Attribute-Based Encryption with Constant-Size Cipher-Text Policy

K. Shobana
P.G Student: Department of CSE
Arasu Engineering College
Kumbakonam, India

M. Anandakumar
Assistant Professor: Department of CSE
Arasu Engineering College
Kumbakonam, India

***Abstract*—With the popularity of outsourced data storage, there have been increasing concerns about its security and privacy. Since the outsourced data storage environment is distributed and untrusted, data owners have to encrypt outsourced data to enforce confidentiality. Therefore, how to achieve practicable access control of encrypted data in an untrusted environment is an urgent issue that needs to be solved.Attribute-Based Encryption (ABE) is a promising scheme suitable for access control in storage systems. We proposes a hierarchical attribute-based access control scheme with constant-size ciphertext. The scheme is efficient because the length of ciphertext and the number of bilinear pairing evaluations to a constant are fixed. Its computation cost in encryption and decryption algorithms is low. Moreover, the hierarchical authorization structure of our scheme reduces the burden and risk of a single authority scenario. We prove the scheme is of CCA2 security under the decisional q-Bilinear Diffie-Hellman Exponent assumption. In addition, we implement our scheme and analyze its performance. The analysis results show the proposed scheme is efficient, scalable, and fine-grained in dealing with access control for outsourced data.**

Keywords: Cloud Data, Dataowuners, Attribute Based Encryption

I. INTRODUCTION

Outsourced data storage computing

Outsourced data storage is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services),which can be rapidly provisioned and released with minimal management effort. Outsourced data storage computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party datacenter that may be located far from the user ranging in distance from across a city to across the world. computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Outsourced data storage Computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unprecedented advantages: on-demand selfservice, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, and usagebased pricing. In particular, the ever cheaper and more powerful processors, together with the “software as a service” (SaaS) computing architecture, are transforming datacenter into pools of computing service on a huge scale.

outsourced data storage Architecture

Basis information about the architecture is provided in this chapter, together with the explanations of relevant terms such as virtualization, Frond/Back end or Middleware.

- Virtualization is best described as essentially designating one computer to do the job of multiple computers by sharing the resources of that single computer across multiple environments. Virtual servers and virtual desktops allow you to host multiple operating systems and multiple applications locally and in remote locations, freeing your business from physical and geographical limitations.

The Outsourced data storage Computing architecture can be divided into two sections, the front end and the back end, connected together through a network, usually Internet. The Front End includes the client's computer and the application required to access the Outsourced data storage computing system. Not all Outsourced data storage computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients.

The Back End of the system is represented by various computers, servers and data storage systems that create the "Outsourced data storage” of computing services. Practically, Outsourced data storage computing system could include any program, from data processing to video games and each application will have its own server. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called Middleware. Middleware allows networked computers to communicate with each other.

Public Outsourced data storage

Public Outsourced data storage (external Outsourced data storage) is a model where services are available from a provider over the Internet, such as applications and storage. There are free Public Outsourced data storage Services available, as well as pay-per-usage or other monetized models.

Private Outsourced data storage

Private Outsourced data storage (Internal Outsourced data storage /Corporate Outsourced data storage) is computing architecture providing hosted services to a limited number of people behind a company's protective firewall and it sometimes attracts criticism as firms still have to buy, build, and manage some resources and thus do not benefit from lower up-front capital costs and less hands-on management, the core concept of Outsourced data storage Computing.

Attribute based Encryption

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). The key issue is that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.

Cipher text-Policy ABE

In cipher text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher text specifies an access policy over a defined universe of attributes within the system. A user will be ale to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text. Policies may be defined over attributes using conjunctions, disjunctions and (k,n)-threshold gates, i.e., k out of n attributes have to be present (there may also be non-monotone access policies with additional negations and meanwhile there are also constructions for policies defined as arbitrary circuits). For instance, let us assume that the universe of attributes is defined to be{A,B,C,D}and user 1 receives a key to attributes{A,B}and user 2 to attribute{D}. If a ciphertext is encrypted with respect to the policy(A∧C)∨D, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice feature is that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows decrypting.

II. LITERATURE CHRONICLE

1. *A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext*

Attribute-based encryption (ABE) is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. Key-policy attribute-based encryption (KP-ABE) is an important class of ABE, where cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. KP-ABE has important applications in data sharing on untrusted Outsourced data storage. However, the cipher text size grows linearly with the number of attributes embedded in cipher text in most existing KP-ABE schemes.

2. *New constructions of hierarchical identity-based encryption in the standard model*

A new hierarchical identity-based encryption scheme (HIBE) is proposed at first. The proposed scheme is constructed in the generalized selective-ID model without using the random oracles. Under the decision bilinear Diffie-Hellman inversion (decision BDHI) assumption, the scheme is provably secure against chosen plaintext attacks(CPA). Furthermore, we convert it to a constant size cipher text scheme and reduce its security to the l-DBDHI problem.

3. *Outsourcing Decryption of Attribute Based Encryption with Energy Efficiency*

In this paper, we propose a new efficient scheme to outsource the decryption of attribute based encryption with energy efficiency. We observe all the previous work on out-sourcing the decryption of ABE cares little about the ciphertext length.

4. *An Identity Preserving Access Control Scheme with Flexible System Privilege Revocation in Outsourced data storage Computing*

The advent of Outsourced data storage computing motivates business organizations to migrate their complex data management systems from local servers to Outsourced data storage servers for scalable and durable resources on pay per use basis. Considering enormous users and large amount of documents at Outsourced data storage servers, there is a requirement of an access control scheme, which supports fine-grained cum flexible access control along with "Query-Response" mechanism to enable users to efficiently retrieve desired data from Outsourced data storage servers.

5. *Achieving Secure, Scalable, and Fine-grained Data Access Control in Outsourced data storage Computing*

Outsourced data storage computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on Outsourced data storage servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving finegrainedness, scalability, and data confidentiality of access control actually still remains unresolved.

6. *Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments*

Node attributes such as MAC and IP addresses, and even GPS position, can be considered as exclusive identity in the distributed networks such as Outsourced data storage computing platform, wireless body area networks, and Internet of Things. Nodes can exchange or transmit some important information in the networks. However, with the openness and exposure of node in the networks, the communications between the nodes are facing a lot of security issues. In particular, sensitive information may be leaked to the attackers in the presence of side-channel attacks, memory leakages, and time attacks.

7. A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram

Ciphertext-policy attribute-based encryption (CP-ABE) is widely used in many cyber physical systems and the Internet of things for guaranteeing information security. In order to improve the performance and efficiency of CP-ABE, this paper makes a change to the access structure of describing access polices in CP-ABE, and presents a new CP-ABE system based on the ordered binary decision diagram (OBDD). The new system makes full use of both the powerful description ability and the high calculating efficiency of OBDD -plaintext attack under the decisional bilinear Diffie-Hellman assumption.

8. An Efficient Fuzzy Identity-Based Signature Scheme without Bilinear Pairings

Biometric-based signature is an emerging cryptographic primitive that allows a user with a biometric identity to produce a signature that can be verified successfully using another biometric identity if both biometric identities are within a predefined distance metric. Fuzzy identity-based signature is of particular value for biometric authentication, where biometric identifiers such as fingerprints, iris and voice are used in human identification. Unfortunately, constructions of fuzzy identity-based signature scheme so far are based on bilinear pairings that need costly operations. In this paper, we propose a new fuzzy identity-based signature scheme that does not depend on bilinear pairings. With both the running time and the size of the signature being saved greatly, our scheme is more practical than the previous related schemes for practical application. The proposed fuzzy identity-based signature scheme is proved to be existential unforgeability against adaptively chosen message attack under the standard discrete logarithm assumption in the selective-set model.

9. Toward hierarchical identity-based cryptography for tactical networks

The nature of the tactical network environment requires using secure, reliable, highly efficient, low delay communication protocols. This is particularly true of cryptographic key management protocols that must be successfully completed prior to the start of sensor and C4ISR communications. One class of cryptographic techniques, noninteractive (i.e., identity-based) cryptosystems, is particularly attractive in this environment since these systems can share a key between tactical network nodes who know the identity of their peer and without exchanging cryptographic information.

10. Identity-Based Encryption with Outsourced data storage Revocation Authority and Its Applications

Identity-based encryption (IBE) is a public key cryptosystem and eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li et al. proposed a revocable IBE scheme with a key-update Outsourced data storage service provider (KU-CSP). However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user. In the article, we propose a new revocable IBE scheme with a Outsourced data storage revocation authority (CRA) to solve the two shortcomings, namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Finally, we extend the proposed revocable IBE scheme to present a CRA-aided authentication scheme with period-limited privileges for managing a large number of various Outsourced data storage services.

III. SYSTEM ANALYSIS

A. PROBLEM STATEMENT

In Outsourced data storage computing, users store their data files in Outsourced data storage servers. Thus, it is crucial to prevent unauthorized access to these resources and realize secure resource sharing. In traditional access control methods, we generally assume data owners and the storage server are in the same secure domain and the server is fully trusted. However, in the Outsourced data storage computing environment, Outsourced data storage service providers may be attacked by malicious attackers. These attacks may leak the private information of users for commercial interests as the data owners commonly store decrypted data in Outsourced data storage servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in an untrusted environment are problems that must be solved by Outsourced data storage computing technologies and applications. Moreover, since the number of users is large in a Outsourced data storage computing environment, how to realize scalable, flexible and fine-grained access control is strongly desired in the service-oriented Outsourced data storage computing model. This proposes a hierarchical cipher text-policy attribute-based encryption (CP-ABE) access control scheme with constant-size ciphertext that can realize scalable, flexible, and fine-grained access control of outsourced data in Outsourced data storage computing.

Our contributions are: the proposed scheme adopts CP-ABE with constant cipher text size and maintains the size of cipher text and the computation of bilinear pairing at a constant value, which improves the efficiency of the system and reduces the extra overhead of space storage,data transmission and computation. Second, we design a hierarchical access control system. This system supports inheritance of authorization that reduces the burden and risk in the case of single authority. Finally, we prove our scheme has indistinguishable security under an adaptive chosen cipher text attack and we analyze the performance of our scheme. We present a simulation model to apply our scheme in a Outsourced data storage environment.

Outsourced data storage services have become increasingly popular in Outsourced data storage computing environment. Because of the importance of privacy on data which are handled by the Outsourced data storage data owners, consider a many Outsourced data storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that Outsourced data storage storage providers are safe and cannot be hacked; however, in practice, some authorities may force Outsourced data storage providers to reveal user secrets or confidential data on the Outsourced data storage , thus altogether circumventing storage encryption schemes. According to the Outsourced data storage data privacy our proposed system to implement the new Outsourced data storage encryption scheme that enables Outsourced data storage providers to create convincing fake user secrets to protect user privacy using deniable Cipher text Policy Attribute Based Encryption. Since coercers cannot tell if obtained secrets are true or not, the Outsourced data storage providers ensure that user privacy is still securely protected from third party access.

Outsourced data storage users are impractical for data owners to encrypt their data by pair wise keys. Moreover, it is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satisfy the conditions are able to decrypt the encrypted data.

B. EXISTING SYSTEM

Though there exist ABE schemes with constant cipher text size and/or constant number of pairing operations in decryption, their access structures are restricted to AND gates or threshold gates which severely limit their practical applications. To overcome this problem, suggested outsourcing decryption in attribute-based encryption. Their verification model suffers from the attack as existed in security model.

In traditional access control methods, we generally assume data owners and the storage server are in the same secure domain and the server is fully trusted. However, in the Outsourced data storage computing environment, Outsourced data storage service providers may be attacked by malicious attackers. These attacks may leak the private information of users for commercial interests as the data owners commonly store decrypted data in Outsourced data storage servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in an untrusted environment are problems that must be solved by Outsourced data storage computing technologies and applications. Moreover, since the number of users is large in a Outsourced data storage computing environment, how to realize scalable, flexible and fine-grained access control is strongly desired in the service-oriented Outsourced data storage computing model.

Disadvantages

- No Access control hierarchy.
- Risk of both online and offline attacks
- Time delay for searching the route between the locations.
- It's hard to communicate between user and the admin.

C. Proposed System

A promising approach to address this issue is attribute-based encryption (ABE), first proposed by Sahib and Waters. ABE schemes can be divided into two categories: Cipher text-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE), depending on the access policy is embedded into the cipher text or the user's private key. Proposed a simple method to adapt their RCCA (repayable chosen-cipher text attack) systems to such a setting formalized a security model for capturing the modification in an outsourced ABE system and proposed a concrete construction with verifiable outsourced decryption. We provide formal proofs of the (selective) chosen-plaintext security and the verifiability in the standard model, which is a slight modification of the security model first proposed in for verifiable outsourced ABE. We present an instantiation of our generic construction based on the outsourced ABE system proposed in which is in turn based on Waters CP-ABE scheme. We begin by introducing some basic notations used in the instantiation.

ADVANTAGE

- Stronger authentication
- The addition of the annotation is simple but purposeful
- Increase resistance to both online and offline attacks
- Reduce time for searching the route between the locations.
- Gives accurate details about the current location.
- User friendly, Reduces paper works.
- Easy communication between user and the admin.

IV. METHODOLOGY

In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the stor- age server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data deter- mines a policy for who can decrypt. Thus, our meth- ods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

FILE UPLOAD

User Logs into his Account for further accessing.File upload is the primary Work of data owner. Here data owner has to upload his file. Uploaded file will be encrypted and stored. Before storing it in database Audit Admin will verify it. He only approves whether the file has to be stored or not. Audit Admin will verify the user and give access of storage to data owner for retrievability .

ATTRIBUTE SELECTION

Here User has to select his attribute by which he want to encrypt his file.In computing, an attribute is a specification that defines a property of an object, element, or file. It may also refer to or set the specific value for a given instance of such. For clarity, attributes should more correctly be considered metadata. An attribute is frequently and generally a property of a property. However, in actual usage, the term attribute can and is often treated as equivalent to a property depending on the technology being discussed. An attribute of an object usually consists of a name and a value; of an element, a type or class name; of a file, a name and extension.

- Each named attribute has an associated set of rules called operations: one doesn't sum characters or manipulate and process an integerarray as an image object—one doesn't process text as type floating point (decimal numbers).

- It follows that an object definition can be extended by imposing data typing: a representation format, a default value, and legal operations (rules) and restrictions ("Division by zero is not to be tolerated!") are all potentially involved in defining an attribute, or conversely, may be spoken of as attributes of that object's type. A JPEG file is not decoded by the same operations (however similar they may be these are all graphics data formats) as a PNG or BMP file, nor is a floating point typed number operated upon by the rules applied to typed long integers.

For example, in computer graphics, line objects can have attributes such as thickness (with real values), color (with descriptive values such as brown or green or values defined in a certain color model, such as RGB), dashing attributes, etc. A circle object can be defined in similar attributes plus an origin and radius.

ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver’s public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice features is, that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows to decrypt. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

KEY GENERATION

Nowadays usage of cloud computing is increasing in popularity and this raises new data protection challenges. In such distributed systems it is unrealistic to assume that the servers are fully trusted in enforcing the access policies. Attribute Based Encryption (ABE) is one of the solutions proposed to tackle these trust problems. In ABE the data is encrypted using the access policy and authorized users can decrypt the data only using a secret key that is associated with their attributes. The secret key is generated by a Key Generation Authority (KGA), which in small systems can be constantly audited, therefore fully trusted. In contrast, in large and distrusted systems, trusting the KGAs is questionable. This paper presents a solution which increases the trust in ABE KGAs. The solution uses several KGAs which issue secret keys only for a limited number of users. One KGA issues a secret key associated with user's attributes and the other authorities issue independently secret keys associated with generalized values of user's attributes. Decryption is possible only if the secret keys associated with the non-generalized and generalized attributes are consistent. This mitigates the risk of unauthorized data disclosure when a couple of authorities are compromised.

FILE SHARING

File sharing is the public or private sharing of computer data or space in a network with various levels of access privilege. While files can easily be shared outside a network (for example, simply by handing or mailing someone your file on a diskette), the term file sharing almost always means sharing files in a network, even if in a small local area network. File sharing allows a number of people to use the same file or file by some combination of being able to read or view it, write to or modify it, copy it, or print it. Typically, a file sharing system has one or more administrators. Users may all have the same or may have different levels of access privilege. File sharing can also mean having an allocated samount of personal file storage in a common file system. More usually, however, file sharing implies a system in which users write to as well as read files or in which users are allotted some amount of space for personal files on a common server, giving access to other users as they see fit. The latter kind of file sharing is common in schools and universities. File sharing can be viewed as part of file systems and their management.

EXPERIMENTATION & RESULT SAMPLING

By carry the experimentation for the particular project development has been done on different input parameters in order to ensure the performance of the outcome results with several domains and environments.

CONCLUSION

Secure sharing of data plays an important role in Outsourced Storage. Attribute-based Encryption can realize data confidentiality in the untrusted environment of server-end, fine-grained access control and large-scale dynamic authorization which are the difficult problems to solve the traditional access control. The proposed scheme adopts CP-ABE with constant-size cipher text that solves the problem of the cipher text size depending linearly on the number of attributes. Our scheme can maintain the size of cipher text and the computation of encryption and decryption at a constant value. Therefore, the scheme can improve the efficiency of the system. Finally, we also demonstrate an application model in a Hadoop distributed cloud environment. This shows our scheme has good adaptability and scalability in Outsourced data storage technique.

REFERENCES

[1] Chang-Ji Wang,Jian-Fa Luo" A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext" 8th International Conference on Computational Intelligence and Security, 2012

[2] Qing Wu, Wenqing Wang "New constructions of hierarchical identity-based encryption in the standard model" 978-1-4244-6837-9/10, 2010 IEEE.

[3] Xu An Wang, Jianfeng Ma, Fatos hafa "Outsourcing Decryption of Attribute Based Encryption with Energy Efficiency" 10th International Conference on P2P, Parallel,Grid,CloudandInternet Computing 2015 978-1-4673-9473-4 /15, 2015 IEEE

[4] Rohit Ahuja,Sraban Kumar Mohanty, Kouichi Sakurai"An Identity Preserving Access Control Scheme with Flexible System Privilege Revocation in Outsourced data storage Computing" 11th Asia Joint Conference on Information Security, 978-1-5090-2285-4/16, 2016 IEEE.

[5] Shucheng Yu, Cong Wang,,KuiRen, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Outsourced data storage Computing" 978-1-4244-5837-0/10,2010 IEEE.

[6] Mingwu Zhang, Yudi Zhang, Yixin Su, Qiong Huang, Yi Mu Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments 1932-8184, 2015 IEEE.

[7] Long Li,Tianlong Gu,Liang Chang,"A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary" pp 1137 – 1145,vol 5, 2169-3536 ,11 January 2017,IEEE.

[8] ChangjiWang,"A Efficient Fuzzy Identity- ased Signature Scheme without Bilinear Pairings", Tenth International Conference on Computational Intelligence and Security,978-1-4799-7434,14-2014 IEEE.

[9] Brian J.Matt, "Toward hierarchical identity-based cryptography for tactical networks", Military CommunicationsConference,0-7803-8847-04,2004,lEEE.

[10] Yuh-MinTseng,Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang" Identity-Based Encryption with Outsourced data storage Revocation Authority and Its Applications"on Cloud Computing,pp1-1,vol-99,10 March 2016, 2168-7161, IEEE