoft Innovation Center,
Shri Arbindo Institute of Technology, Indore, MP, India. Visiting Professor, IIT Indore

Abstract: This paper is the review paper mentioning all methods related to hierarchal access control. In this digital era Hierarchal access control mechanism basically it is very much needed in all sorts of government and private organizations. Access control system is the set of methods have ability to ensure that only authorized users of computer system are given access to some sensitive resources. In this system users are organized in hierarchy formed by security clearance as per their capabilities and responsibility called security classes which are disjoint. With this review paper it is proposed- to use different authentication algorithms to get a hybrid kind of access control which would be secure utmost and support dynamic updates.

Keywords: Hierarchal access control, poset.

INTRODUCTION:

Today is the time of computer communication systems. An enhancement in information system and communication technologies brings with numerous benefits but also there are security issues. Information security is very important topic in the computer communication system.

The multilevel information security problems originally exists in military and government organization as well as in some private corporations where classified and well categorized data management is necessary but in present the popularity of computer networks and very fast progress of computer technologies on a multiuser system make sharing of expensive resources in a reality. In multiuser computing environment the problem of access control to system resources can be an important research area. Since sharing of resources may cause some undesired things such as unauthorized access and inconsistent status of shared resources and frequently occur in database management system, computer network and operating system. Therefore an important issue in multiuser computer environment is the question of how to control the access to computers.

Main emphasis is given to the situation where users are categorized into several privilege classes and organized into a hierarchal structure. Another thing is how to identify whether a user has enough privileged to retrieve the data item or change the access rights of the other user.

In today's time data no longer resides on computer system which is physically isolated within that organization where physical security measures can be taken to safeguard the data and that computer system so solutions are oriented towards the open interconnected environment where storage are outsourced and operations are done on third un trusted party. So open access data storage imposes new security challenges.

To facilitate current development and discovered security issues. We need to develop such a security model which should be data centric where information is protected cryptographically and allowed to travel on the network freely. There is a need of information replication in area like grid computing, distributed system, database management system and enterprise right management system and this replicated information is sent to the user .Since information is very sensitive so privacy and security have to be taken care of.

In many organizations security problem exists where multiple levels of access control are present or we can say hierarchal structure of data sensitivity or privilege exists together like in military and government institutions.

Hierarchal access control mechanism- in this basically access control system is the set of methods have ability to ensure that only authorized users of computer system are given access to some sensitive resources. Users are organized in hierarchy formed by security clearance as per their competency and responsibility called security classes which are disjoint .Why there is hierarchy since some users in a particular organization have more access rights than others in reality. For example in hospital management system doctors are allowed to access data related to patients such as diagnosis, prescription, medication and laboratory tests on the other hand a researcher can be limited to clinical information.

Section 1- Introduction tells how and why this method is needed. Section 2- Literature survey – chronological work under this topic then in rest of the sections proposed method along with all functionalities is there.

LITERATURE SURVEY:

2-In 1982 Akl and Taylor[2] "Cryptographic Solution to a Problem of Access Control in a Hierarchy". This scheme suggests an elegant solution in a poset hierarchy for the access control. Each security class Ci is assigned a distinct prime to be its public parameter PB_i The each security class C_i a secret key K_i is calculated with the help of PB_i .The

data item contained by class C_i is encrypted by a secret key generated by cryptosystem K_i known as enciphering key. This information can accessed only by C_j where $C_i \leq C_j$. With the help of K_j and public parameter PB_i and PBj and the secret key K_j ,C_j can derive K_i to decipher the data item owned by C_i.

Advantage-It support access control in Poset hierarchy

Disadvantage-A large amount of storage is required to store public parameter

3-In 1982 MacKinnon,Taylor and Akl[3] "An Optimal Algorithm for Assigning Cryptographic Keys to Control Access in a Hierarchy".This paper presentd a improved scheme for Akl-Taylor method called canonical assignment to reduce the value of public parameter. This method reduces the number of values of public parameter.

Advantage-It support access control in Poset hierarchy and less storage as compare to Akl-Taylor scheme

Disadvantage-Still requires large amount of storage to store public parameter and difficult to compute optimal canonical algorithm

4-In 1988 Sandhu [4]"Cryptographic Implementation of a Tree Hierarchy for Access Control",He used one-way function to create a cryptographic access control in tree hierarchy. And as we know tree hierarchy is special case of poset hierarchy. In this method for each security class C_i ,a K_i a security key is generated with the help of its own identity and its immediate ancestor's secret key by a one way function.

Advantage-No extra public parameter is needed to derive keys

Disadvantage- Computational overhead is involved to derive keys and this method is only for tree hierarchy

5-In 1990 Harn and Lin[5] ,"A Cryptographic Key Generation Scheme for Multilevel Data Security". This method is same as Akl and Taylor scheme but instead of using top-down design approach as in Akl-taylor scheme they used botton-up approach

Advantage-Smaller storage is required for most of the security classes

Disadvantage-If numbers of security classes are more than large storage space is required to store public parameter for each security class

6-In1992 C C Chang, R J Hwang and T C Wu[6], "Cryptographic Key Assignment Scheme foe access control in a hierarchy Information System" proposed a method which is based on Newton's Interpolation method and a predefined one-way function.

Advantage-Modified method

Disadvantage-Computational overheads

7-In 1993 H. Liaw, S. Wang, and C. Lei[7], "A Dynamic Cryptographic Key assignment Scheme in a Tree Structure" proposed a method which is based on Newton's Interpolation method and a predefined one-way function.

Advantage-Modified method

Disadvantage-Computational overheads

8- In 1993 H T Liaw and C L Lei[8] , "An Optimal Algorithm to assign Cryptographic keys in a tree structure for Access Control" presented an optimal algorithm for assigning cryptographic keys in a tree structure for multilevel data security. Uses top-down approach for key assignment

Advantage-Simple and efficient in deriving keys

Disadvantage-Requires large storage

9-In1993 M S Hwang and W P Yang [9], "Attacks on a Dynamic Cryptography Key Assignment Sheme" discussed possible attacks

10-In C.-H. Lin[10], "Dynamic Key Management Schemes for Access Control in a Hierarchy."

11-In 1997 H. Min-Shiang[11], "A Cryptographic Key Assignment Scheme in a Hierarchy for Access Control" presented an access control scheme for a partially –ordered hierarchy by modifying Liaw-Lei's scheme which can only be used in tree structure

Advantages-Generalized for poset structure and provided security analysis

Disadvantage-Prevent cooperative attacks

12-In 1972 A V Aho, M R Garey, and J D Ullman[12], "The Transitive Reduction of a Directed Graph" calculated transitive closure foe DAG

Advantages-Economical and shown time complexity for best algorithm for it.

Disadvantge- Computational overheads in calculating Transitive Reduction but this is tradeoff between other things

Later on many researchers have subsequently proposed schemes that either have better performance or different ways to evaluate the transitive reduction for example [13],[14],[15],[16],[17],[18],[19]and [20]

28, 32-In 2005-2006 Atallah et al.[29],[33]first addressed the problem of formalizing security requirement for hierarchical key assignment scheme and proposed two concepts security against key discovery and with respect to key indistinguishability Former captures the notion that to which adversary not having access for that it cannot compute key and latter says that adversary should not be able to distinguish between a real key and same length of random string. Different scheme and construction satisfying the above defined concept of security was subsequently proposed in [40], [42], [44], [46], and [48].

50-In 2013 Freire et al[51] proposed a new security definition for hierarchical key assignment schemes. Such definition, called security against strong key recovery and security with respect to key indistinguishability and provide additional compromise capability for adversary. Suggested clear separated notion of security between key recovery and key indistinguishability

53-53 In [53] and[54] it has been proven that security with respect to strong key indistinguishability is not as stronger as compare to key indistinguishability. Same types of results are shown in the unconditionally secure setting

In [31],[34],[35],[37],[40],[50] and [56] extended the security model proposed in[29] to such methods which satisfy additional time dependent constraints

In [54] and [60] A Castiglione et al proposed a more general scenario where the access control is not only hierarchal but also shared between different classes

E. Damiani et al[39] proposed "Selective data encryption in outsourced dynamic environments" and generated

solution based on selective encryption which exploits hierarchal access control schemes.
De Capitani di Vimercati et al [38] also proposed a solution based on selective encryption, for the enforcement of access control and management of is evolution.
C Bulndo et al [45]proposed a heuristic approach to minimize the number of keys which are stored in system and distributed to different users[22],[23],[24],[25],[26],[27],[28],[32,][35],[36],[41],[42],[47],[49],[51],[52],[57],[58],[59] and [60] are some proposed methods for access control but all these methods are based on static adversary means they are fixed and immutable more precisely we can say that adversary are not allowed to make any changes to the hierarchy which is fixed and chosen at the time of attack. And this is remarkable limitation of all above mentioned access control scheme and existing models are no capable to characterize many situation which can arise in different operating environment

OBJECTIVE OF RESEARCH:

To study and analyze all theoretical concepts, application and current problem of information security in depth for multi level authentication. Then design and develop an efficient, dynamic and strongly proven hybrid security model for hierarchal access control.

STATEMENT OF THE PROBLEM:

In case of data centric protection model in multi user environment means there are multiple user are using shared resources which are present in distributed manner. Here multiple users obviously structured into multiple levels or hierarchal manner. Since each user is having different rights to access different kinds of data items, in this manner we can say there is a categorized or classified data storage management system where it is clearly mentioned that which user is accessing what. So for having this we need to implement a proper protection system. This is achieved by standard encryption system and when data is encrypted we need to impose proper access policies to make access to that encrypted data .We need to design a standard access control model for this.
By studying all literature and information security theory a direct solution to above mentioned problem comes into mind is enforce access control with cryptography is to encrypt data with a data key means what data is being accessed by which user is get protected by a securely assigned key.
In this manner each user is authorized for that specific data whenever to user want access that data with assigned encrypted key. Here we can see that one to one mapping between user and data item since user can access only that data for which he is having key. But what happen when a user wants access to other data item for which he is not having key. In many government institutions, private corporations and military organizations there is hierarchal arrangement of different category of user for accessing the data shown in figure given below

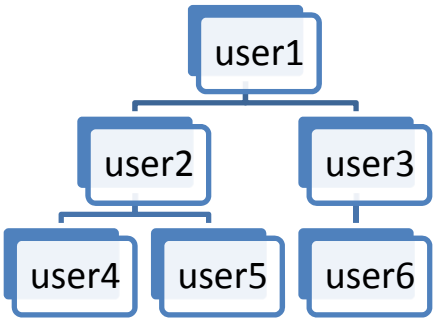

Figure1: Hierarchal arrangement of users

What above figure depict is actually user1 can access his own data but being on top in the hierarchy user1 can control or administer all other user below him in hierarchy. Same principle is for rest of the users. We need to maintain this since this is categorized according to their competency, responsibility or position held in hierarchy. This is actually known as hierarchal access or multi level access.
But thing is that how we can achieve this in practical. As we have discussed earlier that each user is having his/her personal key to access destined data but we also need to provide access to upper users and for this upper user must have key. If we provide key to all upper users for data item of lower users in hierarchy then what happens is – there are multiple copies of data keys are generated encrypted with different user keys. The number of copies of a single data key can reach to the number of users in the system. This number can increase the size of protected data itself. So it highly needed that when upper user in hierarchy wants to access data of user at lower level in hierarchy only that time upper user have that key otherwise not. Although this method increases computational overhead but greatly reduces storage requirements.
For this we need to maintain access configuration list "which user access what with proper granularity". Whole data is maintain by a data set denoted by D={d1,d2…..dn} and all users are assigned to privilege security classes denoted by C1,C2,……Cn and particularly users are denoted by set U={u1,u2……un}.This Hierarchal structure is depicted by poset partially ordered set.
In this proposed system one more thing we can add transitive exception and anti symmetric exception, what happens in this is it is not necessary that user1 can have access to user2 and subsequent users as happens traditionally but have access to user3 and user6 and in some cases user3 can have access to access user2's data item. For achieving security we can use more than one encryption algorithm in succession and combination so that we can get highest level of security and have a hybrid kind of access control system. Keys are different at different time for authenticating data items,a different key version we can assign at different time period.
Once this hierarchal access control system is developed .We need to take care of dynamic updates like run time insertion of a class or user. Run time deletion of a class or user. New access priorities need to be set etc.

MOTIVATIONAL FACTORS:

i. First motivation for this problem domain is my ME thesis topic "Study and Implementation of Multi-Criterion Authentication to Secure Mobile Payment System" in which I had worked on multiple authentication criteria like a) User-id password b) Encrypted keys c) A message comes on mobile to take permission for transaction
ii. Second motivation is - fast pace of internet usage via Wi-Fi needs good level of security since different types of users are acquiring access to different data items in present time of internet of things
iii. Thirdly- remote usage of shared resources like printer scanner etc. needs proper and efficient access control system.

FUNCTIONALITIES:

i. Efficient strong time bounded key generation algorithm need to be designed.
ii. An algorithm which assign time stamp to generated key to keep different versions of key for a data item.
iii. Efficient secure key distribution algorithm need to be designed.
iv. Need to formalize a security policy for hierarchal key assignment.
v. Need to combine different encryption algorithm to get hybrid one.
vi. A generalized poset structure needs to be developed for hierarchal arrangement of user classes.
vii. Need to compute a minimal representation for poset structure for less time and space requirement.
viii. Need to develop a method which can access data items in decentralized manner.
ix. Need to support dynamic updates to the poset structure with minimum computation overheads.
x. Need to design algorithm for dynamic updates.
xi. Need to develop attack simulations for testing the designed system.
xii. To protect overall system a strong cryptographic concepts need to apply.
xiii. Above all it is needed to keep system simple, efficient and easy to understand.

REFERENCES:

1. Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci Francesco Palmieri,, Aniello Castiglione Xinyi Huang,"Cryptographic Hierarchical Access Control for Dynamic Structures"IEEE transaction june 2016
2. S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans. Comput. Syst., vol. 1, no. 3,239–248, 1983
3. S. J. MacKinnon, P. D. Taylor, H. Meijer, and S. G. Akl, "An Optimal Algorithm for Assigning Cryptographic Keys to Control Access in a Hierarchy," IEEE Trans. Computers, vol. 34, no. 9, pp. 797–802, 1985.
4. R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Inf. Process. Lett., vol. 27, no. 2, pp. 95–98, 1988
5. L. Harn and H. Lin, "A Cryptographic Key Generation Scheme for Multilevel Data Security," Computers & Security, vol. 9, no. 6, pp. 539– 546, 1990.
6. C C Chang, R J Hwang and T C Wu, "Cryptoghraphic Key Assignment Scheme foe access control in a hierarchy Information System," 17 (3), 243-247(1992)
7. H T Liaw, S. Wang, and C. Lei, "A Dynamic Cryptographic Key Assignment Scheme in a Tree Structure," Computers & Mathematics with Applications, vol. 25, no. 6, pp. 109 – 114, 1993
8. H T Liaw and C L Lei , "An Optimal Algorithm to assign Cryptographic keys in a tree structure for Access Control," BIT 33 46-56,(1993)
9. M S Hwang and W P Yang , "Attacks on a Dynamic Cryptography Key Assignment Sheme ,"IEEE Electornics Letter 29(24),2095-2096,(Nov 1993)
10. C.-H. Lin, "Dynamic Key Management Schemes for Access Control in a Hierarchy," Computer Communications, vol. 20, no. 15, pp. 1381 – 1385, 1997.
11. H. Min-Shiang, "A Cryptographic Key Assignment Scheme in a Hier-archy for Access Control," Math. Comput. Model., vol. 26, no. 2, pp. 27–31, Jul. 1997
12. A. V. Aho, M. R. Garey, and J. D. Ullman, "The Transitive Reduction of a Directed Graph," SIAM J. Comput., vol. 1, no. 2, pp. 131–137, 1972.
13. S. Goldwasser and S. Micali, "Probabilistic Encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.
14. M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudorandom bits," SIAM J. on Computing, vol. 13, pp. 850–864, 1984.
15. O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," J. of the ACM, vol. 33, no. 4, pp. 792–807, 1986.
16. J. A. L. Poutre´ and J. van Leeuwen, "Maintenance of Transitive Closures and Transitive Reductions of Graphs," in Graph-Theoretic Concepts in Computer Science, International Workshop, WG '87, Kloster Banz/Staffelstein, Germany, June 29 - July 1, 1987, Proceedings, ser. Lecture Notes in Computer Science, H. Gottler¨ and H. J. Schneider, Eds., vol. 314. Springer, 1987, pp. 106–120.
17. G. F. Italiano, "Finding Paths and Deleting Edges in Directed Acyclic Graphs," Information Processing Letters, vol. 28, no. 1, pp. 5–11, 1988.
18. S. Goldwasser, S. Micali, and R. L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Comput., vol. 17, no. 2, pp. 281–308, 1988.
19. M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in CRYPTO 1996, LNCS, vol. 1109, 1996, pp. 1–15.
20. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in The 38th IEEE Symp. on Foundations of Comp. Sci., 1997, pp. 394–403.
21. C. Lin, "Hierarchical key assignment without public-key cryptography," Computers & Security, vol. 20, no. 7, pp. 612–619, 2001.
22. V. R. L. Shen and T. Chen, "A novel key management scheme based on discrete logarithms and polynomial interpolations," Computers & Security, vol. 21, no. 2, pp. 164–171, 2002
23. A. L. Ferrara and B. Masucci, "An information-theoretic approach to the access control problem," in Theoretical Computer Science, 8th Italian Conference, ICTCS 2003, Bertinoro, Italy, October 13-15, 2003, Proceedings, ser. Lecture Notes in Computer Science, C. Blundo and C. Laneve, Eds., vol. 2841. Springer, 2003, pp. 342–354
24. M. Naor and O. Reingold, "Number-theoretic constructions of efficient pseudo-random functions," J. of the ACM, vol. 51, no. 2, pp. 231–262, 2004.
25. C. Yang and C. Li, "Access control in a hierarchy using one-way hash functions," Computers & Security, vol. 23, no. 8, pp. 659–664, 2004.
26. A. De Santis, A. L. Ferrara, and B. Masucci, "Cryptographic Key Assignment Schemes for any Access Control Policy." Information Pro-cessing Letters, vol. 92, no. 4, pp. 199–205, 2004.
27. T. Chen and J. Huang, "A novel key management scheme for dynamic access control in a user hierarchy," Applied Mathematics and Computa-tion, vol. 162, no. 1, pp. 339–351, 2005.
28. A. De Santis, A. L. Ferrara, and B. Masucci, "A new key assignment scheme for access control in a complete tree hierarchy," in Coding and Cryptography, International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers, ser. Lecture Notes in Computer Science, Ø. Ytrehus, Ed., vol. 3969. Springer, 2005, pp. 202–217.
29. M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and Efficient Key Management for Access Hierarchies," in Proceedings of the 12th ACM Conference on Computer and Communications

Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005, V. Atluri, C. Mead-ows, and A. Juels, Eds. ACM, 2005, pp. 190–202.
30. A. De Santis, A. L. Ferrara, and B. Masucci, "Unconditionally Secure Key Assignment Schemes," Discrete Applied Mathematics, vol. 154, no. 2, pp. 234–252, 2006.
31. "Enforcing the Security of a Time-Bound Hierarchical Key Assignment Scheme," Inf. Sci., vol. 176, no. 12, pp. 1684–1694, 2006.
32. J. Katz and M. Yung, "Characterization of Security Notions for Prob-abilistic Private-Key Encryption," J. of Cryptology, vol. 19, pp. 67–95, 2006.
33. M. J. Atallah, M. Blanton, and K. B. Frikken, "Key Management for Non-Tree Access Hierarchies," in SACMAT 2006,11th ACM Symposium on Access Control Models and Technologies, Lake Tahoe, California, USA, June 7-9, 2006, Proceedings, D. F. Ferraiolo and I. Ray, Eds. ACM, 2006, pp. 11–18.
34. G. Ateniese, A. De Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," in Proceedings of the 13th ACM Conference on Computer and Communica-tions Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006, A. Juels, R. N. Wright, and S. D. C. di Vimercati, Eds. ACM, 2006, pp. 288–297
35. A. De Santis, A. L. Ferrara, and B. Masucci, "New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," in SACMAT 2007, 12th ACM Symposium on Access Control Models and Technologies, Sophia Antipolis, France, June 20-22, 2007, Proceedings, V. Lotz and B. M. Thuraisingham, Eds. ACM, 2007, pp. 133–138.
36. A. De Santis, A. L. Ferrara, and B. Masucci, "Efficient Provably-Secure Hierarchical Key Assignment Schemes," in Mathematical Foundations of Computer Science 2007, 32nd International Symposium, MFCS 2007, Cesky´ Krumlov, Czech Republic, August 26-31, 2007, Proceedings, ser. Lecture Notes in Computer Science, L. Kucera and A. Kucera, Eds., vol. 4708. Springer, 2007, pp. 371–382.
37. M. J. Atallah, M. Blanton, and K. B. Frikken, "Incorporating Tempo-ral Capabilities in Existing Key Management Schemes," in Computer Security - ESORICS 2007, 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24-26, 2007, Proceedings, ser. Lecture Notes in Computer Science, J. Biskup and J. Lopez, Eds., vol. 4734. Springer, 2007, pp. 515–530.
38. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and K Samarati "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23-27, 2007, C. Koch, J. Gehrke, M. N. Garofalakis, D. Srivastava, Aberer, A. Deshpande, D. Florescu, C. Y. Chan, V. Ganti, C. Kanne, w klas and E. J.N euhold Eds. ACM, 2007, pp. 123–134
39. E. Damiani, S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Selective data encryption in outsourced dynamic environments," Electr. Notes Theor. Comput. Sci., vol. 168, pp. 127– 142, 2007.
40. A. De Santis, A. L. Ferrara, and B. Masucci, "New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," Theor. Comput. Sci., vol. 407, no. 1-3, pp. 213–230, 2008.
41. A. V. D. M. Kayem, S. G. Akl, and P. Martin, "On replacing cryptographic keys in hierarchical key management systems," Journal of Computer Security, vol. 16, no. 3, pp. 289–309, 2008.
42. M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, 2009.
43. P. D'Arco, A. De Santis, A. L. Ferrara, and B. Masucci, "Security and Tradeoffs of the Akl-Taylor Scheme and Its Variants," in Mathematical Foundations of Computer Science 2009, 34th International Symposium, MFCS 2009, Novy Smokovec, High Tatras, Slovakia, August 24-28, 2009. Proceedings, ser. Lecture Notes in Computer Science, R. Kralovic´ and D. Niwinski, Eds., vol. 5734. Springer, 2009, pp. 247–257.
44. "Variations on a theme by Akl and Taylor: Security and Tradeoffs," Theor. Comput. Sci., vol. 411, no. 1, pp. 213–227, 2010.
45. C. Blundo, S. Cimato, S. D. C. di Vimercati, A. De Santis, S. Foresti,S Paraboschi and P. Samarati, "Managing key hierarchies for access control enforcement: Heuristic approaches," Computers & Security, vol. 29, no. 5, pp. 533–547, 2010.
46. A. De Santis, A. L. Ferrara, and B. Masucci, "Efficient Provably-Secure Hierarchical Key Assignment Schemes," Theor. Comput. Sci., vol. 412, no. 41, pp. 5684–5699, 2011.
47. J. Lo, M. Hwang, and C. Liu, "An efficient key assignment scheme for access control in a large leaf class hierarchy," Inf. Sci., vol. 181, no. 4, pp. 917–925, 2011.
48. E. S. V. Freire and K. G. Paterson, "Provably Secure Key Assign-ment Schemes from Factoring," in Information Security and Privacy - 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings, ser. Lecture Notes in Computer Science, U. Parampalli and P. Hawkes, Eds., vol. 6812. Springer, 2011, pp. 292–309.
49. J. Lo, M. Hwang, and C. Liu, "An efficient key assignment scheme for access control in a large leaf class hierarchy," Inf. Sci., vol. 181, no. 4, pp. 917–925, 2011.
50. G. Ateniese, A. De Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryp-tology, vol. 25, no. 2, pp. 243–270, 2012
51. E. S. V. Freire, K. G. Paterson, and B. Poettering, "Simple, Efficient and Strongly KI-Secure Hierarchical Key Assignment Schemes," in Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA, February 25-March 1, 2013. Proceedings, ser. Lecture Notes in Computer Science, E. Dawson, Ed., vol. 7779. Springer, 2013, pp. 101–114.
52. G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Keccak," in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual Interna-tional Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, T. Johansson and P. Q. Nguyen, Eds., vol. 7881. Springer, 2013, pp. 313–314.
53. A. Castiglione, A. De Santis, and B. Masucci, "Hierarchical and Shared Key Assignment," in 17th International Conference on Network-Based Information Systems, NBIS 2014, IEEE, 2014, pp. 263–270.
54. A. Castiglione, A. De Santis, and B. Masucci, "Key Indistinguishability vs. Strong Key Indistinguishability for Hierarchical Key Assignment Schemes," IEEE Trans. Dependable Sec. Comput., 2015.
55. M. Cafaro, R. Civino, and B. Masucci, "On the equivalence of two security notions for hierarchical key assignment schemes in the uncon-ditional setting," IEEE Trans. Dependable Sec. Comput., vol. 12, no. 4, pp. 485–490, 2015.
56. J.-S. Pan, T.-Y. Wu, C.-M. Chen, and E. K. Wang, "An efficient solution for time-bound hierarchical key assignment scheme," in Genetic and Evolutionary Computing. Springer, 2015, pp. 3–9.
57. Y.-F. Chang, "A flexible hierarchical access control mechanism enforcing extension policies," Security and Communication Networks, vol. 8, no. 2, p 189–201, 2015.
58. A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, and A. Castiglione, "On the Relations Between Security Notions in Hierarchical Key Assignment Schemes for Dynamic Structures," in Proceedings of the 21st Australasian Conference on Information Security and Privacy - ACISP 2016, Part II, Melbourne, Australia, Lecture Notes in Computer Science, Springer Verlag., vol. 9723, 2016, pp. 1–18. Springer, 2015, pp. 3–9.
59. C.-C. Lee, C.-T. Li, S.-T. Chiu, and S.-D. Chen, "Time-bound key-aggregate encryption for cloud storage," Security and Communication Networks, 2016.
60. A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, and X. Huang, "Hierarchical and shared access control," IEEE Trans. Information Forensics