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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Data Centric Access Control in the Cloud Environment

N.Tamil Elakkiya[1], S. Usha[2]

M.E. Computer Science and Engineering, University College of Engineering, Tiruchirapalli, Bit Campus, Mandaiyur, Trichy-620024, India.

Assistant Professor, Department of Computer Science and Engineering, University College of Engineering, Tiruchirapalli, Bit Campus, Mandaiyur, Trichy-620024, India.

ABSTRACT: The main objective of this system is to develop an experimental model to store the data securely in cloud computing environment and provides high level of trustworthy data maintenance scheme to its users with Advanced Cryptographic Standards (ACS) scheme. More and more clients would like to store their data to PCS (public cloud servers) along with the rapid development of cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload them. Security is the main constraint in cloud computing environment, which depicts the nature of the surveillance mechanisms in remote server based data maintenance scheme. The authorization and authentication schemes provide the data owners and users to feel safe to maintain and retrieve their data without any interventions or intrusions. In this system a novel proof based trustworthy data management scheme, which allows the data owners to upload the data into the server with proper cryptographic principles such as Advanced Cryptographic Standards (ACS), RSA and so on. With these systems the data owner and data users can successfully maintain and retrieve the data to and from the server. For all the entire system of secure cloud computing scheme maintains the data into the remote server with proper authorization and authentication schemes as well as provides trust based services to its users with maximum level.

KEYWORDS: Data-Centric Security, Cloud Computing, Role-Based Access Control, Authorization.

I. INTRODUCTION

Security is one of the main user concerns for the adoption of Cloud computing. Moving data to the Cloud usually implies relying on the Cloud Service Provider (CSP) for data protection. Although this is usually managed based on legal or Service Level Agreements (SLA), the CSP could potentially access the data or even provide it to third parties. Moreover, one should trust the CSP to legitimately apply the access control rules defined by the data owner for other users. The problem becomes even more complex in Intercloud scenarios where data may flow from one CSP to another. Users may loss control on their data. Even the trust on the federated CSPs is outside the control of the data owner. This situation leads to rethink about data security approaches and to move to a data-centric approach where data are self-protected whenever they reside.

Encryption is the most widely used method to protect data in the Cloud. In fact, the Cloud Security Alliance security guidance recommends data to be protected at rest, in motion and in use. Encrypting data avoids undesired accesses. However, it entails new issues related to access control management. A rule-based approach would be desirable to provide expressiveness. But this supposes a big challenge for a data-centric approach since data has no computation capabilities by itself. It is not able to enforce or compute any access control rule or policy. This raises the issue of policy decision for a self-protected data package: who should evaluate the rules upon an access request? The first choice would be to have them evaluated by the CSP, but it could potentially bypass the rules. Another option

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

would be to have rules evaluated by the data owner, but this implies that either data could not be shared or the owner should be online to take a decision for each access request.

To overcome the aforementioned issues, several proposals try to provide data-centric solutions based on novel cryptographic mechanisms applying Advanced Cryptographic Standard (ACS). These solutions are based on Attribute-based Access Control (ABAC), in which privileges are granted to users according to a set of attributes. There is a long standing debate in the IT community about whether Role-based Access Control (RBAC) is a better model for authorization. Without entering into this debate, both approaches have their own pros and cons. To the best of our knowledge, there is no data-centric approach providing an RBAC model for access control in which data is encrypted and self-protected. The proposal in this system supposes a first solution for a data-centric RBAC approach, offering an alternative to the ABAC model.

An RBAC approach would be closer to current access control methods, resulting more natural to apply for access control enforcement than ABE-based mechanisms. In terms of expressiveness, it is said that ABAC supersedes RBAC since roles can be represented as attributes. However, when it comes to data-centric approaches in which data is encrypted, ABAC solutions are constrained by the expressiveness of ABE schemes. The cryptographic operations used in ABE usually restrict the level of expressiveness for access control rules. For instance, role hierarchy and object hierarchy capabilities cannot be achieved by current ABE schemes. Moreover, they usually lack some combination with a user-centric approach for the access control policy, where common authorization-related elements like definition of users or role assignments could be shared by different pieces of data from the same data owner.

This system presents SecRBAC, a data-centric access control solution for self-protected data that can run in untrusted CSPs and provides extended Role-Based Access Control expressiveness. The proposed authorization solution provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources.

This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing. Role and resource hierarchies are supported by the authorization model, providing more expressiveness to the rules by enabling the definition of simple but powerful rules that apply to several users and resources thanks to privilege propagation through roles and hierarchies. Policy rule specifications are based on Semantic Web technologies that enable enriched rule definitions and advanced policy management features like conflict detection.

A data-centric approach is used for data self-protection; where novel cryptographic techniques such as Proxy Re-Encryption (PRE), Identity-Based Encryption (IBE) and Identity-Based Proxy Re-Encryption (IBPRE) are used in past but in this system we follow Advanced Cryptographic Standard to secure the data. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. These techniques are used to protect both the data and the authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also combines a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data.

II. ENCRYPTION METHODOLOGIES - A SURVEY

SecRBAC makes use of cryptography to protect data when moved to the Cloud. Advanced cryptographic techniques are used to protect the authorization model in order to avoid the CSP being able to disclose data without data owner consent. Concretely, the solution is based on Proxy Re-Encryption (PRE). A PRE scheme is a cryptographic scheme that enables an entity called proxy to re-encrypt data from one key to another without being able to decrypt it. That is, given a couple of key pairs and proxy could re-encrypt a ciphertext c encrypted under public key to another ciphertext c that can be decrypted using private key. Using this kind of cryptography, a user u can encrypt a piece of data m using his own public key pub to obtain a ciphertext c. A re-encryption key rk can be generated for a proxy to reencrypt from to thus transforming c to another ciphertext c. Then, another user u can use his own private key priv to decrypt c and obtain the plain piece of data m. Several works in this direction have arisen, resulting in diverse Proxy Re-Encryption schemes with different features. The solution proposed in this paper is not tied to a concrete PRE scheme or implementation. However, not all

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

the available PRE schemes are suitable to achieve the goals of this research. In order to characterize and compare different schemes, provided a set of features relevant to proxy re-encryption. Based on this characterization, the following set of features are required by the Proxy Re-Encryption scheme used for the proposal in this paper: Unidirectionality. A unidirectional scheme enables the generation of a re-encryption key rk without allowing re-encryption from to Non-interactivity.

A non-interactive scheme enables a user u to construct a re-encryption key rk without the participation of u or any other entity. Multi-use. A multi-use scheme enables the proxy to perform multiple re-encryption operations on a single ciphertext. That is, to re-encrypt from c to c from c to c and so on. On the other hand, Identity-Based Encryption (IBE) is a type of public key cryptography in which key pairs for a given entity are generated based on the identity of that entity. Using this kind of cryptography, a piece of datamcan be encrypted using the identity id of a user u to obtain a ciphertext c. Then, user u can use his private key priv to decrypt c and obtain the plain piece of data m. Note that no public key pub is used for encryption, but the identity of the user id is applied instead. IBE schemes usually require the generation of a master key pair that is used to derive user keys based on their identities.

The master public key is publicly known and can be directly employed by users to generate the public key of another user based on his identity. In turn, the master private key should be kept private and users can obtain their private keys from a trusted entity that owns the master private key. This entity is called Private Key Generator (PKG). As will be seen in following sections, an authorization model is composed of several elements (e.g. subjects, roles, grants, etc). The usage of IBE avoids the need to generate and manage a public and private key pair for every authorization element. Instead, the identities of such elements can be directly used within the cryptographic operations. In past systems, an Identity-Based Proxy Re-Encryption (IBPRE) approach is proposed. It combines both IBE and PRE, al lowing a proxy to translate a ciphertext encrypted under a user's identity into another ciphertext under another user's identity. In this approach, a Master Secret Key (MSK) is used to generate user secret keys from their identities. These secret keys are equivalent to private keys in IBE.

No public keys are needed, since identities are directly used in the cryptographic operations. With this approach, a user u can encrypt a piece of data m using his identity id to obtain a ciphertext cid encrypted under id. A re-encryption key rk can be generated to re-encrypt from id to id. Then, a proxy can use rk to obtain another ciphertext cid under the identity of another user u. This can then use his own secret key sk to obtain the plain piece of data m. As for IBE approaches, the MSK should be kept private and users can obtain their secret key from the PKG. This IBPRE scheme is the one selected for the authorization solution proposed in this paper. It has been selected because it combines both PRE and IBE. It fulfills the three aforementioned requirements of proxy re-encryption and supports IBE, what allows to use the identities of the authorization elements for cryptographic operations, avoiding the need to generate and manage a key pair for each element.

The Advanced Cryptographic Standard (ACS), which is derived from the classical encryption algorithm called Advanced Encryption Standard (AES), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. ACS is a subset of the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the ACS selection process. Rijndael is a family of ciphers with different key and block sizes. For ACS, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. ACS has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977.

The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. In the United States, ACS was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable.

Authorization Model With Enriched Role based Expressiveness

The management of access control and security could become a difficult and error prone task in distributed systems like Cloud computing. Authorization models providing high expressiveness can help to control and manage security and to deal with this complexity. They can aid administrators with this task by enabling the specification of high-level access control rules that are automatically interpreted by system for this to behave as defined by the

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

administrator. Role-Based Access Control (RBAC) is an authorization scheme supported by most of the current authorization solutions. In this approach, the authorization model makes use of the Role concept to assign privileges to subjects. A set of subjects can be assigned to one or more roles which, in turn, can be associated to a set of privileges.

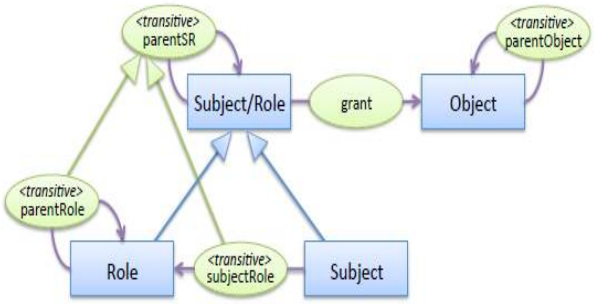

Fig. 1. Ontology representing the authorization model

This provides more expressiveness to the authorization model, making it easier to manage privilege assignments through roles. To illustrate the concepts described along this system, let us consider an example where a company uploads to the Cloud a couple of documents called DocumentX and DocumentY which could be accessed only by the managers of the company. Also consider that Bob and Alice are managers of this company. Without role support in the authorization model, the company should define and manage individual privilege assignments for every user and every document. That is, four privileges should be defined in this example: Bob ! DocumentX, Bob ! DocumentY , Alice ! DocumentX and Alice ! DocumentY.

On the other hand, making use of roles, a Managers role could be defined to group all users that are managers of the company and two single privileges need to be defined: Managers DocumentX and Managers ! DocumentY . Let us denote them p1 and p2, respectively. This provides more expressiveness to the model, making it more natural for the administrator to manage privileges, as well as avoiding the need to manage individual privileges.

This authorization model can be extended to hierarchical RBAC (hRBAC). Hierarchical RBAC enables the definition of role hierarchies. These hierarchies establish privilege inheritance between roles, making a child role to inherit all the privileges defined for parent roles in the hierarchy. The major motivation for adding role hierarchy to RBAC is to simplify role management. A child role r1 2 T can be defined as member of another parent role r2 2 T. It makes the system to consider instances belonging to any parent role, to be also belonging to its child roles in the hierarchy. Following the example, consider that Bob is a sales manager whereas Alice is a finance manager.

```
SELECT ?authorizedRole ?authorizedObject
WHERE {
   {
      <subject> <GRANTED> <object>
   } UNION {
      <subject> <GRANTED> ?authorizedObject .
      <object> <PARENT_OBJECT> ?authorizedObject
   } UNION {
      ?authorizedRole <GRANTED> <object> .
      <subject> <PARENT_SUBJECT> ?authorizedRole
   } UNION {
      ?authorizedRole <GRANTED> ?authorizedObject .
      <subject> <PARENT_SUBJECT> ?authorizedRole .
      <object> <PARENT_OBJECT> ?authorizedObject
   }
}
```

Listing 1. SPARQL authorization query

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Also consider that another document DocumentZ is only intended for sales managers. Both users should still have access to DocumentX and DocumentY, but only Bob should have access to DocumentZ. Making use of role hierarchies, two roles SalesManager and FinanceManager could be defined as children of the Managers role. Then, Bob would be assigned to SalesManager and Alice to FinanceManager –instead of being both assigned to Managers. Another privilege p3 could be now defined as SalesManager ! DocumentZ. This way, Bob would have access to DocumentZ by p3. Moreover, by privilege propagation through the role hierarchy, both users would still have access to DocumentX and DocumentY by p1 and p2. It should be noticed that privilege inheritance in this hierarchy is transitive. That is, if r1 2 T is a child of r2 2 T and r2 is a child of r3 2 T, then r1 will inherit all the privileges from both r2 and r3.

Self-Protected Authorization Model For Data-Centric Security

The authorization model presented in earlier system determines the privileges that are granted to subjects. It should be evaluated by the Cloud Service Provider upon an access request in order to decide whether such a request is permitted or not. However, if data is not cryptographically protected then the CSP could potentially access the data for its own benefit. Moreover, the data owner should trust the CSP to legitimately evaluate the model and enforce the authorization decision. If the authorization rules are not cryptographically protected then they can be overridden by the CSP, making it able to access the data or to release it to any third party. A self-protected authorization model is needed to achieve a data-centric mechanism that technically guarantees the CSP cannot access or disclose data to unauthorized parties. This section describes a protected authorization model for a data-centric solution. A self-protection mechanism is provided to assure data can only be accessed by authorized subjects according to the data owner rules.

III. EXISTING SYSTEM

Data Security over remote environments are the major issue in the remote server data maintenance or cloud environments. The problem becomes even more complex in Inter-cloud scenarios where data may flow from one CSP to another. Users may loss control on their data. Even the trust on the federated CSPs is outside the control of the data owner. This situation leads to rethink about data security approaches and to move to a data-centric approach where data are self-protected whenever they reside.

Disadvantages

- Lack of data
- Missing Data Integrity
- Trust Failure nature in maintenance

IV. PROPOSED METHODOLOGY

- Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.
- Rule-based approach for authorization where rules are under control of the data owner.
- High expressiveness for authorization rules applying the RBAC scheme with role hierarchy and resource hierarchy (Hierarchical RBAC or hRBAC).
- Access control computation delegated to the CSP, but being unable to grant access to unauthorized parties.
- Secure key distribution mechanism and PKI compatibility for using standard X.509 certificates and keys with ACS support.

V. LITERATURE SURVEY

CSA Security Guidance for Critical Areas of Focus in Cloud Computing seeks to establish a stable, secure baseline for cloud operations. This effort provides a practical, actionable roadmap to managers wanting to adopt the cloud paradigm safely and securely. Domains are reviewed to emphasize security, stability, and privacy in a multi-tenant environment. Security Guidance Version 3.0 incorporates the highly dynamic nature of IT and new developments within other CSA research projects, tying in various CSA activities into one comprehensive C-level best

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

practice. Security Guidance v3.0 will serve as the gateway to emerging standards being developed in the world's standards organization and is designed to serve as an executive-level primer to any organization seeking a secure, stable transition to hosting their business operations in the cloud.

In the past few years, cloud computing has emerged as one of the most influential paradigms in the IT industry. As promising as it is, this paradigm brings forth many new challenges for data security because users have to outsource sensitive data on untrusted cloud servers for sharing. In this paper, to guarantee the confidentiality and security of data sharing in cloud environment, we propose a Flexible and Efficient Access Control Scheme (FEACS) based on Attribute-Based Encryption, which is suitable for fine-grained access control. Compared with existing state-of-the-art schemes, FEACS is more practical by following functions. First of all, considering the factor that the user membership may change frequently in cloud environment, FEACS has the capability of coping with dynamic membership efficiently. Secondly, full logic expression is supported to make the access policy described accurately and efficiently. Besides, we prove in the standard model that FEACS is secure based on the Decisional Bilinear Diffie-Hellman assumption. To evaluate the practicality of FEACS, we provide a detailed theoretical performance analysis and a simulation comparison with existing schemes. Both the theoretical analysis and the experimental results prove that our scheme is efficient and effective for cloud environment.

We present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under concrete and noninteractive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, ciphertext size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

VI. SYSTEM ARCHITECTURE DESIGN

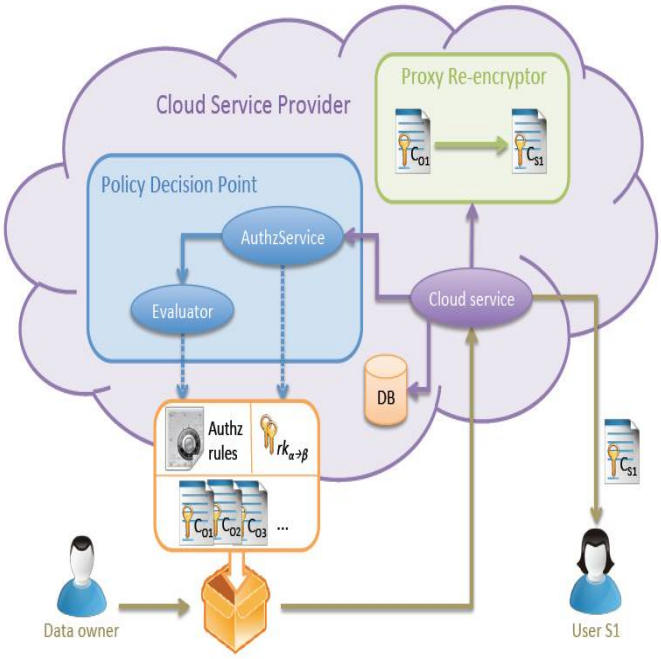

Fig.1 System Architecture Design

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VII. EXPERIMENTAL RESULTS

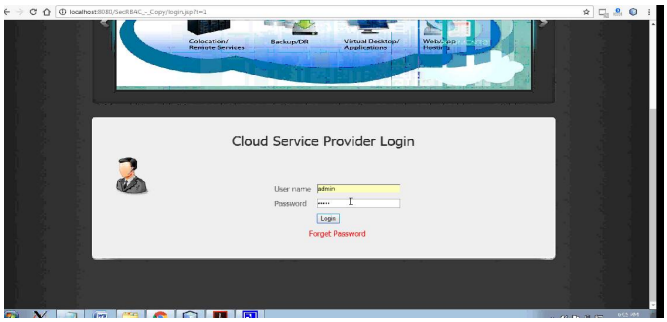

Fig.2 Cloud service Provider Login

Fig.3 CSP Home Page

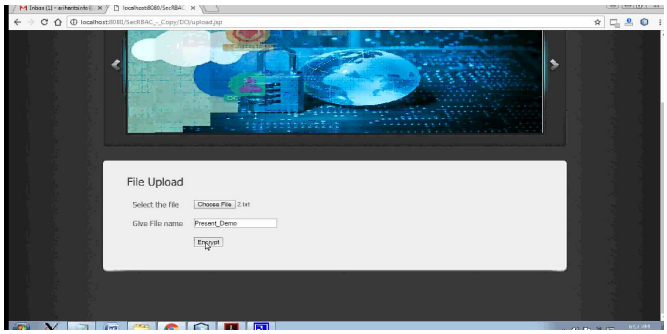

Fig.4 Upload File

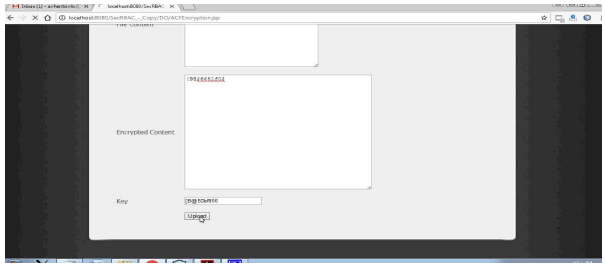

Fig.5 File Encrypted

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

VIII. CONCLUSION AND FUTURE SCOPE

A data-centric authorization solution has been proposed for the secure protection of data in the Cloud. SecRBAC allows managing authorization following a rule-based approach and provides enriched role-based expressiveness including role and object hierarchies. Access control computations are delegated to the CSP, being this not only unable to access the data, but also unable to release it to unauthorized parties. Advanced cryptographic techniques have been applied to protect the authorization model. A re-encryption key complements each authorization rule as cryptographic token to protect data against CSP misbehavior. The solution is independent of any PRE scheme or implementation as far as three specific features are supported.

A concrete IBPRE scheme has been used in this system in order to provide a comprehensive and feasible solution. A proposal based on Semantic Web technologies has been exposed for the representation and evaluation of the authorization model. It makes use of the semantic features of ontologies and the computational capabilities of reasoners to specify and evaluate the model. This also enables the application of advanced techniques such as conflict detection and resolution methods. Guidelines for deployment in a Cloud Service Provider have been also given, including a hybrid approach compatible with Public Key Cryptography that enables the usage of standard PKI for key management and distribution. A prototypical implementation of the proposal has been also developed and exposed in this system, together with some experimental results.

Future work of this approach includes the analysis of novel cryptographic techniques that could enable the secure modification and deletion of data in the Cloud. This would allow extending the privileges of the authorization model with more actions like modify and delete. Another interesting point is the obfuscation of the authorization model for privacy reasons. Although the usage of pseudonyms is proposed, but more advanced obfuscation techniques can be researched to achieve a higher level of privacy.

REFERENCES

[1] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” CSA, Tech. Rep., 2003.
[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, “Feacs: A flexible and efficient access control scheme for cloud computing,” in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.
[3] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.
[4] B. B and V. P, “Extensive survey on usage of attribute based encryption in cloud,” Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS ’06, New York, NY, USA, 2006, pp. 89–98.
[6] InterNational Committee for Information Technology Standards, “INCITS 494-2012 - information technology - role based access control - policy enhanced,” INCITS, Standard, Jul. 2012.
[7] E. Coyne and T. R. Weil, “Abac and rbac: Scalable, flexible, and auditable access management,” IT Professional, vol. 15, no. 3, pp. 14–16, 2013.
[8] Empower ID, “Best practices in enterprise authorization: The RBAC/ABAC hybrid approach,” Empower ID, White paper, 2013.
[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, “Adding attributes to rolebased access control,” Computer, vol. 43, no. 6, pp. 79–81, 2010.
[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-encryption schemes with applications to secure distributed storage,” ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.
[11] F. Wang, Z. Liu, and C. Wang, “Full secure identity-based encryption scheme with short public key size over lattices in the standard model,” Intl. Journal of Computer Mathematics, pp. 1–10, 2015.
[12] M. Green and G. Ateniese, “Identity-based proxy re-encryption,” in Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ser. ACNS ’07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 288–306.
[13] A. Lawall, D. Reichelt, and T. Schaller, “Resource management and authorization for cloud services,” in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, ser. S-BPM ONE ’15, New York, NY, USA, 2015, pp. 18:1–18:8.
[14] D. Y. Chang, M. Benantar, J. Y.-c. Chang, and V. Venkataramappa, “Authentication and authorization methods for cloud computing platform security,” Jan. 1 2015, uS Patent 20,150,007,274.
[15] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.
[16] G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS ’10, New York, NY, USA, 2010, pp. 735–737.
[17] J. Liu, Z. Wan, and M. Gu, “Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing,” in Information Security Practice and Experience. Springer Berlin Heidelberg, 2011, vol. 6672, pp. 98–107.
[18] W3C OWL Working Group, “OWL 2 Web Ontology Language: Document overview (second edition),” World Wide Web Consortium (W3C), W3C Recommendation, Dec. 2012.
[19] J. M. A. Calero, J. M. M. Perez, J. B. Bernabe, F. J. G. Clemente, G. M. Perez, and A. F. G. Skarmeta, “Detection of semantic conflicts in ontology and rule-based information systems,” Data & Knowledge Engineering, vol. 69, no. 11, pp. 1117 – 1137, 2010.
[20] W3C OWL Working Group, “OWL 2 Web Ontology Language: Profiles (second edition),” World Wide Web Consortium (W3C), W3C Recommendation, Dec. 2012.