ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

Survey on Identity-Based Access Control for Big Data with Revocation Function

Tejashri Ekatpure [1], Vikas Nandgaokar [2]

P.G. Student, Department of Computer Network, PCET's NMIET, Pune, India[1]

Assistant Professor, Department of Compute Network, PCET's NMIET, Pune, India[2]

ABSTRACT: To be able to leverage huge knowledge to realize increased strategic insight, method improvement and build hep call, we need to be associate economical access management mechanism for ensuring end-to-end security of such data plus. Signcryption is one in every of several promising techniques to simultaneously achieve huge knowledge confidentiality and credibleness. However, signcryption suffers from the limitation of not having the ability to revoke users from a large-scale system with efficiency. We tend to proposes, in this paper, the primary identity-based (ID-based) signcryption theme with economical revocation moreover because the feature to source unsigncryption to change secure huge knowledge communications between data collectors and knowledge analytical system(s). Our scheme is designed to realize end-to-end confidentiality, authentication, non-repudiation, and integrity simultaneously, whereas providing scalable revocation practicality specified the overhead demanded by the non-public key generator (PKG) within the key-update part only will increase logarithmically supported the cardiality of users. Although in our theme the majority of the unsigncryption tasks are outsourced to associate untrusted cloud server, this approach will not have an effect on the protection of the planned theme. we tend to then prove the security of our theme, moreover as demonstrating its utility using simulations.

KEYWORDS: Access control, Big data, identity-based signcryption, revocation, verifiable outsourced computing.

I. INTRODUCTION

Big data analytics and big data is wide range of application such as biology, Internet of things, smart grid. The knowledge mined from this big dataset cannot only enhance the efficiency and reliability of the legacy grid, but also inform the strategic undertaken by the utility company to enhance consumer interaction.

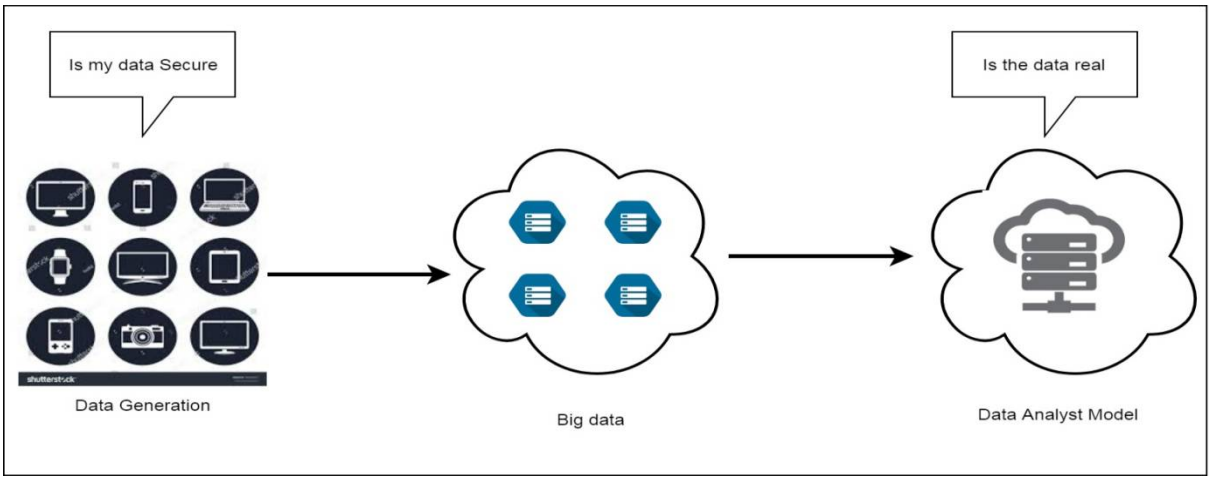

Fig 1: Security challenges in big data

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

As the data becomes bigger so it has data security and data privacy. Data security is one of the solution for the big data. Leakage of sensitive user data can be extremely loss to the individual concern as well as the organization, thus eroding the confidence of the users. The data can only be accessible by only authorized user. The system is crucial in guaranteeing confidentiality of these data. On the another way the without the capability to ensure the integrity, non-repudiation and authentication of big data, is the decision may be made on false or misleading information. Security solution of the big data is need to be scalable, volume, veracity and variety of the big data. Fig.1 shows security solution o the big data.

The data authenticity and confidentiality can be achieved using secure signature and encryption method. This provide confidentiality, integrity, non-repudiation and authentication, one can use the conventional "signature-then-encryption" strategy, which allows the sender to sign a message prior to encrypting the signed message. In th6is approach is not fit -for-purpose in a big data environment which requires real-time and large scale data processing.

So signcryption comes in a picture which provide both public key signature and encryption simultaneously and has been shown to outperform the traditional signature'-then'-encryption strategy. This improve speed of data processing. There are number of signcryption scheme designed for vehicle ad hoc network smart grid, wireless mobile network, secure email. The expensive certificate management inherent in a PKI(Public key Infrastructure) implementation, PKI'-based signcryption is not suitable for big data deployment. Therefore to eliminate the limitation of PKI, the security researcher have suggested a number of signcryption scheme designed for identity based public key cryptography(ID-PKC) system.

ID-based signcryption is potential solution for the secure communication in a big data environment. In the public key infrastructure the revocation is achieved by broadcasting certificate in the revocation function. But this method is not done for ID-PKC due to absence of public key certificate. Boneh and Franklin consist a method of an identity and a pre-determined time period. This revocation function is carried out by PKG, so PKG perform the key update information associated with each time interval. The non-revoked users are able to obtain short term secret keys in the current time interval by incorporating their own long-term private keys and key update information distributed by the PKG. Due to the need to support large scale data processing, it is important that the revocation function is also scalable without incurring significant computational overheads.

Cloud computing is another method of which enables on-demand and ubiquitous provision of configurable computing and storage resources in real-time and on an ad-hoc basis. Cloud computing allows one to outsource expensive computation tasks from the users to the cloud server in a pay-per-use fashion. The IBSC method users can benefit by leveraging the cloud to undertake expensive unsigncryption operations without the need for significant investment in hardware and software purchasing and maintenance. But in this the important thing is a receiver may receive a large number of messages from the sender, therefore it is design for the IB-SC scheme with unsigncryption outsourcing function.

Identity (ID)-based encryption, or IBE for short, is an exciting alternative to public-key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that makes publicly available the mapping between identities, public keys, and validity of the latter. The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption. The private keys of the users are issued by a trusted third party called the private key generator (PKG).

The main contribution of these paper is:

- A novel ID-based signcryption is with revocation functionality is based on the binary tress structure. The construction offers is the shorter cipher text size and faster signcryption. It is also achieve short term key exposure.
- The receiver can be offloaded to the untrusted cloude server. Then we also present key randomization and cipher text blinding.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

II. LITERATURE REVIEW

A. Secure Outsourcing of Attribute –Based Encryption

Extending the concept of IBE,A Sahai and B. Waters[11] provides flexible and different types of access control over encrypted data by enabling one-to-many encryption based on user attribute .To annihilate the decryption overhead on the user side, Green et al.[12] proposed on ABE paradigm equipped with outsourced decryption based on a key blinding technique . By applying the transformation key which is provided by user a semi-trusted cloud server is able to convert any ABE ciphertext into a ELGamal-style ciphertext without accessing the data or secrete keys. With the transformed ciphertext from the cloud server, the user can perform the complete decryption with a small computational overhead at the clients end. To determine correctness of the conversion carried out by the semi-trusted cloud server, Lai et al. [13] imported verifiability of the clouds decryption service and contingent a accurate construction using a parallel encryption technique. For correctness checking, a redundancy ciphertext is applied to the original ciphertext. Observing the bulky bandwidth and computation cost in[13], Lin et al.[14] and Mao et al.[15] provide alternative approaches to construct ABE equipped with verifiable outsourced decryption by by incorporating the idea of commitment independently. Ma et al.[16] proposed an ABE paradigm that support both outsourced decryption and encryption , and defined a new security notion of exculpability for the outsourced decryption to guarantee the user cannot “accuse” the cloud server of incorrect translation, while the cloud server performs the transformation honestly. To realize the strongest from of access policy, Xu et al.[17] put forward a circuit ABE scheme with verifiable decryption outsourcing based on the multi linear map. Although decryption outsourcing has been extensively studied in the ABE environment already, there is no IBSC, with unsigncryption outsourcing in the literature so far.

B. Revocable ID Based Cryptosystem

Since the seminal work of Boneh and Franklin [18], Boldyreva et al. [19] put forward the first IBE supporting an efficient revocation, named as scalable RIBE, based on fuzzy identity-based encryption [11] and the binary tree structure [22],such that the overload on the PKG side only increases with the cardinality of the users in logarithmic manner. This is a significant improvement to the solution in[18] since the overload of PKG in [19] grows linearly with cardinality of users. Inspired by the idea in[19] , Libert et al.[20] and Chen et al. [21] proposed an adaptive-identity secure and a lattice –based revocable IBE scheme, respectively .

By revisiting the security model for RIB, Seo and Emura [23],[24] identified the short-term private key exposure attack to demonstrate that the RIBE scheme in[19], [20], [21] are vulnerable to this attack and presented the RIBE scheme with short-term private key exposure resistance. Following [23], [24] , the RIBE scheme featured with key generation delegation [25],[26] and key-escrow elimination [27] have also been investigated. Revocable ID-based signature with short-term key exposure resilience was proposed in [24]. As far as we know, the only known revocable IB-SC scheme is reported in [28]. Unfortunately this scheme is far from being scalable and is vulnerable to a short-term key exposure attack. Thus constructing IBSC supporting efficient revocation and temporary key exposure resilience remains a research challenge.

III. SYSTEM ARCHITECTURE

Compared with the model for typical R-IBSC a cloud server is involved in the outsourced R-IBSC scheme. To provide authenticity and confidentiality in big data. The data generator are collecting large scale of the data from the distributed system is considered as the large scale sender. Data generator are(sender) send the data to the analytical system these data are the secure data. These analytical system extracting useful knowledge from the big data considered as the receiver. The analytical system is free from the heavy computational load. Data generator are sends the information analytical system these information is the secure information.

These message is transfer from the cipher text. In fig shows the PKG(Private key generator) The private key generator send the key to the data generator and analytical system. There are send two types of the key are sending. First is the private key and another is the updated key. Data generator send the some information to the analytical system. In the data generator there are number of users so these are using searching and ranking algorithm. The analytical system these are the secure computation outsource to the cloud . In the cloud they are stored secure data. A cloud server is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

maintained by semi-trusted third party to deliver redundant computing resource to the analytical system. During the outsourcing the analytical system sends the transformation key to the cloud. These are perform the operation to the unsincryption type algorithm. These are the cipher text. This architectural model is shown in the fig 2.

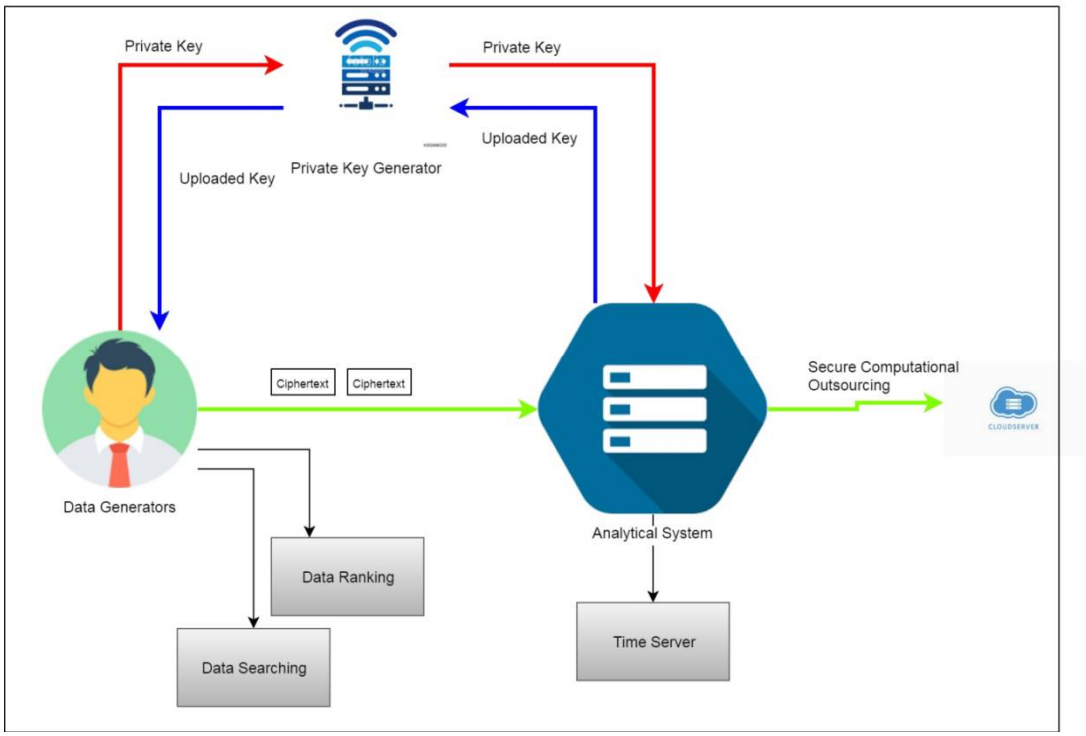

Fig 2: System model for the outsourced R-IBSC in big data paradigm.

It is desirable that the computational task carried out by the analytical system in the outsourcing unsingcryption should be strictly less than those performed in normal unsigncryption. The R-IBSC scheme is formally defined as follows.
A R-IBSC with verifiable Outsourced unsigncryption scheme is specified by the following eleven polynomial time algorithm.
Setup, IniKeyGen, KeyUpdate,KeyDer, Signcrypt, Unsigncrypt, Revoke, Setup.out, Ciphertext.ran, Transform.out, and Unsigncrypt.out
1) Setup, IniKeyGen, KeyUpdate,KeyDer, Signcrypt, Unsigncrypt, Revoke: These algorithm are identical to the R-IBSC scheme.
2) Setup.Out: On input params and the private key skIDr,T of receiver , this algorithm is carried out by the receiver to output transformation key tkIDr,T a corresponding retrieving key rkIDr,T and a string String contains the information needed in the outsourcing.
3) Ciphertext.ran: On input a normal ciphertext sigma, this algorithm is carried out by the receiver to generate a re-randomized ciphertext sigma hash.
4)Transform.out: On input params a randomizedciphertexts sigma hash , a transformation key tkIDr, the senders identity Ids and time period T,this algorithm is carried out by the cloud server to compute the transformed ciphertext sigma double hash.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

5)Unsigncrypt.out: This algorithm takes in input params, the retrieving key rkIDr,T, a normal ciphertext sigma and a transforme ciphertext sigma double hash , the outsourcing unsigncryption algorithm is performed by the receiver to output m or T in case sigma s valid.

IV. SYSTEM ANALYSIS

To achieve revocation function, the private key of user (data generator or Analytical system) comprises a fixed component associated with the identity (also called initial private key) and an updatable component corresponding with the time period (also named as updated key). The Signcrypt and Unsigncrypt algorithms can be performed exclusively by the user featured with both the initial private key and updated key. In case a user is revoked, PKG simply stops publishing updated key for that user. Inspired by the KeyUpdateNode algorithm, the binary tree structure can be employed to achieve efficient revocation by reducing the workload of the PKG. Concretely, PKG issues the initial private key for a registered user by associating each user to a leaf node randomly selected from a binary tree and generating a group of private keys (associated with the identity of this user) according to the data stored in each node in the path ranging from the root node to the corresponding terminal node. According to the revocation list generated in each time period, the PKG executes the KeyUpdateNode algorithm to output a group of nodes and broadcasts the data stored in this set as the updated key to each user in the system. In this way, only the legitimate (non-revoked) users can generate the short-term private key in current time period by invoking the KeyDer algorithm. When the data generator intends to deliver a message m to the analytical system, the data generator runs Signcrypt algorithm using its short-term private key and delivers the ciphertext to the analytical system. Once receiving the ciphertext from the data generator, the analytical system runs Unsigncrypt algorithm to recover the message m. With this R-IBSC scheme, confidentiality, integrity, authentication, non-repudiation and revocation can be offered simultaneously. As for the secure outsourcing, the main trick behind our construction is to incorporate a key blinding technique and a ciphertext re-randomization technique to outsource the unsigncryption such that the adversary (including the malicious cloud server) cannot learn any information about the encrypted message. Meanwhile, the correctness of the outsourced computation done by the cloud server can be validated. More precisely, the receiver supplies the cloud server with a transformation key which enables the latter to perform the partially unsigncryption. It is remarkable that the transformation key only needs to be uploaded to the cloud once in a time period and unlimited number of cipher texts can be transformed by the cloud server in this time period. During this time period, the receiver can re-randomize the receiving cipher text and forward it to the cloud server, which transforms the cipher text and returns the partially-unsigncrypted result to the receiver. Once obtaining the partial cipher text from the cloud server, the receiver can retrieve the plaintext with the secret retrieving key and validate the correctness of outsourced computation with the random factor used in the ciphertext re-randomization.

V. CONCLUSION

In this paper is to provide the secure communication for big data and cloud computing, then we proposed a novel ID-based signcryption with efficient revocation and unsigncryption outsourcing.

REFERENCES

[1] V. Marx, “Biology: The big challenges of big data”, Nature, vol. 498, pp. 255-260, 2013.
[2] G. King, “Ensuring the data-rich future of the social sciences”, Science, vol. 331, no. 6018, pp. 719-721, 2011.
[3] C. L. Stimmel, “Big Data Analytics Strategies for the Smart Grid”, pp. 1-258, CRC Press, 2015.
[4] D. Quick, K.-K. R. Choo, “Impacts of increasing volume of digital forensic data: A survey and future research challenges”, Digital Investigation, vol. 11, no. 4, pp. 273-294, 2014
[5] D. Quick, K.-K. R. Choo, “Big forensic data reduction: digital forensic images and electronic evidence”, Cluster Computing, vol. 19, no. 2, pp. 723-740, 2016
[6] M. Chen, S. Mao, Yin Zhang, Victor C. M. Leung, “Big Data-Related Technologies, Challenges and Future Prospects”, Springer Briefs in Computer Science, pp. 1-89, Springer, 2014.
[7] M Shargal, D Houseman, “The big picture of your coming smart grid”, Smart Grid News, 2009.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

[8] S. Spiekermann, A. Acquisti, R. Bohme, K.-L. Hui, "The challenges of personal data markets and privacy", Electronic Markets, vol. 25, no. 2, pp. 161-167, 2015
[9] S. Yu, " Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data", IEEE Access, DOI 10.1109/ACCESS.2016.2577036.
[10] J. Baek, Q. Vu, J. Liu, X. Huang, Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid", IEEE Transactions on Cloud Computing, vol. 3, no. 2, pp. 233-244, 2015.
[11]A. Sahai and B. Waters, "Fuzzy identity-based encryption", Advances in Cryptology-EUROCRYPT 2005, Springer, LNCS 3494, pp. 457-473, 2005.
[12] M. Green, S. Hohenberger, B. Waters, "Outsourcing the Decryption of ABE Ciphertexts", 20th USENIX Security Symposium, 2011.
[13] J. Lai, R. H. Deng, C. Guan, J. Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE Transactions on Information Forensics and Security, vol. 8, no. 8), pp. 1343-1354, 2013.
[14] S. Lin, R. Zhang, H. Ma, S. Wang, "Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2119-2130, 2015.
[15] X. Mao, J. Lai, Q. Mei, K. Chen, J. Weng, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption", IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2015.2423669.
[16] H. Ma, R. Zhang, Z. Wan, Y. Lu, S. Lin, Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing, IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2015.2499755.
[17] J. Xu, Q. Wen, W. Li, Z. Jin, Circuit Ciphertext-Policy Attribute-Based `Hybrid Encryption with Verifiable Delegation in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 119-129, 2016.
[18] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology-CRYPTO 2001, LNCS 2139, pp. 213-229, 2001.
[19] A. Boldyreva, V. Goyal, V. Kumar, "Identity-based Encryption with Efficient Revocation", 15th ACM Conference on Computer and Communications Security (CCS 2008), pp. 417-426, 2008.
[20] B. Libert and D. Vergnaud, "Adaptive-ID secure revocable identity-based encryption", in Cryptographers' Track at the RSA Conference 2009 (CTRSA), LNCS. 5473, Springer-Verlag, pp. 1-15, 2009.
[21] J. Chen, H. W. Lim, S. Ling, H. Wang, K. Nguyen, "Revocable Identity-Based Encryption from Lattices", 17th Australasian Conference on Information Security and Privacy (ACISP 2012), Springer, LNCS 7372, pp. 390-403, 2012.
[22] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Advances in Cryptology-CRYPTO 2001, LNCS 2139, pp. 41-62, 2001.
[23] J. H. Seo and K. Emura, "Revocable Identity-Based Encryption Revisited: Security Model and Construction", 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2013), LNCS 7778, pp. 216-234, 2013.
[24] J. H. Seo and K. Emura, "Revocable Identity-Based Cryptosystem Revisited: Security Models and Constructions", IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1193-1205, 2014.
[25] J. H. Seo, K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption", Topics in Cryptology-CT-RSA 2013, Springer-Verlag, LNCS 7779, pp. 343-358, 2013. [35] J. H. Seo, K. Emura, "Revocable hierarchical identity-based encryption, Theoretical Computer Science", vol. 542, no. 3, pp. 44-62, 2014.
[26] J. H. Seo, K. Emura, "Revocable hierarchical identity-based encryption, Theoretical Computer Science", vol. 542, no. 3, pp. 44-62, 2014.
[27] H. Xiong, Z. Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks", IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1442-1455, 2015.
[28] T.-Y. Wu, T.-T. Tsai and Y.-M. Tseng, "A Revocable ID-based Signcryption Scheme", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 240-251, 2012.