J Inf Process Syst, Vol.15, No.3, pp.538~549, June 2019
https://doi.org/10.3745/JIPS.03.0117

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

# A Secure Cloud Computing System by Using Encryption and Access Control Model

Ghassan Sabeeh Mahmood*,**, Dong Jun Huang*, and Baidaa Abdulrahman Jaleel**

**Abstract**

Cloud computing is the concept of providing information technology services on the Internet, such as software, hardware, networking, and storage. These services can be accessed anywhere at any time on a pay-per-use basis. However, storing data on servers is a challenging aspect of cloud computing. This paper utilizes cryptography and access control to ensure the confidentiality, integrity, and proper control of access to sensitive data. We propose a model that can protect data in cloud computing. Our model is designed by using an enhanced RSA encryption algorithm and a combination of role-based access control model with extensible access control markup language (XACML) to facilitate security and allow data access. This paper proposes a model that uses cryptography concepts to store data in cloud computing and allows data access through the access control model with minimum time and cost for encryption and decryption.

**Keywords**

Access Control, Cloud Storage, Encryption, Security

## 1. Introduction

Cloud computing allows network access to a shared set of resources, such as servers, services, networks, applications, and storage) [1]. Cloud is a common topic in applications research; cloud is considered as important as electrical facility services, gas, water, and telecommunication services [2].

Cloud services consist of three services, namely, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). With IaaS, the provider offers the user with handling, storage, communities, and standard computing resources that he or she can manage; the user can then utilize almost any software with an operating system (OS). The user of an OS, space of storage, or installed applications is not necessary to manage the key of cloud infrastructure, for example service host firewalls [3].

PaaS allows customers to improve, implement, and manage the applications without the difficulty of construction and preserving the infrastructure associated with the development and launch of an application. In PaaS, any user can manage implemented applications with configurations for program hosting surroundings, such as the Google Apps Engine [4].

SaaS pertains to the simple use of applications that run on a cloud computing infrastructure; these

Manuscript received September 22, 2017; first revision March 14, 2018; accepted July 14, 2018.

**Corresponding Author:** Ghassan Sabeeh Mahmood (ghassan.programer@gmail.com)

* School of Information Science and Engineering, Central South University, Changsha, China (ghassan.programer@gmail.com, djhuang@csu.edu.cn)

**Dept. of Computer Science, College of Science, University of Diyala, Baquba, Iraq (baidaa.rahman@gmail.com)

applications are provided through the provider of cloud computing. The user does not need to control and manage the cloud infrastructure, except for a user-specific application that requires setting configurations [3].

The services in the cloud can be classified to four deployment models, namely, private cloud, public cloud, hybrid cloud, and community cloud. The configuration of a public cloud is distributed among people or in a big market group held by a marketing cloud service. One company controls the structure of a private cloud. A private cloud is usually maintained or even authorized by a company. The composition of a hybrid cloud includes a formula that consists of additional clouds, such as community, public, or private clouds. The structure of a community cloud can be contributed by several agencies, may help a specific area, and facilitate team awareness of contributed problems. A community cloud is enabled by agencies and third parties [5].

The cloud is increasingly used as it allows users convenient access to data and it is done from anywhere and at any time via the Internet [6]. Cloud data storage gives users easy access without having to know directly of deployment and management of infrastructure or hardware. The cloud is stronger than a personal computer, but with all these benefits of cloud computing, it brings challenges and security problems. Access control mechanisms are used to ensure that unauthorized users cannot access the system in cloud computing. This mechanism also ensures that users who have access to the system cannot do unauthorized changes or alterations.

Access control models are being on three kinds, namely, discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC). Access control in DAC is based on user identity. It is used in commercial transactions, but not convenient for military attitudes that requires specific monitoring is for the many flows of information. In MAC, access rights are determined by an essential authority or manager of the system. MAC is considered a suitable solution in terms of dealing with government programs as well as military. But it is very accurate for business solutions. In RBAC, access rights are defined for roles rather than separate users. Privileges are allocated to various roles, which are then assigned to users [7].

The RBAC model has more advantages than discretionary and mandatory access control models, but it poses problems in real world applications. Divide subjects into groups depending on roles can make works worse, while choosing the appropriate roles that representing the model is a difficult task. A role in RBAC model classifies subjects in a number of classes. Each subject should have a role to facilitate access to the system. Roles can provide subjects with additional rights and acquire another role, which could lead to abuse of access security policies [8].

Security is a key requirement in robust and meaningful cloud computing systems. Security risks motivated us to devise sound solutions to protect cloud data. Therefore, in this paper cryptography technique is used to validate data confidentiality prior to outsourcing data to cloud computing and allows data access through the access control model. The rest of this paper is organized as follows. Section 2 describes related works. Section 3 includes cloud computing security. Section 4 describes the proposed scheme used in the paper. Section 5 demonstrates the experimental results. Conclusions are given in Section 6.

## 2. Related Works

In this section, we have summarized several previous cloud computing models that are more related to our model, as well as the challenges they face. Zhou et al. [9] suggested a model that achieves RBAC securely and is applied to data that has been encrypted before being sent to the cloud. This model then presents an RBAC that allows an organization to store data in a public cloud while maintaining information related to the organizational structure in a private cloud. A cloud system is then developed, which is characterized by a decryption key and constant size cipher text. The experiment showed that encryption and decryption computations belong to the client side. Decryption time can be reduced by utilizing multiple processors. The proposed model is useful in commercial states, flexibly captures practical and offers secure data storage in the cloud. Nevertheless, does not consider the overall credibility of the user and delegation of authority. While Wei et al. [10,11] presented a RBAC proxy at the application level for packet filtering in the substation domain using Distributed Network Protocol 3.0 (DNP3). In their system, RBAC is described in XML and roles are denoted as numbers. XML is a normal language for encoding files and does not describe access control policies. The semantics of a role are carried in its name and numbers are used for names, thereby resulting in a semantic ambiguity. Cloud optimized RBAC model (CORBAC) proposed by Zhu et al. [12] includes numerous features of role-based access control and distributed RBAC l. In the CORBAC model, each organization has its own internal RBAC with a single managerial role. This model confers power to the certificate authority and connects distributed authentication services. This model works by assigning domains that can handle users and their roles within the network. Hierarchical caches were affixed within the CORBAC model to augment the effectiveness of the access control system. Certificate issuance may lead to efficiency problems. These problems can affect the functioning of organizations with several users because these users require novel certificates for each access.

Mon and Naing [13] proposed a privacy enhancement model based on private cloud computing; this model used the source cloud computing infrastructure Eucalyptus Open. This model was called attribute role-based access control. This model is a combination of RBAC and ABAC model. The model aims to ensure the privacy of cloud computing users and security of private information, but it does not offer clarity on how the same shall be achieved. Distributed RBAC (DRBAC) model proposed by Wang et al. [14] to reduce authorization loads, entities of RBAC are distributed on a network in a substation. Moreover, roles can be defined locally or globally. A specific local role is defined to a substation or many local roles to a substation. Also a global role is defined to the substation, and activating the role by a remote user in the substation to obtain all the local roles. However, this model is conceptual without implementation details. Rosic et al. [15] proposed access control model for Smart Grid systems depending on areas of responsibility and regional division. For that, the role based access control model extended to the protection of the resource. The study of Rosic et al. [15] is also without implementation, like Wang et al.'s work. Bell and La Padula [16] proposed mandatory access control scheme by focused on securing and controlling data flow, but protecting the confidentiality of data in access control systems is not the only goal.

Other models of data protection cloud computing include the use of direct encryption. Through these models, data encryption is directly allowed to users who want to share data on the cloud-computing environment [17,18]. This concept is similar to DAC model. They are therefore commonly used in systems where the DAC model is adopted.

## 3. Cloud Computing Security

Data are important. Data are formed from several sources, such as people, devices, and sensors. Given the multifaceted nature of data, we are forced to deal with an important concept that affects all scientific areas [19]. Information safety and trust matters are the key tasks of cloud [20]. The risk of data abuse emerges when multiple users share resources. Thus, access and process must be secured to avoid data abuse.

The three important requirements of cloud security are confidentiality, integrity, and availability.

- *Confidentiality*: Confidentiality limits access of information to authorized persons. The use of cloud computing to store data means providing authority to cloud computing systems. Providing strong authentication and protecting user account from being stolen is a chief concern in external security, as well as avoidance of internal threat.
- *Integrity:* It is a main element of important electronic information, where only authorized persons can modify the information. Data access within the local infrastructure can be limited and monitored to guarantee integrity. However, cloud computing is owned by another party and all information uploaded to cloud computing are recorded and controlled by a cloud service provider. Users require authentication to control the integrity of data.
- *Availability*: When requirements are not satisfied, users need to know what is happening, why they cannot access the data, and how and when it will be fixed. Users want to obtain the information they need. Availability is not a problem in the cloud because the service provider has several servers. They can backup data and hire professionals to manage the information center. The backup mechanism is processed in cloud computing and the user can never know whether a backup server exists or not. This process limits use control [21].

In addition to the main requirements of cloud computing, there are also important requirements for the cloud access control that are:

- *Assign of privileges*: It is an important concept in any model of access control. As few steps are required to set or mitigate privileges, this reduces the number of human errors or system errors. Therefore, the steps to add, remove, and change privileges or capabilities to a particular theme in the access control system are necessary and critical to their usability in such systems [22].
- *Flexibility*: Cloud computing is a dynamic environment, so flexibility in the access control system is essential to deal with such dynamic environments. Through flexibility, effective management of access control models can be provided [22].
- *Delegation*: To enable access control models to be flexible and have the dynamic management of the resources used in cloud computing, it is important to support delegation of roles and permissions [23].
- *Auditing:* The auditing is one of the key aspects of protecting cloud computing paradigm and access control models used in it. The audit shall monitor the status of the system in access control models, record any system failures and monitor any attempt to violate the access policy or make a change of privileges [24].
- *Confidentiality*: It is a key issue of protecting data in the cloud; the data owner encrypts the data before sending it to cloud storage. Consequently, the unauthorized user and cloud service provider cannot know the encryption data [25].
- *Scalability*: As the number of authorized cloud computing user's increases, the cloud-computing server has been able to implement efficiently. Therefore, increasing the number of authorized users does not affect cloud server performance [26].

# 4. Proposed Scheme

## 4.1 Sub-parameters of Our System

In order to protect and ensure the security of data in the cloud, we proposed data security protection using encryption and access control model. Therefore, the security system in this proposed model is completed according to the following sub-parameters.

### 4.1.1 Cryptography

Cryptography algorithms are the most common solution used for ensuring data security in the cloud. A key security is one of the challenges related to cryptography in cloud computing; this approach prevents compromise of encrypted data and ensures that authentic users can access the keys [27].

Rivest et al. [28] proposed a practical public-key system named RSA. This algorithm utilizes two keys, namely, public key, which is utilized in order to encrypt plaintexts published to the public, and private key, which is utilized in order to decrypt ciphertext known to the owner only.

The RSA encryption algorithm has been widely used to provide privacy and to ensure high confidentiality of data. Despite this use, many attacks render the use of this algorithm inefficiently. Specifically, when a coefficient is used not at the required level. This makes the factorization attacks achieve their results efficiently, which affects the performance of this algorithm [29].

In the proposed scheme, an improved RSA algorithm to overcome the drawbacks of standard RSA is suggested. This scheme utilizes two keys, namely, valuation key, which is utilized by a third party to execute operations on encrypted data, and the second key (private key), which is used to encrypt and decrypt data and known only to the data owner.

### 4.1.2 Access control

The access control mechanism is used to prevent unauthorized users from accessing the system in cloud computing. On the other hand, provide a guarantee that authorized clients cannot make any inappropriate modifications.

In RBAC, access rights are defined for roles and the privileges are allocated to various roles, which are then allocated to users. RBAC can verify user identity, but it does not consider the overall credibility of the user. A user can exercise his or her permission, but RBAC model cannot supervise this process. Thus, we suggest a combination of RBAC model with extensive access control markup language (XACML) to limit user access and protect the system from unauthorized access. The propose scheme use XACML, a standard access control policy language, to specify RBAC policies, request, and response. XACML offers a perfect reference for implementing an authorization principle that consists of policy administration point (PAP), policy decision point (PDP), policy enforcement point (PEP), policy info point (PIP), and policy retrieval point (PRP) [30].

## 4.2 The Complete Scheme

In the proposed system, the data owner will encrypt the data by RSA encryption to achieve the confidentiality of data, which will then be accessed by that user only. His access has an appropriate role specified by RBAC using XACML.

### 4.2.1 Maintaining data confidentiality

Confidentiality is a key issue for secure data in this model. The data owner encrypts the data using our enhanced RSA algorithm when a user requests access to this model. The enhanced RSA algorithm uses two keys, namely, valuation key, which is used by a third party to perform operations on encrypted data, and the second key (private key), which is used to encrypt and decrypt. The main part of the enhanced RSA algorithm is as follows:

- Key generation stage: The data owner at first generates both the valuation key and the private key as well.
- Encryption stage: Data owner encrypts the data using the private key and he then sends the encrypted data to the cloud before sending the valuation key and the private key to a third party.
- Processing stage:
  - The data owner sends a request to a third party for performing operations on the encrypted data when the user sends requests to the access manager to obtain access and to the data owner to obtain the data.
  - The third party sends a request to a cloud to get the encrypted files.
  - The third party handles the demand and executes the operations using the valuation key after the user obtaining permissions to access.
  - The third party returns the result of the process (in encrypted mode) and the user's private key.
- Decryption stage: The user decrypts the returned result using the private key.

### 4.2.2 Supporting RBAC using XACML

Since cloud has a dynamic environment, the relationship between the role and the actual activity of access control does not change, but will change because of its conditions and external environment. Therefore, a dynamic element is necessary between the role and the permission that governs the relationship between them, according to the current changes in cloud computing.

The proposed scheme will introduce the concept of security based on a RBAC model using the XACML model for access control. When the user requests access to the model it will be depending on the role, otherwise the user request will be rejected.

After the user has requested access to the model, the access manager sends a request for the policy enforcement point, which then validates the credibility by sending XACML request to the policy decision point. The policy management point sends the policy decision point relevant to the credibility decision policy. The policy decision point, then returns the policy decision result to the policy enforcement point of returning the XACML response. The policy enforcement point returns the credibility value achieved through computation to access management. Access management returns the credibility value received from the policy enforcement point to roles and permissions. Trusted users, then performs role mapping. After obtaining permissions, the role is assigned and permission is granted to the corresponding role. The cloud then sends the required data. The third party handles the request and performs the operations requested by the data owner using the valuation key. The third party, then returns the processed result (in encrypted form) with a private key to the user. The user decrypts the returned result using the private key. Fig. 1 shows the architecture of the proposed model.

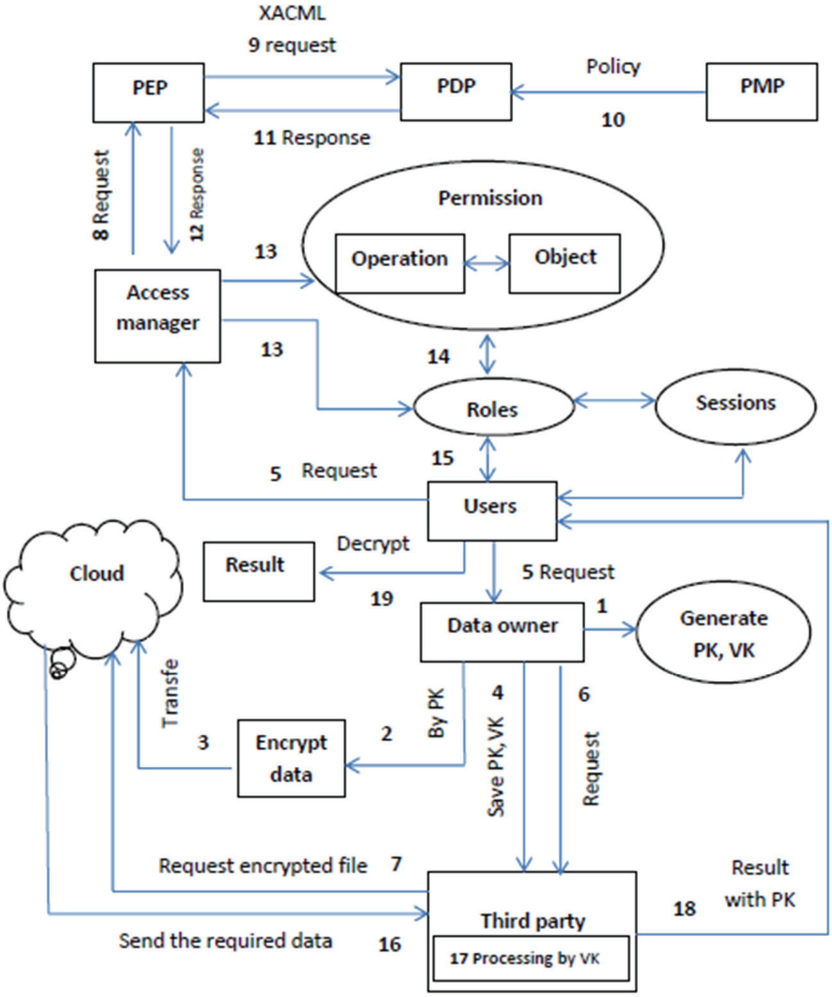


**Fig. 1.** Architecture of the proposed model.

## 4.3 Supporting Security Principles

Data are currently an important element in all areas of life. They are assembled and created from many sources, such as users, multiple devices that generate data, and so on. Consequently, we are dealing with an important issue that is involved in all fields of science. In addition, the problem of protecting this data is a key issue in cloud computing. When users share resources, the risk of data misuse is imperative. It is therefore necessary to secure these data to avoid the risk of abuse [25].

Therefore, the access control in the proposed scheme supports a number of security principles that enable the client to work on cloud computing environment securely as follows:

- *Principle of privilege:* the principle of granting the subject only the required permissions, regardless of whether the subject has more permissive than is necessarily required. In this model and to achieve this principle, each user of this model has multiple roles, each role has a collection of completed operations, and these operations have a collection of permissions. Therefore, the user assigns the roles that use the requested operation, and this process only requires permission to perform its actions even when it has full privileges.

- *Delegation of authority:* Establishing a relationship between roles, permissions and roles, as well as between users of the model and roles. This ability between these relations enables security policies to be implemented properly, especially with regard to the delegation of authority. This allows to assign delegation permissions from a role to another role. In this model, if a user has a particular role and has a process that works for them but cannot complete the process, the administrator assigns the process to another user instead.
- *Separation of duties:* To complete a critical task in this model, there can be a necessary need for mutual roles. Such as the request of the registration director and the officer responsible for issuing the documents to participate in the issue of a university graduate certificate.
- *Authorization principle:* RBAC can verify user identity, but it does not consider the overall credibility of the user. A user can exercise his or her permission, but RBAC model cannot supervise this process. Thus, the proposed scheme use XACML to specify RBAC policies, request, and response. XACML offers a reference model for executing an authorization scheme.
- *Confidentiality of data:* To achieve data confidentiality in this model, the concept of encryption is used before data is sent and stored in cloud computing by using the enhanced RSA algorithm. To avoid misuse of CSP or any threat to data in cloud storage.

# 5. Experimental Analysis

This section focuses on the performance of the proposed system. This system is implemented using Java Technology based on files size and time required to process these files. The performance results are gotten from Intel Core i5 CPU runs at 1.70 GHz, 8 GB of memory (RAM). Table 1 highlights the response time of cryptographic in terms of encryption and decryption as well as the execution time of sending and receiving data with different sizes.

**Table 1.** Execution time and cryptographic performance

| Response time (s) | | | Execution time (s) | |
|---|---|---|---|---|
| **Block size (kB)** | **Encryption performance** | **Decryption performance** | **Send data** | **Receive data** |
| 256 | 0.3122 | 0.6245 | 0,5242 | 0,8372 |
| 512 | 0.6873 | 0.7648 | 0,8143 | 0,9743 |

The simulation experiment for access control compares the difference between the RBAC in [20] and the proposed model, which is a combination of RBAC and XACML (see Table 2). The number of service requests of our access model is higher that of the traditional RBAC model. This experiment indicates that our access model can perform better than role-based access model [20] in terms of throughput. Therefore, our access control mode has a more secure permission granting mechanism that can improve data security in a cloud-computing environment.

**Table 2.** Difference in mean throughput

| User requests | Mean throughput (kr/s) | |
|---|---|---|
| | **Traditional RBAC** | **Our proposal** |
| 5 | 29 | 30 |
| 7 | 40 | 42 |
| 9 | 48 | 50 |
| 11 | 49 | 53 |
| 13 | 45 | 47 |
| 15 | 43 | 44 |

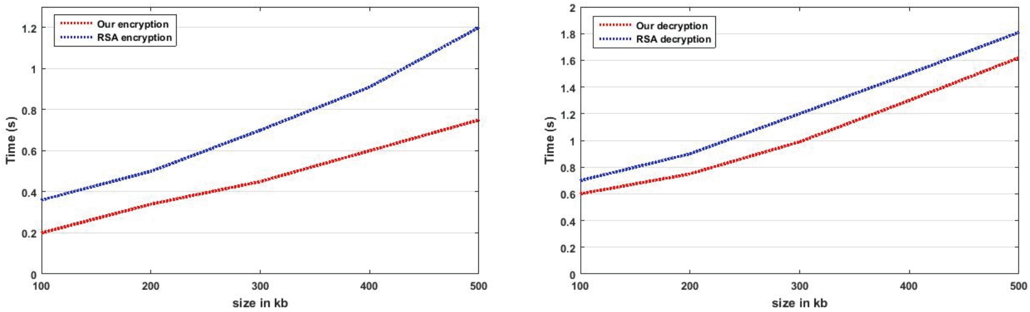
In order to validate the proposed model, it is compared with classical access models (DAC [18], Mac [16], and RBAC [9]) based on security features that include (scalability, privileges, delegation, auditing, flexibility, data confidentiality and authorization) as shown in Table 3. As noted from a table the proposed model meets all of the security features mentioned, making it applicable in the cloud computing environment.

**Table 3.** Comparison of access control models

| Comparison criteria | DAC [18] | MAC [16] | RBAC [9] | Our model |
|---|---|---|---|---|
| Scalability | No | No | Yes | Yes |
| Privileges | No | No | Yes | Yes |
| Delegation | Yes | No | No | Yes |
| Auditing | Yes | Yes | Yes | Yes |
| Flexibility | No | No | Yes | Yes |
| Data confidentiality | No | Yes | Yes | Yes |
| Authorization | No | No | No | Yes |

Depending on these features, we are very confident that the model discussed in this research paper is a scalable and effective model. So that a set of users can be handled through the role principle in the access control model. In addition, this model can support the principle of Privileges by giving this subject the required permissions only. Even when the subject has more permissive than is required. Moreover, this model can support segregation of duties by exchanging roles to complete a critical task. In order to make the proposed access control model flexible enough and dynamic in terms of operating in the cloud computing environment, the proposed model supports delegation of capabilities so that users working on this model collaborate to fulfill their desired tasks. While the proposed model provides a secure way of controlling access in the cloud-computing environment, in terms of using the audit to monitor the state of the system and recording the information required for control. To ensure data confidentiality our model uses cryptography concept using an enhanced RSA algorithm before store the data in cloud computing. We also used XACML to define RBAC policies, responses, and requests. This is because XACML is considered a reference to the implementation of the authorization process. In terms of flexibility, our model is flexible and easy to implement in a cloud computing environment. On the other hand, it uses the role and the principle of XACML, which ensures easy access and efficient privileges.

Furthermore, Fig. 2(a) and (b) present the results of the time differences based on the encryption and decryption of both our proposal and RSA. The experimental results shown in Fig. 2 were based on different data sizes. Our model simulates the encryption process before sending sensitive data to cloud computing as shown in Fig. 2(a). The results in figures showed that our scheme took less time than the RSA algorithm.



(a) (b)

**Fig. 2**. Comparison between our cryptography and original RSA: (a) encryption process and (b) decryption process.

## 6. Conclusion

This scheme presented a model for protecting data in cloud computing, which called a secure cloud computing system by using encryption and access control model. This model is designed using enhanced RSA algorithm and a mixture of RBAC and XACML to strengthen security and allow data access. This model can achieve encryption and decryption at the shortest time and lowest cost. The simulation experiment proves that this access model show is more advantageous than the traditional RBAC with throughput. This access model has secure permission mechanism that can improve security, maintenance of cloud data and other resources.

## References

[1] E. F. Coutinho, F. R. de Carvalho Sousa, P. A. L. Rego, D. G. Gomes, and J. N. de Souza, “Elasticity in cloud computing: a survey,” *Annals of Telecommunications*, vol. 70, no. 7-8, pp. 289-309, 2015.

[2] X. Liu and J. Liu, “A distributed management method in cloud computing environment,” *International Journal of Hybrid Information Technology*, vol. 9, no. 5, pp. 371-380, 2016.

[3] J. Carretero and J. G. Blas, “Introduction to cloud computing: platforms and solutions,” *Cluster Computing*, vol. 17, no. 4, pp. 1225-1229, 2014.

[4] C. N. Hofer and G. Karagiannis, “Cloud computing services: taxonomy and comparison,” *Journal of Internet Services and Applications*, vol. 2, no. 2, pp. 81-94, 2011.

[5] S. Carlin and K. Curran, “Cloud computing security,” in *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*. Hershey, PA: Information Science Reference, 2013, pp. 12-17.

[6] G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,” *Computers & Security*, vol. 30, no. 5, pp. 320-331, 2011.

[7] W. Elsayed, T. Gaber, N. Zhang, and M. I. Moussa, “Access control models for pervasive environments: a survey,” in *The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015)*. Cham: Springer, 2016, pp. 511-522.

[8] Y. A. Younis, K. Kifayat, and M. Merabti, “An access control model for cloud computing,” *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 45-60, 2014.

[9] L. Zhou, V. Varadharajan, and M. Hitchens, “Achieving secure role-based access control on encrypted data in cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947-1960, 2013.

[10] D. Wei, F. Darie, and L. Shen, “Application layer security proxy for smart Grid substation automation systems,” in *Proceedings of 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, 2013, pp. 1-6.

[11] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, “Protecting smart grid automation systems against cyberattacks,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782-795, 2011.

[12] T. Zhu, W. Liu, and J. Song, “An efficient role based access control system for cloud computing,” in *Proceedings of 2011 IEEE 11th International Conference on Computer and Information Technology*, Pafos, Cyprus, 2011, pp. 97-102.

[13] E. E. Mon and T. T. Naing, “The privacy-aware access control system using attribute-and role-based access control in private cloud,” in *Proceedings of 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, Shenzhen, China, 2011, pp. 447-451.

[14] B. Wang, S. Zhang, and Z. Zhang, “DRBAC based access control method in substation automation system,” in *Proceedings of 2008 IEEE International Conference on Industrial Technology*, Chengdu, China, 2008, pp. 1-5.

[15] D. Rosic, U. Novak, and S. Vukmirovic, “Role-based access control model supporting regional division in smart grid system,” in *Proceedings of 2013 5th International Conference on Computational Intelligence, Communication Systems and Networks*, Madrid, Spain, 2013, pp. 197-201.

[16] D. E. Bell and L. J. La Padula, “Secure computer system: unified exposition and multics interpretation,” MITRE Corp Bedford, MA, Report No. MTR-2997-REV-1, 1976.

[17] E. J. Goh, H. Shacham, N. Modadugu, and D. Boneh, “SiRiUS: securing remote untrusted storage,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, 2003, pp. 131-145.

[18] 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 (TISSEC)*, vol. 9, no. 1, pp. 1-30, 2006.

[19] H. Shirvani and H. Vahdat-Nejad, “Storing shared documents that are customized by users in cloud computing,” *Computing*, vol. 98, no. 11, pp. 1137-1151, 2016.

[20] X. Lei, X. Liao, X. Ma, and L. Feng, “Securely and efficiently perform large matrix rank decomposition computation via cloud computing,” *Cluster Computing*, vol. 18, no. 2, pp. 989-997, 2015.

[21] M. Y. Shabir, A. Iqbal, Z. Mahmood, and A. Ghafoor, “Analysis of classical encryption techniques in cloud computing,” *Tsinghua Science and Technology*, vol. 21, no. 1, pp. 102-113, 2016.

[22] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhn, “A role-based access control model and reference implementation within a corporate intranet,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 2, no. 1, pp. 34-64, 1999.

[23] K. Hasebe, M. Mabuchi, and A. Matsushita, “Capability-based delegation model in RBAC,” in *Proceedings of the 15th ACM Symposium on Access Control Models and Technologies*, Pittsburgh, PA, 2010, pp. 109-118.

[24] V. C. Hu and K. A. Kent, *Guidelines for Access Control System Evaluation Metrics*. Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology, 2012.

[25] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, “Data security protection in cloud using encryption and authentication,” *Journal of Computational and Theoretical Nanoscience*, vol. 14, no. 4, pp. 1801-1804, 2017.

[26] A. D. Keromytis and J. M. Smith, “Requirements for scalable access control and security management architectures,” *ACM Transactions on Internet Technology (TOIT)*, vol. 7, no. 2, article no. 8, 2007.

[27] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, “Security transparency: the next frontier for security research in the cloud,” *Journal of Cloud Computing*, vol. 4, no. 1, article no. 12, 2015.

[28] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[29] X. Yi, R. Paulet, and E. Bertino, *Homomorphic Encryption and Applications*. Cham: Springer, 2014.

[30] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, “Proposed NIST standard for role-based access control,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224-274, 2001.

**Ghassan Sabeeh Mahmood** https://orcid.org/0000-0001-7099-7780

He received M.S. degree in School of Information Science and Engineering from Central South University, China in 2015. He is lecturer in University of Diyala. His current research interests include cloud computing and image watermarking.

**Dong Jun Huang** https://orcid.org/0000-0002-5474-8167

He is a professor in School of Information Science and Engineering, Central South University, China. His current research interests include image processing, communication and content analysis.

**Baidaa Abdulrahman Jaleel** https://orcid.org/0000-0001-9384-9078

She received B.S. degree in College of Science from University of Diyala University in 2007. She is a student in University of Diyala. Her current research interests include image processing and cloud computing.