Enhanced Cloud Data Storage with Flexible and Fine-Grained Attribute-Based Access Control

[1]Dr B.GOPI, [2]CHENNURU GOGUL CHANDHU, [3]RAVULA BHANU PRAKASH

[1]Associate Professor, Dept. of MCA, Krishna Chaitanya Institute of Science And Technology, Kakutur, Nellore, AP,India.

[2]PG Student, Dept. of MCA, Krishna Chaitanya Institute of Science And Technology, Kakutur, Nellore, AP,India.

[3]PG Student, Dept. of MCA, Krishna Chaitanya Institute of Science And Technology, Kakutur, Nellore, AP,India.

ABSTRACT_ The growing use of cloud computing has made data outsourcing to cloud servers a hot topic. Attribute-based encryption, or ABE, was suggested and implemented in cloud storage systems to provide security and accomplish flexible fine-grained file access control. However, the main problem with ABE schemes is user revocation. In this paper, we present an efficient user revocation technique for cloud storage systems using ciphertext-policy attribute-based encryption (CP-ABE). The idea of a user group can be introduced to effectively tackle the problem of user revocation. The group manager will update each user's private key when they depart, with the exception of those whose access has been revoked. Furthermore, because the CP-ABE technique rises linearly with the access structure's complexity, it has a high computational cost. We outsource heavy calculation loads to cloud service providers in order to lower computation costs without disclosing file contents or secret keys. Interestingly, our system is resistant to collusion attacks carried out by banned users collaborating with active users. We demonstrate the security of our approach based on the Diffie-Hellman (DCDH) assumption of divisible computation. Our experiment's outcome demonstrates that the computing cost for local devices can be constant and is quite low. Our plan works well on smartphones with limited resources.

1.INTRODUCTION

Cloud computing is regarded as a prospective computing paradigm in which resource is supplied as service over the Internet. It has met the increasing needs of computing resources and storage resources for some enterprises due to its advantages of economy, scalability, and accessibility. Recently, several cloud storage services such as Microsoft Azure and Google App

Engine were built and can supply users with scalable and dynamic storage. With the increasing of sensitive data outsourced to cloud, cloud storage services are facing many challenges including data security and data access control. To solve those problems, attribute-based encryption (ABE) schemes [1-3] have been applied to cloud storage services. Sahai and Waters [1] first proposed ABE scheme named fuzzy identity-based encryption which is derived from identity-based encryption (IBE) [4]. As a new proposed cryptographic primitive, ABE scheme not only has the advantage of IBE scheme, but also provides the character-istic of "one-to-m any" encryption. Presently, ABE mainly includes two categories called ciphertext -policy ABE (CP-ABE) [2] and key-policy ABE (KP-ABE) [3]. In CP-ABE, ciphertexts are associated with access policies and user's private keys are associated with attribute sets. A user can decrypt the ciphertext if his attributes satisfy the access policy embedded in the ciphertext. It is contrary in KP-ABE. CP-ABE is more suitable for the outsourcing data architecture than KP-ABE because the access policy is defined by the data owners. In this article, we pr esent an efficient CP-ABE with user revocation ability.

2.LITERATURE SURVEY

2.1 Ciphertext-policy attribute based encryption

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In a few disseminated frameworks a client ought to possibly have the option to get to information if a client groups a specific arrangement of certifications or traits. As of now, the main strategy for implementing such strategies is to utilize a confided in server to store the information and intercede access control. In any case, in the event that any server putting away the information is compromised, the classification of the information will be compromised. In this paper we present a framework for acknowledging complex access control on scrambled information that we call Ciphertext-Strategy Property Based Encryption. By utilizing our methods encoded information can be kept secret regardless of whether the capacity server is untrusted; in addition, our strategies are secure against conspiracy assaults. Past Quality Based Encryption frameworks utilized properties to portray the scrambled information and incorporated strategies into client's keys; while in our framework credits are utilized to portray a client's qualifications, and a party encoding information decides a

strategy for who can unscramble. Accordingly, our strategies are adroitly nearer to customary access control techniques, for example, Job Based Admittance Control (RBAC). Moreover, we give an execution of our framework and give execution estimations.

2.2 Getting correspondences between outside clients and remote body region organizations

Creators: C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen,

Remote Body Region Organizations (Boycotts) are supposed to assume a pivotal part in understanding wellbeing checking sooner rather than later. Laying out secure correspondences between Boycott sensors and outside clients is critical to tending to the pervasive security and protection concerns.

In this paper, we propose the crude capabilities to execute a mystery sharing based Ciphertext-Strategy Property Based Encryption (CP_ABE) plot, which scrambles the information in view of an entrance structure determined by the information source. We likewise plan two conventions to safely recover the delicate patient information from a Boycott and train the sensors in a Boycott. Our investigation shows that the proposed plot is doable, can give message credibility, and can counter conceivable significant goes after, for example, agreement assaults and battery-depleting assaults.**2.3 Exploiting prediction to enable secure and reliable routing in wireless body area networks**

AUTHORS: X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuan

In this paper, we propose a dispersed Expectation based Secure and Dependable steering system (PSR) for arising Remote Body Region Organizations (WBANs). It tends to be coordinated with a particular steering convention to work on the last's dependability and forestall information infusion assaults during information correspondence. In PSR, utilizing past connection quality estimations, every hub predicts the nature of each and every coincidental connection, and subsequently any adjustment of the neighbor set too, for the short term. At the point when there are different conceivable next bounces for parcel sending (as indicated by the steering convention utilized), PSR chooses the one with the most elevated anticipated interface quality among them. Uniquely custom-made lightweight source and information verification techniques are utilized by hubs to get information correspondence. Further, every hub adaptively empowers or cripples source verification as per anticipated neighbor set

change and expectation exactness to rapidly channel misleading source confirmation demands. We show that PSR essentially increments steering dependability and actually opposes information infusion assaults through inside and out security examination and broad recreation study.

3.PROPOSED SYSTEM

The main goal of this system is to create an effective user revocation CP-ABE method for cloud storage systems.

• Our goal is to simulate a collusion attack carried out by banned users collaborating with active users.

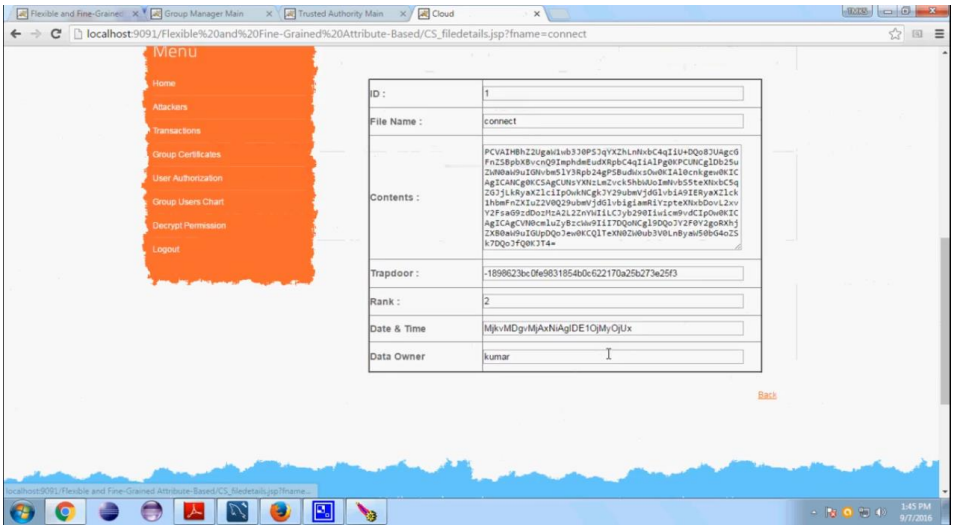
• In addition, we demonstrate that our system is CPA secure under the selective model and build an effective user revocation CP-ABE method by enhancing the current technique.
• We incorporate a certificate into each user's private key to address the current security vulnerability. Each user's group secret key is unique in this way, linked to his private key that is connected to certain attributes.

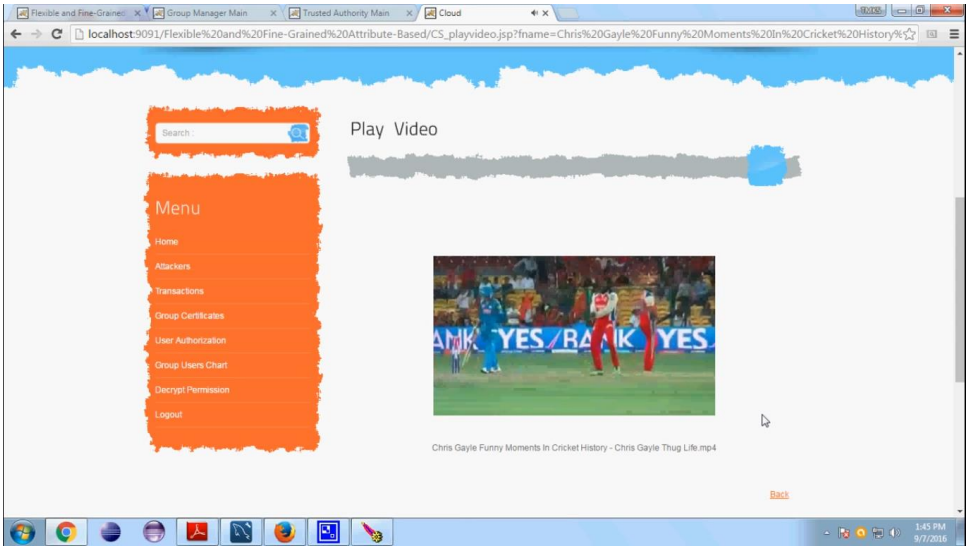
• We develop two cloud service providers, namely encryption-cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP), to lessen the computational strain on consumers.
• E-CSP is responsible for carrying out the outsourced encryption operation, and D-CSP is responsible for the outsourced decryption operation.
• During the encryption phase, E-CSP handles the sub-tree operation while local personnel handles the action related to the dummy attribute.

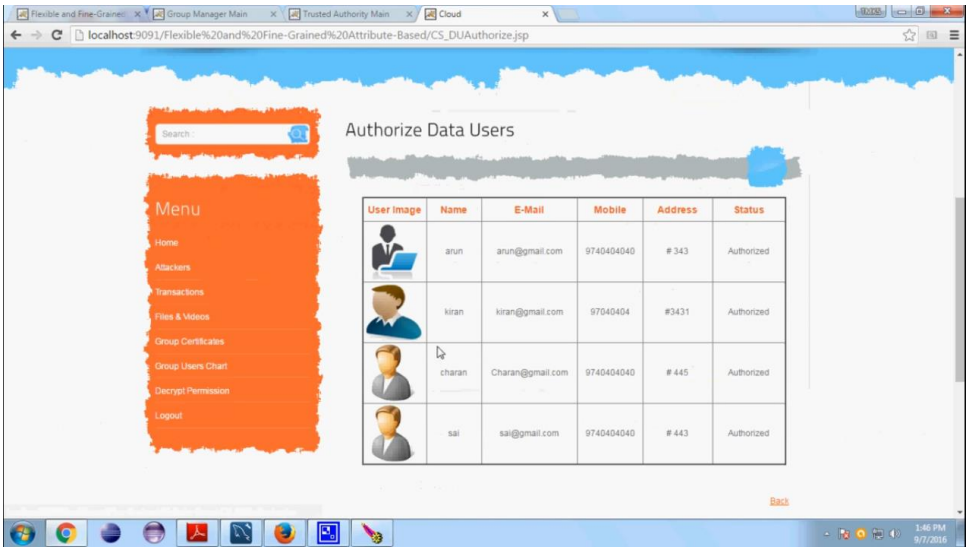
3.1 IMPLEMENTATION

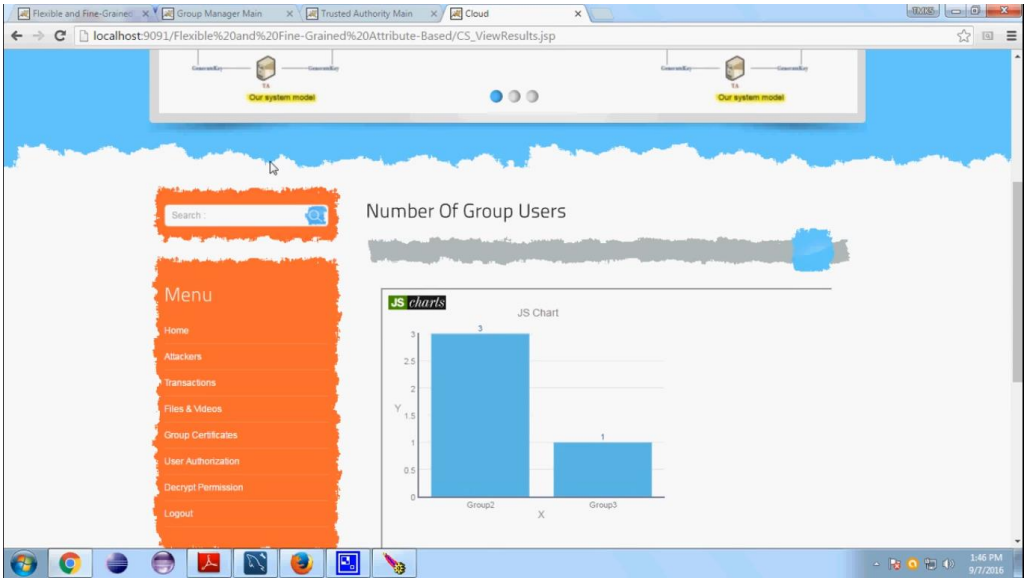
1. Data Owner
2. Cloud Server
3. Key Distribution center
4. Data Consumer/End User

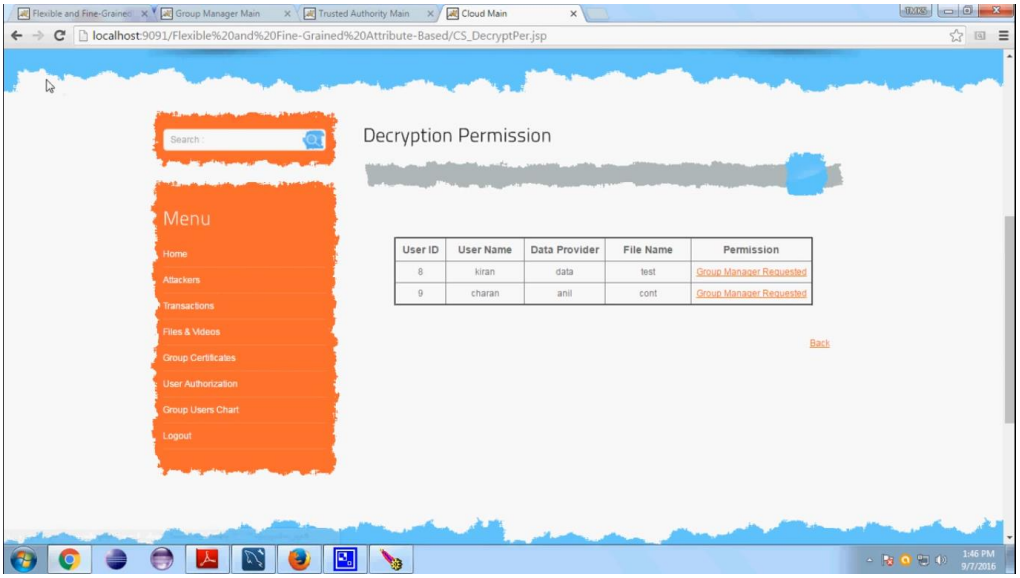
4.RESULTS AND DISCUSSION








localhost:9091/Flexible%20and%20Fine-Grained%20Attribute-Based/CS_ViewResults.jsp
Our system model
Our system model
Search :
Number Of Group Users
Menu
Home
Attackers
Transactions
Files & Videos
Group Certificates
User Authorization
Decrypt Permission
Logout
JS charts
JS Chart
Group2
Group3
X
Y


localhost:9091/Flexible%20and%20Fine-Grained%20Attribute-Based/CS_DecryptPer.jsp
Search :
Decryption Permission
Menu
Home
Attackers
Transactions
Files & Videos
Group Certificates
User Authorization
Group Users Chart
Logout
User ID
User Name
Data Provider
File Name
Permission
8
kiran
data
test
Group Manager Requested
9
charan
anil
cont
Group Manager Requested
Back


localhost:9091/Flexible%20and%20Fine-Grained%20Attribute-Based/TA_ViewAllVideos.jsp
Search :
All Videos
Menu
Home
Secret Key Requests
Secret Key Transactions
Logout
ID
File Name
Data Owner
Date & Time
6
ChillerParty.mp4
kumar
29/08/2016 18:04:29
8
Varadanayaka.mp4
kumar
29/08/2016 18:47:28
Back
collusion attack
attribute-based encryption
outsource decryption

5.CONCLUSION

We presented a formal definition and security model of CP-ABE with user revocation in this article. Based on the DCDH assumption, we also build a concrete CP-ABE method that is CPA secure. We incorporate a certificate into the user's private key to thwart collusion attacks. in order to prevent malicious users and banned users from merging their

private keys to create a working private key. To lessen the user's computing burden, we also outsource high-cost computation tasks to E-CSP and D-CSP. By using the outsourcing strategy, local devices' computation costs are significantly reduced and essentially fixed. Our experiment's findings demonstrate the effectiveness of our plan for devices with limited resources.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *EUROCRYPT '05*, LNCS, vol. 3494, pp. 457-473, 2005.

[2] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," *Proc. IEEE Symposium on Security and Privacy*, IEEE Transactions on Services Computing,Volume:PP,Issue:99,Date of Current Version:22.January.2016pp. 321-334, May 2007, doi: 10.1109/SP.2007.11.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based En-cryption for Fine-Grained Access Control of Encrypted Data," *Proc. 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586-615, 2003.

[5] A. Boldyreva, V. Goyal, and V. Kumar , "Identity-Based En-cryption with Efficient Revocation," *Proc. 15th ACM conference on Computer and communications security (CCS ' 08)*, pp. 417-426, 2008.

[6] S. Yu, C. Wang, K. Ren, and W. Lou , "Attribute Based Data Sharing with Attribute Revocation," *Proc. 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS ' 10)*, pp. 261-270, 2010.

[7] M. Yang, F. Liu, J. Han, and Z. Wang, "An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control," *Proc. 2011 International Conference on Instru-mentation, Measurement, Computer,*

Communication and Control, pp. 516-520, 2011.

[8] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applica-tions in Clouds," *IEEE Transactions on Cloud Computing*, pp. 172-186, 2013.

[9] J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," *IEEE Transactions on Parallel and Distributed Systems*, pp. 1214-1221, 2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scal-able, and Fine-Grained Data Access Control in Cloud Comp u-ting," *Proc. of IEEE INFOCOM '10*, pp. 1-9, 2010.

[11] M. Green, S. Hohenberger and B. Waters, "Outsourcing the decryp-tion of ABE ciphertexts," *Proc. 20th USENIX Conference on Security (SEC '11),* pp. 34, 2011.

[12] J. Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Ma and W.J. Lou, "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryp-tion," *Proc. 18th European Symposium on Research in Computer Security (ESORICS '13)*, LNCS 8134, Berlin: Springer-Verlag, pp. 592-609, 2013.

[13] J.W. Li, C.F. Jia, J. Li and X.F. Chen, "Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce," *Proc. 14th International Conference on Information and Communications Security (ICICS '12),* LNCS 7618, Berlin: Springer-Verlag, pp. 191-201, 2012. doi: 10.1007/978-3-642-34129-8_17

[14] M. Chase, "Multi-authority Attribute Based Encryption," *Proc. 4th Theory of Cryptography Conference (TCC '07)*, LNCS 4392, Berlin: Springer-Verlag, pp. 515-534, 2007.

[15] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen, "Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles," *Proc. 16th European Symposium on Research in Computer Security (ESORICS '11)*, LNCS 6879, Berlin: Springer-Verlag, pp. 278-297, 2011.

[16] J.G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentral-ized Key-Policy Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no.11, pp. 2150-2162, Nov 2012, doi: 10.1109/TPDS.2012.50.

[17] H.L. Qian, J.G. Li and Y.C. Zhang, "Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Ac-cess Structure," *Proc. 15th International Conference on Information and Communications Security (ICICS '13)*, LNCS 8233, Berlin: Springer- Verlag, pp. 363-372, 2013.

[18] H.L. Qian, J.G. Li, Y.C. Zhang and J.G. Han, "Privacy Preserv-ing Personal Health Record Using Multi-Authority Attribute- Based Encryption with Revocation," *International Journal of Information Security*, doi: 10.1007/s10207-014-0270-9.

[19] Z. Liu, Z.F. Cao and Duncan S. Wong, "Black-Box Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay," *Proc. 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS '13)*, pp. 475-486, 2013, doi: 10.1145/2508859.2516683.

[20] Z. Liu, Z.F. Cao and Duncan S. Wong, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures," *IEEE Transactions on Information Fo-rensics and Security*, vol. 8, no. 1, pp. 76-88, 2013, doi: 10.1109/TIFS.2012.2223683.

[21] J.T. Ning, Z.F. Cao, X.L. Dong, L.F. Wei and X.D. Lin, "Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Trace-ability," *Proc. 19th European Symposium on Research in Computer Security (ESORICS '14)*, LNCS 8713, Berlin: Springer-Verlag, pp. 55-72, 2014.

[22] J.D. Yu, P. Lu, Y.M. Zhu, G.T. Xue and M.L. Li, "Toward Secure Mul-tikeyword Top-k Retrieval over Encrypted Cloud Data," *IEEE Trans-actions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239-250, 2013, doi:10.1109/TDSC.2013.9

[23] T. Yang, P.P.C. Lee, J.C.S. Lui, R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903-916, 2012, doi: 10.1109/TDSC.2012.49

[24] L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE," *Proc. 14th ACM Conference on Computer and Communications Se-curity (CCS '07),* pp. 456-465, 2007, doi:10.1145/1180405.1180418.

[25] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil

Pairing," *CRYPTO '01*, LNCS, vol. 2139, pp. 213-229, Aug. 2001.

[26] A. Beimel, "Secure Schemes for Secret Sharing and Key Distr i-bution" PhD thesis, Israel Institute of Technology, 1996.

[27] M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atom-ic Proxy Cryptography," *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '98)*, LNCS 1403, Berlin: Springer-Verlag, pp. 127-144, 1998.

[28] A.D. Caro, "Java Pairing-Based Cryptography Library," http://gas.dia.unisa.it/projects/jpbc, 2013.

[29] B. Lynn, "Pairing-Based Cryptography (PBC) Library," http://crypto.stanford.edu/pbc, 2013.

[30] H.D Robert, F. Bao, H. Zhu, "Variations of Diffie-Hellman Problem," *Proc. 5th International Conference on Information and Com-munications Security (ICICS '03),* LNCS 2836, Springer-verlag, pp. 301-312, 2003