IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SYSTEMATIC ATTRIBUTE-BASED ENCRYPTION SCHEME IN CLOUD COMPUTING

[1]E.Sunil, [2]Sk Mahaboob Basha,[3]T R Mani Chigurupati

[1, 2, 3] Assistant Professor

[1, 2, 3] Computer Science and Engineering

[1, 2, 3] Holy Mary Institute of Technology & Science,Hyderabad,India.

Abstract :-Cipher text-policy attribute-based encryption (CP-ABE) has been a favored encryption innovation to take care of the difficult issue of secure information partaking in distributed computing. The mutual information documents for the most part have the trait of staggered progressive system, especially in the zone of social insurance and the military. Be that as it may, the chain of importance structure of shared records has not been investigated in this paper, a productive record progressive system property based encryption plot is proposed in distributed computing. The layered access structures are incorporated into a solitary access structure, and afterward, the progressive records are encoded with the coordinated access structure. The cipher text parts identified with qualities could be shared by the documents. Along these lines, both cipher text stockpiling and time cost of encryption is spared. Besides, the proposed plot is end up being secure under the standard presumption. Test reproduction shows that the proposed conspire are profoundly effective regarding encryption and decoding. With the quantity of the records expanding, the benefits of our plan become increasingly prominent.

Index Terms: Cipher text-policy attribute-based encryption (CP-ABE)

Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Fig.1 Structure of cloud computing

Cloud computing working process

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

1.2 Existing System

a) Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang *et al.* proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE.
b) Wan *et al.* proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A cipher text policy hierarchical ABE scheme with short cipher text is also studied.
c) In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.

1.3 Disadvantages of Existing System

1. In Existing System time and cost for encryption is high.
2. No any exceptional different various leveled records are utilized.
3. Decryption framework time and calculation cost are high.

1.4 Proposed System

a) In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.
b) The contributions of our scheme are three aspects.
c) Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure.
d) Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.
e) Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption.

1.5 Advantages of Proposed System

a) CP-ABE feasible schemes which has much more flexibility and is more suitable for general applications
b) Multiple hierarchical files sharing are resolved using layered model of access structure.
c) In proposed system both cipher text storage and time cost of encryption are saved.
d) The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files.
e) The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.

1.6 Benefits of cloud computing:

a) Achieve economies of scale – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
b) Reduce spending on technology infrastructure. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
c) Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection.
d) Streamline processes. Get more work done in less time with less people.
e) Reduce capital costs. There's no need to spend big money on hardware, software or licensing fees.
f) Improve accessibility. You have access anytime, anywhere, making your life so much easier!
g) Monitor projects more effectively. Stay within budget and ahead of completion cycle times.
h) Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
i) Minimize licensing new software. Stretch and grow without the need to buy expensive software licenses or programs.
j) Improve flexibility. You can change direction without serious "people" or "financial" issues at stake.

2. Literature Survey

1) A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing

In this paper, just because, we characterize a general idea for proxy re-encryption (PRE), which we call deterministic limited automata-based useful PRE (DFA-based FPRE). In the interim, we propose the first and cement DFA-based FPRE framework, which adjusts to our new thought. In our plan, a message is scrambled in a figure text related with a discretionary length list string, and unscramble or is genuine if and just if a DFA related with his/her mystery key acknowledges the string. Moreover, the above encryption is permitted to be changed to another figure text related with another string by a semi confided in intermediary to whom a re-encryption key is given. In any case, the intermediary can't access the hidden plaintext. This new crude can expand the adaptability of clients to appoint their unscrambling rights to other people. We additionally demonstrate it as completely picked figure text secure in the standard model.

2) Fine-grained two factor access control for Web-based cloud computing services

In this paper, we present another fine-grained two-factor confirmation (2FA) get to control framework for online distributed computing administrations. In particular, in our proposed 2FA access control framework, a trait based access control system is actualized with the need of both a client mystery key and a lightweight security gadget. As a client can't get to the framework in the event that they don't hold both, the instrument can improve the security of the framework, particularly in those situations where numerous clients share a similar PC for electronic cloud administrations. Moreover, quality based control in the framework additionally empowers the cloud server to limit the entrance to those clients with a similar arrangement of traits while protecting client security, i.e., the cloud server just realizes that the client satisfies the necessary predicate, however has no clue on the specific character of the client. At long last, we likewise do a reproduction to exhibit the practicability of our proposed 2FA framework.

3) Cipher text-policy attribute based encryption

In a few appropriated frameworks a client should possibly have the option to get to information if a client forces a specific arrangement of accreditations or properties. At present, the main technique for upholding such strategies is to utilize a believed server to store the information and intervener gets to control. In any case, on the off chance that any server putting away the information is undermined, at that point the secrecy of the information will be undermined. In this paper we present a framework for acknowledging complex access control on scrambled information that we call Cipher text-Policy Attribute-Based Encryption. By utilizing our strategies scrambled information can be kept private regardless of whether the capacity server is depended; additionally, our techniques are secure against agreement assaults. Past Attribute Based Encryption frameworks utilized credits to depict the scrambled information and incorporated approaches with client's keys; while in our framework ascribes are utilized to portray auser's accreditations, and a gathering encoding information decides strategy for who can unscramble. In this way, our techniques are thoughtfully nearer to customary access control strategies, for example, Role-Based Access Control (RBAC). Likewise, we give an execution of our framework and give execution estimations.

3 System Analyses

3.1Modules Description:

Data Owner Module: In the principal module, we build up the Data Owner Module. Proprietor Will Sign up and Wait for the endorsement Key of administrator. Subsequent to Getting key Owner can login utilizing the key, and transfer any records identified with clients clinical Information on the cloud. In this module, information proprietor will check the advancement status of the record transfer by him/her. It has enormous information should have been put away and partaken in cloud framework. In our plan, the element is responsible for characterizing access structure and executing Encrypt activity. Also, it transfers figure text to CSP. After the finishing, proprietor logout the meeting

User and Physician Module: In the principal module, we build up the Data Owner Module. Proprietor Will Sign up and Wait for the endorsement Key of administrator. Subsequent to Getting key Owner can login utilizing the key, and transfer any records identified with clients clinical Information on the cloud. In this module, information proprietor will check the advancement status of the record transfer by him/her. It has enormous information should have been put away and partaken in cloud framework. In our plan, the element is responsible for characterizing access structure and executing Encrypt activity. Also, it transfers figure text to CSP. After the finishing, proprietor logout the meeting

Cloud Service Provider: It is a semi-confided in substance in cloud framework. It can sincerely play out the doled out errands and return right outcomes. Be that as it may, it might want to discover however much touchy substance as could be expected. In the proposed framework, it gives figure text stockpiling and transmission administrations. In this module, we additionally create administrator module process. Administrator Will Login on the adman's page. He/she will check the pending solicitations of any of the above individual. In the wake of tolerating the solicitation from the above individual, he/she will create ace key for encode and Secret key for decode.

3.2 System Study

Feasibility Study: The practicality of the undertaking is broke down in this stage and strategic agreement is advanced with a general arrangement for the venture and some quotes. During framework examination the attainability investigation of the proposed framework is to be done. This is to guarantee that the proposed framework isn't a weight to the organization. For possibility investigation, some comprehension of the significant necessities for the framework is basic.

Three key considerations involved in the feasibility analysis are

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

4 System Design

A system architecture diagram would be used to show the relationship between different components. Usually they are created for systems which include hardware and software and these are represented in the diagram to show the interaction between them. However, it can also be created for web applications.

System architects are responsible for designing and implementing short and long-term strategic goals for managing and maintaining systems and software. They provide their expertise and architectural assistance to other IT personnel including software teams, System Analysts and Engineers

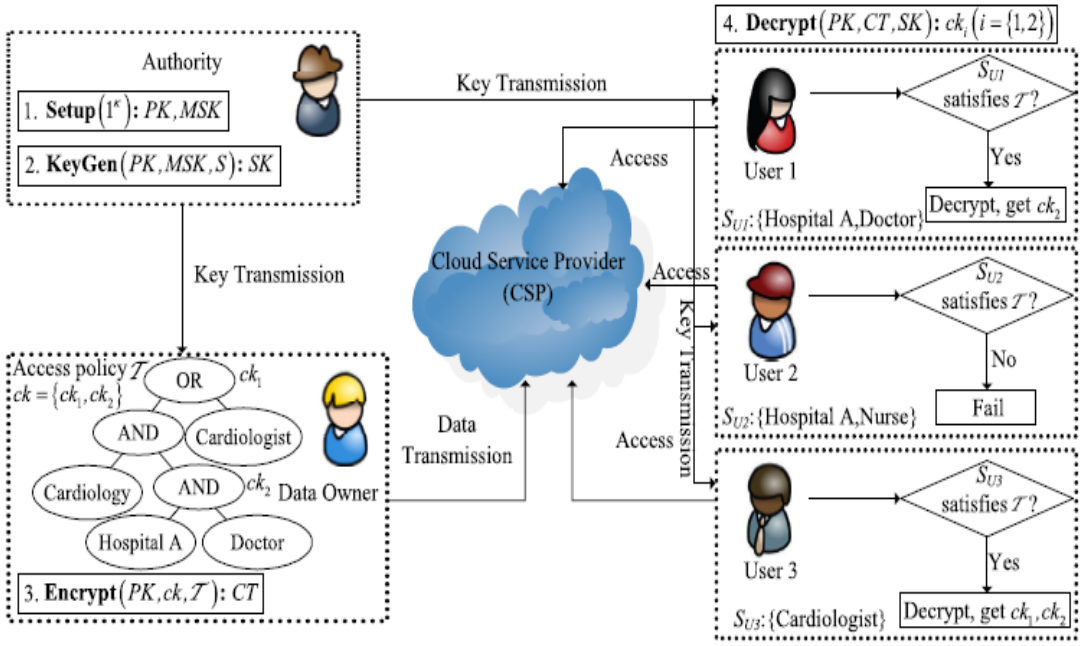

Fig.2 System Architecture

4.3. UML Diagrams:

1. UML represents Unified Modeling Language. UML is a normalized universally useful demonstrating language in the field of item arranged programming building. The standard is overseen, and was made by, the Object Management Group.
2. The objective is for UML to turn into a typical language for making models of article arranged PC programming. In its present structure UML is involved two significant segments: a Meta-model and documentation. Later on, some type of technique or procedure may likewise be added to; or related with, UML.
3. The Unified Modeling Language is a standard language for indicating, Visualization, Constructing and archiving the antiquities of programming framework, just as for business displaying and other non-programming frameworks.
4. The UML speaks to an assortment of best designing practices that have demonstrated fruitful in the displaying of enormous and complex frameworks.

Data Flow Diagram:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

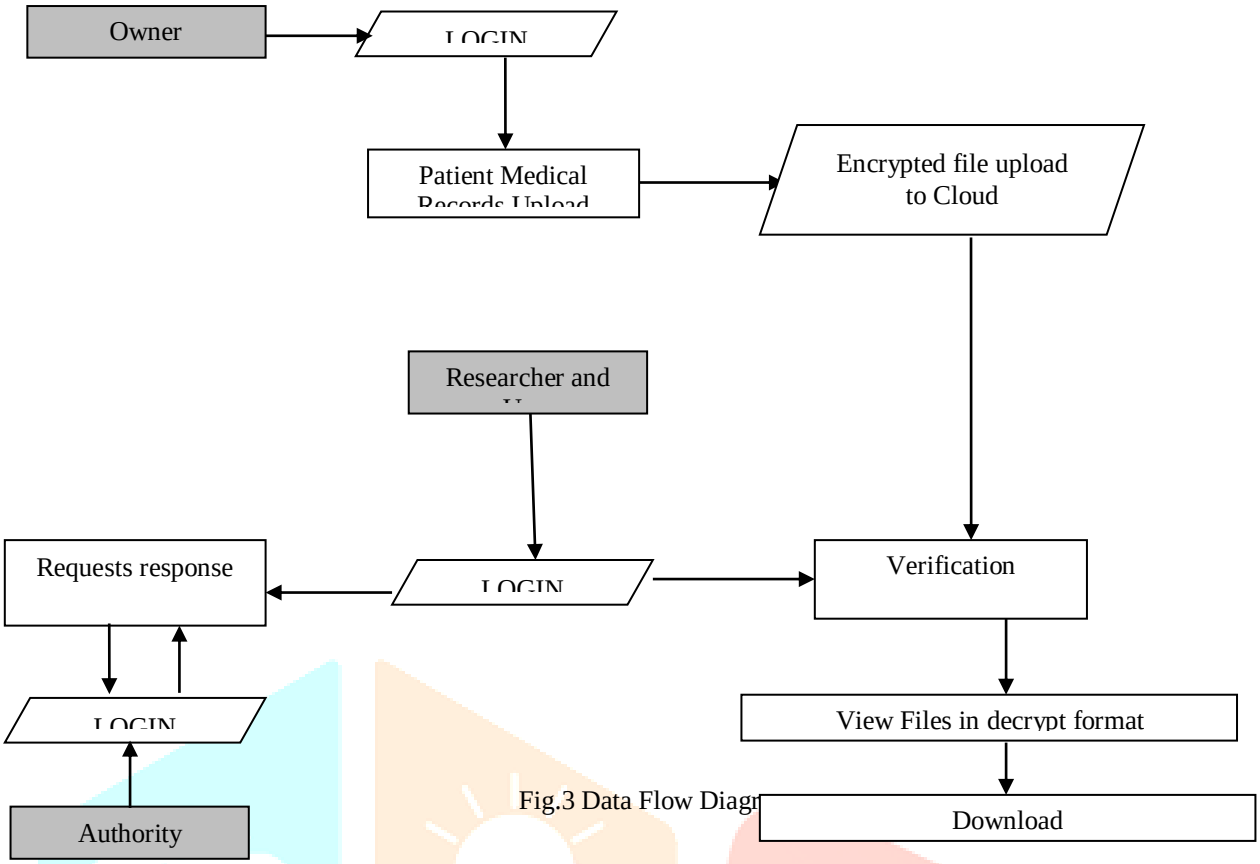

Fig.3 Data Flow Diagr

5. Implementation

5.1 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

a) What data should be given as input?
b) How the data should be arranged or coded?
c) The dialog to guide the operating personnel in providing input.
d) Methods for preparing input validations and steps to follow when error occur.

Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

5.2 Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

a) Convey information about past activities, current status or projections of the

b) Future.
c) Signal important events, opportunities, problems, or warnings.
d) Trigger an action.
e) Confirm an action.

Conclusion

In this paper, we proposed a variation of CP-ABE to productively share the various leveled documents in distributed computing. The various leveled records are encoded with a coordinated access structure and the figure text parts identified with characteristics could be shared by the documents. Along these lines, both figure text stockpiling and time cost of encryption are spared. The proposed plot has a preferred position that clients can decode all approval records by registering mystery key once. Along these lines, the time cost of decoding is likewise spared if the client needs to unscramble different records. Additionally, the proposed conspire is end up being secure under DBDH supposition.

References

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[2] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Secur., Oct. 2007, pp. 456–465.

[3] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. 10th Int. Workshop Inf. Secur. Appl., Aug. 2009, pp. 309–323.

[4] X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing," J. Universal Comput. Sci., vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[5] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, pp. 763–771, May 2014.

[6] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Inf. Sci., vol. 276, pp. 354–362, Aug. 2014.

[7] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," Int. J. Netw. Secur., vol. 16, no. 6, pp. 437–443, Nov. 2014.

[8] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in Proc. 16th Int. Conf. Inf. Commun. Secur., vol. 8958. Dec. 2014, pp. 274–289.

[9] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), vol. 9327. Sep. 2015, pp. 146–166.

[10] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," Future Generat. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015.

[11] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[12] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int. Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp. 346–358.

[13] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th Eur. Symp. Res. Comput. Secur., vol. 8712. Sep. 2014, pp. 257–272.

[14] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in Proc. 19th Eur. Symp. Res. Comput. Secur., vol. 8712. Sep. 2014, pp. 130–147.

[15] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[16] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "k-times attribute-based anonymous access control for cloud computing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[17] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[18] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp. 457–473.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., Oct. 2006, pp. 89–98.

[20] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," Chin. J. Electron., vol. 23, no. 4, pp. 778–782, Oct. 2014.