Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 689 – 696

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Enhanced Attribute Based Encryption for Cloud Computing.

Saravana Kumar N[a],Rajya Lakshmi G.V[b],Balamurugan B[a,*]

[a]*School of Information Technology and Engineering,VIT University,Vellore 632014,India*
[b]*College of Science and Mathematics,University of Massachusetts,Boston 02125,USA*

Abstract

Cloud computing is emerging paradigm provides various IT related services. The security and privacy are two major factors that inhibits the growth of cloud computing. Security factors are reasons behind lesser number of real times and business related cloud applications compared to consumer related cloud application. Firstly, the pros and cons of different Attribute Based encryption methods are analysed. Secondly, a new encryption method based on Attribute Based Encryption (ABE) using hash functions, digital signature and asymmetric encryptions scheme has been proposed. Our proposed algorithm is simplified yet efficient algorithm that can implemented for cloud critical application.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Cloud computing;security;privacy;Attribute based Encryption

1. Introduction

Cloud computing is a paradigm shift from traditional computing that relies on sharing of computer resources rather than having personal devices[1]. Cloud computing provides flexible and cost effective way to access the data to end users in multiplatform at any time. The sharing of resources includes storage, software and hardware. The cloud offers various services like SaaS, PaaS, IaaS, MaaS, SecaaS[2].The basic concept behind the cloud is Virtualization. The confidentiality, accessibility, security, privacy, performance, integrity are the major issue of cloud .The cloud provides

* Corresponding author. Tel.: +91 9894955250.
E-mail address: balamuruganb@vit.ac.in

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.127

different types of cloud deployment models like Public, private and hybrid, community[1]. Cloud computing is an emerging technology as the number of cloud service providers and the cloud users are increased in recent years. The revenue of cloud service providers had been increased year by year. The revenue of cloud computing in 2009 is about 58 billion US dollars. In 2010, 70 billion US dollars[3] .The revenue increase is about 16-17 compared to last year. The present day cloud application dealt with consumer and small business needs rather than mission critical or large business application. Impact of security breaches for large scale business and mission critical application will be considerably high compared to small scale business. The revenue generated by the cloud computing depends upon the Quality of Service offered by the cloud service provider. The primary attribute of Quality of Service is security and the cloud service provider has to give full assurance of security in terms of confidentiality, accessibility, privacy and integrity. Among the factors privacy is a primary and uncompromisable factor of security[4]. Encryption is the way to secure the data in the untrusted cloud server. Most of Encryption methods currently available had no effect on real time cloud applications. The possibility of their use in critical cloud application is limited. Thus we categorize different encryption algorithms based on their usability and adaptability .using Attribute Based Encryption (ABE). Unlike other encryption methods the ABE dealt with encrypting and decrypting the data based on user attributes. It provides promising and flexible access control by using controlled access structures associated with private key, master key and the cipher text respectively[5].The attribute based encryption is best way to secure when compared to other encryption types like Role based access as it has the capability to restrict access based on roles. As a result it is appropriate only to the small scale applications. The ABE is overhead in terms of data retrieval. Considering the privacy and security factors the limitation are negligible.

1.1. Classification of Attribute Based Encryption

The term encryption refers to converting the original data into human unreadable form (encoding). The conversion of the encoded data into original form is known as decryption. By encrypting the data only the authorized person can decode the original data. Thus data confidentiality is achieved by the encryption. There are many encryption algorithms currently available and has its own advantages. The attribute based encryption is a proven algorithm for cloud computing environment[7].The limitations of some of attribute based encryption method are to be analysed. Attribute based encryption generally involves encrypting the attributes neither encrypting the whole data. Encryption in ABE is easy and secure and inexpensive compared to other encryption discussed. The ABE is secure because the encrypted data contains the attributes rather than the data. In case of any malicious attacks the data never is leaked. The limitation of the attribute based encryption is decryption of data is expensive[7].The attribute based encryption makes the application to be secure .the performance of the ABE is high compared to other encryption methods. Thus attribute based encryption is the solution to all cloud applications in future. The cloud is moved to next generation computing with critical applications and real time applications. The fig 1 represents the classification of different types of ABE.

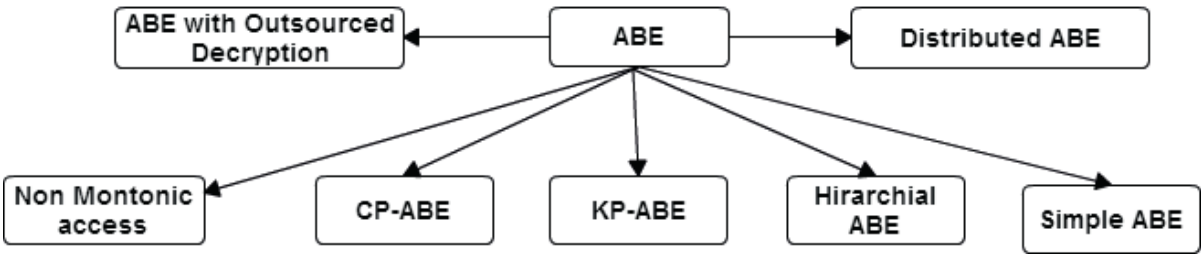

Fig. 1. Classification of Attribute Based Encryption

2. Related Work

In cloud computing the data is stored in an unknown place to the end user. Firstly, data has to be secure in database. Virtualization provides solution to safeguard the data. In order to achieve the security and integrity, the place of data centre is kept secret[6]. The issue is whether to believe in untrusted cloud server. We stated it is untrusted, as it involves many malicious attacks during processing of data. The cipher text attribute based encryption was proposed by Brent waters[8]. The ABE is proposed to solve the complex access control mechanism over encrypted data. Basically , ABE is public key based one to many encryption that decrypt the cipher text only if the private key associated with the user matches with public key and master secret key. The decryption of data takes place directly by the server itself. Thereby performance is increased with effective encryption methodologies. It suffers from serious disadvantage of expensive decryption. The key policy attribute based encryption was proposed by goyal et al [9]. The KP-ABE has three algorithms. The access structure granted full access to the user. This is major limitation of the key policy attribute based encryption. Full access granted to user creates a lot of problem. The KP-ABE fails the distinguish the necessary access control to the users as the access policy embedded in the decryption key. In 2011 green et al proposed the concept of outsourcing the decryption for ABE ie user has to decrypt the data by him[10]. The ABE with outsourced decryption overcomes the limitation of waters and it assures security from malicious attackers. The cipher text is decrypt only with the public key matches with the user private key. The green et al algorithm modifies the water algorithm with transformation key and retrieving key[15]. The original data is compared with partially encrypted data to achieve confidentiality of the data. The limitation includes non-verifiability of data whether the required cipher text is decrypted. It might produce the previous cipher text or any other cipher that associated with particular file or anything. The other disadvantages include the user has additional work to decrypt the data. Probability of attackers to hack the account is very less. In 2013 Junzuo Lai et al proposed the ABE outsourced decryption [7]. This overcomes the limitation of green et al with verifiable outsourcing of data. The proposed algorithm matches the cipher text with the decrypted cipher text. Thus verification of data is the main advantage of this algorithm. The proxy re- encryption is used for decryption of the ciphers. And size of ciphers also very small in size. The performance of the proposed system is relatively high. Thus cloud is ready for mission critical applications with outsourced decryption of data. The limitation this system includes robustness and scalability. Security and performance measured are relatively varied in real time applications as they have high network traffic and complex access structure. When the number of users increases the performance of the system will be decreased.

3. Categorization of Cloud Applications

Various types of cloud applications are already classified into private, public and hybrid based on the cloud deployment models. Based on the risk involved in cloud application we are classifying the cloud broadly into three major categories high- critical, medium –critical and low-critical. All the cloud based applications are critical in nature as it contains the data of the user. In case of the search application, forecasting application or any other application are considered to be critical since it contains the users' details. Thus based on factors such as Timeliness, accuracy, dependability,confidentiality,performance,privacy,security,scalability,roboutness, Integrity etc classified the cloud.

3.1. High Critical Application

The high critical applications are real time systems that need to retrieve the data with cent percent accuracy with in the stipulated time. In case of failure of application result in loss of life and huge amount of money loss. The high critical applications are very less in number. The medical records of the patient, ticket reservation system are examples of high critical cloud applications. Though cloud service provider says that the cloud service is secure. There are many outages in cloud. The largest web service provider Amazon itself experienced the outages in year 2008. And Microsoft azure also had outage of nearly 8 hours recently in the month of august 2014.The reason behind the outages was it is publicly accessible. Less transparent nature of cloud is one of biggest advantage in terms of security. Indeed the end user had to trust their Cloud service provider. This were the various reasons cloud has limited number of critical applications. Even the SLA between the cloud service provider and the user has been failed in case of Microsoft azure. Often cloud is a misunderstood thing. This outage doesn't mean cloud is insecure. There are many advantages and

currently many researches going on cloud security. For cloud critical application all the parameters need to satisfy. The private cloud or community clouds are well suited applications for the high critical applications

Table 1. Classification of cloud based applications.

Attributes	High Critical	Medium-Critical	Low Critical
Timeliness	✓	×	×
Accuracy	✓	✓	×
Dependability	✓	✓	✓
Confidentiality	✓	✓	×
Performance	✓	×	✓
Privacy	✓	×	×
Security	✓	✓	×
Scalability	✓	×	×
Robustness	✓	×	×
Integrity	✓	✓	✓
Reliability	✓	×	×
Accessibility	✓	✓	×

3.2. Medium Critical Application

The medium critical applications have less impact in case of failures. Cloud storage, project management are better examples of this type. Drop box has cloud storage application had been failed many times but it doesn't have much impact. Still billion of people share the data in drop box cloud storage application[11].consider the scenario of the amazon web service outage in 2008 or Drop box outage. Though the outage has happen there is no data loss in the amazon or the drop box as the cloud has backup in multiple datacenters. Thus simple cloud application like storage or business was not affected by the particular outages. The services are continued after a period of time. The revenue of the cloud proved that. Thus applications like simple storage services, software as a service applications come under medium critical applications.

3.3. Low Critical Application

This application doesn't produce any impact in case of failures. Example of cloud application includes zomato, call fire etc. Thus no need of encryption for this kind of application. Though low critical application doesn't have impact. The application needed to be tested in terms of code. The application should not communicate with the other application or get the user data. Map applications, GPS tracking system, Meteorological applications, restaurant search applications are the best Fig.2 represents the classification of cloud applications for the past five years. There are huge numbers of cloud application. The number denotes the percentage of cloud application rather than number of cloud application. The graph clearly explains the percentage of cloud application where mission critical application has very number compared to other two types of the cloud application. The reason is mission critical application should have attributes that is listed. Moreover it should have cent percent security and privacy. In case of medium critical there is negligible level of security as well as privacy. Therefore the cloud has very less number of critical applications. The cloud is secure but it is not cent percent. This is drawback and that is major reason for less number of high critical cloud application.

4. Classification of Attribute Based Encryption with suitable Attribute Types

All cloud application need not to follow the same kind of encryption methods. Based on the risk and cloud deployment models we classify the suitable encryption methods. Taking railway reservation system there will be a maximum server load if it reaches the maximum number of user it fails to work. But cloud application can withstand the server load compared to traditional web servers provided the proper access control and data security. The ABE with fine grained access control algorithm provides solution to the mentioned problem. The scalability will be high in cloud as it handles by the numerous servers. By moving to cloud it provides better service to the user compared to the traditional server. Though currently this application unavailable in cloud it might be implemented in future. It is inexpensive with high performance. The Medium critical applications like storage it is necessary to follow ABE with verifiable outsourced decryption to achieve the confidentiality of the data. By means of outsourcing the decryption the cost is reduced comparatively. The data confidentiality is the advantage of using Attribute based encryption with outsourced decryption. But in case of project management the ABE with direct decryption / fully homomorphic encryption is better suitable. As in case of homomorphic encryption the verification of data is possible. In both methods cost nearly equal. ABE has better performance than homomorphic encryption. Low critical application the attribute based encryption is better suitable. As there is no verification of data. The primary objective is to retrieve the data from the data centre. Therefore to cost effective and increase in the performance it is better to encrypt the data with simple ABE. Fig.2. represents the classification of cloud based application based on the complexity and risk associated with it.

.

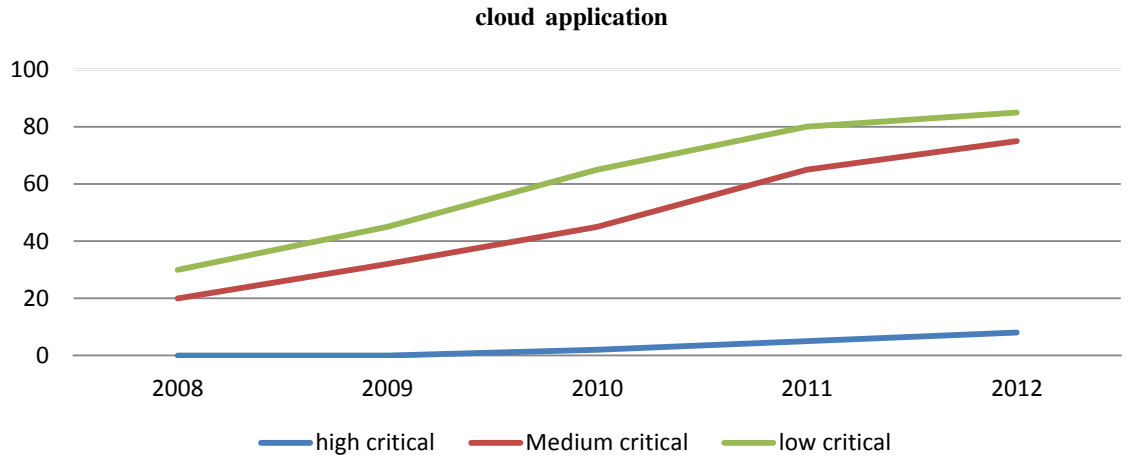

Fig. 2. Classification of Cloud Application Based on Risk.

5. Proposed Work

5.1. Preliminaries

We have proposed the simplified algorithm. To understand the prelims the various concepts like Bi- linearity, Non degeneracy, and computable, Digital signature and hash function needs to be studied. The modification of the ABE algorithm with hash function associated with the asymmetric encryption the algorithm could be applicable for the real time systems.

5.2. Access Structures

The access structure specifies controlled access to the legitimate users. And it specifies the different access structures to the users based on their role and attributes. Let {p1, p2,....pn}be set of parties. Let A 2 power {p1….pn) B and C. Therefore B is a subset of A and C is subset of A therefore C A. And the set A is non empty set. The set in A is called authorized sets otherwise it is unauthorized set. The original message has been partitioned to equal size in order to efficiently encrypt the data.

5.3. Setup (λ, U, S):

The registered user has to set up the algorithm λ –security parameter. U – Universal description. The U= {1,2,….n) The Φ(λ) generates output (p, G, Gt, e) where G and Gt are the cyclic groups of prime order p. ∀ attribute ∃ i in 'U' . ∀ i ∈ U ∃ "sk " ∈ group G . And there is mapping between the elements of group G to produce the Group Gt . ie G*G→ G_t [14]. Thus the master key is generated and it kept secret by itself. The public key (PK) is as follows (p,G,Gt, e ,H) where H is a Hash function.

5.4. Keygen (PK,SK):

Following the setup phase ,key generation phase takes care of assembling the keys needed for the entire operation.The input to the key generation is public key and secret key and the attribute S. consider the hash function H(x). Consider the vectors$\bar{vi}$, v$\vec{j}$,…..v $\vec{n} \in Z_p$. where zp is a cyclic group. The secret key will be generated with the input of the asymmetric key public key.

5.5. Encryption(PK,SK):

It takes the input public key and secret key. The generated Secret key (SK) , H matches with the access tree and encrypt the hash function. That results in Digital signature. The encryption of hash function takes place if and only if it matches with the Access structure (A). Otherwise it returns the ⊥. The encryption method is to find value of H(x). Thus resultant of encryption is H(x).Thus Encryption of data is done using Cloud server.

5.6. Decryption(PK, SK, A, private key):

The input to the decryption is public key, secret key, access structure and private key. The user with the private key. Thus the user can decrypt with digital signature and private key. The private key matches with the secret key and access structure. If private key matches, then it will decrypt the hash function. Else it returns ⊥ to the user. Here the decryption carried out by server directly. And the decrypted hash function H(y) = H(x) data is verified. Here decryption is done directly by the server. Though the outsourced decryption is cost effective in nature compared to the proposed algorithm it doesn't suites the real time systems as it has overheads in terms of time. The overall architecture describes the step by step process. Firstly the user is authenticated with the public key associated with the access structures. If the user is authenticated moved to step 2, where the secret key is being generated. The input will be the private key of the user with the digital signature of the user which is the private key. The user has to private key with the generated secret key has to be matched. That is not equal. Once the secret key is generated by the cloud service provided. The access id will be generated. The id associated with the user private key and the generated secret key need to be matched. The hashing function is being used here for mapping the two sets. Thus the user is being authenticated more than once. The encryption algorithm is hard to decrypt (already proved by the existing ABE). Thus we have provided the simplified ABE structures with hashing and digital signature. The access limits are based on user attributes of the user hierarchy. The user hierarchy reflects the overall organisational structure and it depends upon the power hierarchy .The main aspect of attribute based encryption is giving a fine grained and individual access to each and every individual of the access structure. The possibility of changing the access structure based on the requirement of organisation is made possible in the decryption phase. Fig.3 explains about the overall architecture of our proposed

system. Finally as a result of the decryption the plain text will be given to the users based upon the access privileges and access limits

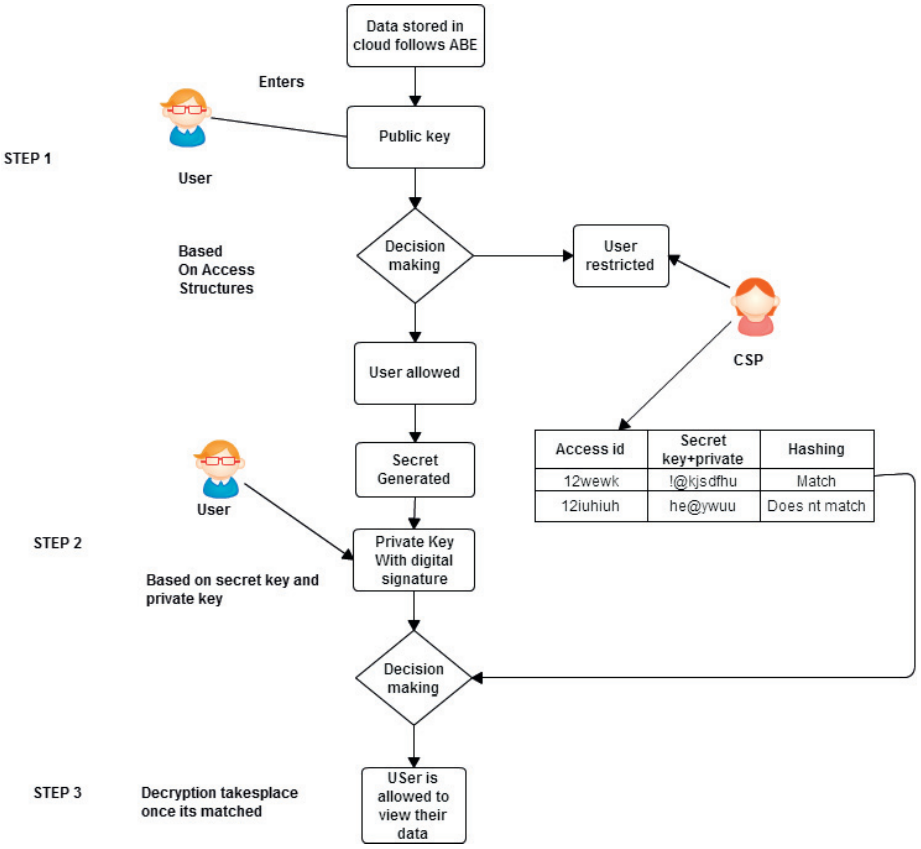

Fig. 3. Overall Architecture of the proposed Algorithm

6. Discussion and Future Work

The algorithm is proposed using the digital signature, hash function. And it follows the asymmetric encryption. The algorithm is very difficult for the hackers as it involves multiple steps. All the steps are instance per call server. Once the authentication fails it doesn't move to next step. Moreover the dual authentication scheme with the help of the digital signature and with the public key. The secret key will be generated. Thus it is hard to decrypt the data. Since it involves multiple steps in encryption and decryption there will be little bit overhead in time. But considering the security as the factor it is negligible. The adversary submits the two message M0 and M1 and access structure A and restriction follows that S where D is empty set. And A cannot be satisfied with S. Then the adversary challenges with trial and error by selecting the $\beta(0,1)$ and try to decrypt the message . Since CP-ABE is secure our proposed method need to be cent per cent secure. Thus the proposed algorithm using ABE is a framework for real time systems. The proposed algorithm has to verify and validate using simulator. The proposed algorithm is provides security from

the malicious insiders and threats during processing of the data. Thus it can be used for cloud application. The performance of the algorithm is to be measured in future. The algorithm has been proved mathematically. It needs to be implemented for the cloud applications.

7. Conclusion

The current status Attribute Based Encryption for cloud computing has been discussed with its advantages and limitations. And we have classified the cloud application based on the risk involved in the application by considering certain parameters. In depth analysis of attribute based encryption is done. And we categories the cloud application based on risk involved and classified the application with suitable encryption methods. And finally we have proposed the new ABE based encryption algorithm with hash functions, digital signature and asymmetric encryption method[13].The proposed algorithm is simplified ABE and it will be suitable for the application that needs high level security and accessed time is being reduced which indeed cost is reduced comparatively. Certain outages doesn't really mean cloud is insecure. The cloud is actually misunderstood thing by others. Microsoft azure is being shifted fully to the cloud nowadays. Cloud computing has lot of advantages. Thus the cloud shouldn't lose its scope in future. Thus cloud has to shift to the next level by moving it to application like healthcare.

References

1. Qiang Duan, Yuhong Yan, Vasilakos,AV.A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing *Network and Service Management, IEEE Transactions on*, vol.9, no.4, pp.373,392.
2. Computing by Mohit Marwaha1, Rajeev Bedi. Applying Encryption Algorithm for Data Security and Privacy in Cloud in *International Journal of Computer Science* Issues, Vol. 10, Issue 1, No 1, January 2013.
3. Gartner worldwide total public cloud Market. http://www.gartner.com/newsroom/id/2352816 .
4. Arshad, J, Townend, P, Jie Xu.Quantification of Security for Compute Intensive Workloads in Clouds *Parallel and Distributed Systems (ICPADS), 2009 15th International Conference on* , vol., no., pp.479,486, 8-11 Dec. 2009.
5. A. Sahai and B. Waters.Fuzzy identity-based encryption,‖ in Proc.EUROCRYPT, 2005, pp. 457–473.
6. Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, and Diego Zamboni. 2009. Cloud security is not (just) virtualization security: a short paper. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (CCSW '09). ACM, New York, NY, USA, 97-102.
7. Junzuo Lai,Deng, R.H, Chaowen Guan, Jian Weng,.Attribute-Based Encryption With Verifiable Outsourced Decryption *Information Forensics and Security, IEEE Transactions on* , vol.8, no.8, pp.1343,1354, Aug. 2013.
8. B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization in Proc. Public Key Cryptography, 2011, pp. 53–70.
9. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (CCS '06). ACM, New York, NY, USA, 89-98.
10. Matthew Green, Susan Hohenberger, and Brent Waters. 2011. Outsourcing the decryption of ABE ciphertexts. In *Proceedings of the 20th USENIX conference on Security* (SEC'11). USENIX Association, Berkeley, CA, USA, 34-34.
11. Dropbox news.https:// www.dropbox.com/news.
12. Rafail Ostrovsky, Amit Sahai, and Brent Waters. 2007. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM conference on Computer and communications security* (CCS '07). ACM, New York, NY, USA, 195-203.
13. S. Chatterjee and A.Menezes. On cryptographic protocols employing asymmetric pairings—The role of revisited,‖Discrete Appl.Math., vol. 159, no. 13, pp. 1311–1322, 2011.
14. Patrick P. Tsang, Sherman S. M. Chow, and Sean W. Smith. 2007. Batch pairing delegation. In*Proceedings of the Security 2nd international conference on Advances in information and computer security* (IWSEC'07), Atsuko Miyaji, Hiroaki Kikuchi, and Kai Rannenberg (Eds.). Springer-Verlag, Berlin, Heidelberg, 74-90.
15. Rosario Gennaro, Craig Gentry, and Bryan Parno. 2010. Non-interactive verifiable computing: outsourcing computation to untrusted workers. In *Proceedings of the 30th annual conference on Advances in cryptology* (CRYPTO'10), Tal Rabin (Ed.). Springer-Verlag, Berlin, Heidelberg, 465-482