International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

The Evolution of Access Control in Cloud Security: A Survey of Key Literature

K. Raja[1], Dr. K. Sujith[2]
[1]Research Scholar, Department of Computer Science, Annai College of Arts & Science (Affiliated to Bharathidasan University, Tiruchirappalli), Kovilacheri, Kumbakonam, Tamilnadu, India.
[2]Associate Professor, Department of Computer Science, Annai College of Arts & Science (Affiliated to Bharathidasan University, Tiruchirappalli), Kovilacheri, Kumbakonam, Tamilnadu, India.

Abstract
Cloud Computing is a distributed model that enables users to access, meet and exchange resources and resource requirements hosted by various service providers. Authentication of requesting users and the permitting of their rights of access are extremely necessary in order to avoid unauthorised or unlawful access to cloud services. In the cloud scenario, access control of distributed resources is most critical. Access control is a basic aspect of the security of information that is directly linked to the fundamental features of confidentiality, honesty and availability. This article provides a literature analysis of the Cloud Computing Access Control Mechanism.

Keywords: Cloud computing, Access Control, Security, Attribute based Access Control, Encryption, Decryption, time consumption.

1. INTRODUCTION

The sixth-generation service-based model is cloud computing [1]. This model has low cost of computing equipment, increased performance, quick updates, extended storing of data, high protection of data and simple adaptation. In other words, high resources can be reached immediately; resource use can be controlled at the appropriate level. In this case, when a high resource usage is required, immediate demand can be met [2]. It also has internal mechanisms which influence the service quality of the cloud services. Under-components including compliance managers, service managers, provision managers and access control managers perform numerous positions and responsibilities and perfect cloud operations. Each subsystem is responsible for its own area of responsibility and everybody has different ways of operating dynamically. Security remains a dangerous concern in cloud computing. You will still be affected by attacks on other cloud computing resources [3] even though your resources are not targeted. Exemplification from real life cloud computing; Office 365 is an MS Office cloud branded clutch cloud with the OpenStack Cloud, which offers traditional hardware cloud computing services.

Since cloud storage services are available, versatile and cost-effective in recovery [4], a great many businesses are encouraged to outsource their data to cloud storage servers. This minimises the need for the businesses to store their data on special facilities, ensuring that such information is secured against natural disasters, stealings or device crashes. Scalability is also one of the key advantages of the cloud. This helps the business to be extended to meet future requirements.

However, it is a crucial problem to store data in remote external servers and to delegate the cloud service provider a wide range of important tasks for the management and maintenance of these data without the data owners being involved. The data owners lose ownership of their data as data is outsourced to cloud servers. As cloud users do not trust the cloud service provider entirely and a large number of the stored data is highly sensitive, integrity and protection are essential questions in cloud computing.

Therefore, such cryptographic techniques need to be performed to fulfil two main features [5] to optimise the acceptance of the cloud storage service. The first is the protection that guarantees that the provider of cloud services does not know the customer details. The second feature is the honesty of the cloud customers' ability to detect any unauthorised alteration by the cloud service provider and attackers of their data.

In the Cloud, access control is the primary responsibility for the management of rights of access by cloud users that need access to cloud-specified data. One of the key methods used in the cloud environment to manage permitted access. It allows approved users to access and bans other users from accessing data[14]. Because of the distributed world of untrusted cloud servers, efficient mechanisms are needed to control access to encrypted data. Thus, researchers have characterised and identified several system models and algorithms for access control in order to provide stable and efficient cloud access control.

2. TYPES OF ACCESS CONTROL

Control of access is a technique which allows us to highlight a selected data / privileges restriction to approved

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

users. Identification, authentication and authorizations are the three main activities that form the model of access control (audit / verification against predefined policies / rules). A mechanism of access control enables subjects (users) to use their credentials to mark themselves as legitimate users and access services. The forms of access control available are the following:

- Role Based Access Control
- Attribute Based Access Control
- Fine Grained Access Control
- Hierarchical Attribute Based Access Control
- Attribute Based Encryption Fine Grained Access Control
- Discretionary Access Control
- Mandatory Access Control

3. LITERATURE REVIEW ON ACCESS CONTROL MECHANISM FOR CLOUD COMPUTING

Hu, Vincent C., et al [1] The paper includes the concept of attribute-based access control (ABAC) for federal agencies. ABAC is a logical access control system where authorisation to perform a set of operations shall be determined by evaluating attributes relating to the subject, entity, operations requested and, in some cases, conditions in the environment contrary to policies, rules or relationships describing permissible operations for a set of attributes.

Choi, Chang, Junho Choi, and Pankoo Kim [2] proposed Onto-ACM (on-ontology access management model) is a semantic theoretical model to resolve the disparity between service providers and consumers in allowable access controls. The model proposed is a smart context-conscious access model for the constructive implementation of resource access levels, based on ontological reasoning and the process of semantical analysis.

Chen, Hongsong, Bharat Bhargava, and Fu Zhongchuan [3] proposed a multi-label Access Control Model offering versatile protection for Big Data security. Our scalable access management model uses labels to ensure that a broad data application in the health sector receives scalable granularity protection.

Su, Jinshu, et al [4] described EPASS, a novel ABS method, which uses an attribute tree and exemplifies all AND, OR threshold gates under the Diffie-Hellman computational problem. Users are unable to forge signatures with attributes they don't have, and the signature ensures that the message will only be endorsed by a user who has adequate attributes which fulfil the policy.

Zheng, Qingji, Shouhuai Xu, and Giuseppe Ateniese [5] proposed a novel cryptographic solution, which is known as verifiable keyword search attribute-based (VABKS). The solution allows a data user, whose credentials fulfil the access control policy of a data owner, to (1) check the outsourced encrypted data of the data owner, (2) outsourcing the tedious search operations to a server, and (3).

Tian, Ye, et al [6] designed a fine-grained WBAN access control attribute-based encryption scheme. In our schema, a user can decrypt a ciphertext if the user access structure is fulfilled by the attributes of a ciphertext. If required, the users can be revoked. Patient protection and privacy should also be safeguarded.

Rajpoot, Qasim Mahmood, Christian Damsgaard Jensen, and Ram Krishnan [7] proposed A type of access control incorporating the two versions in a different way to unify the advantages. Our approach offers a comprehensive framework for access control that takes current contextual knowledge into account when making decisions on access control.

Yao, Xuanxia, Zhi Chen, and Ye Tian [8] In order to resolve security and privacy concerns in IoT, a lightweight, non-pairing ABE device based on elliptical curve (ECC) is proposed. Instead of a bilinear Diffie – Hellman assumption, the security of the proposed scheme is based on the ECDDH assumption and is seen in the selective set attribute model.

Da Silva, Roan Simões, and Sergio Donizetti Zorzo [9] presented a framework for access control that allows the user to set fine-grained access policy for NDN, a common ICN architecture. The data protection is assured by the use of an attribute-based encryption method that automatically repeals privileges.

Rouselakis, Yannis, and Brent Waters [10] proposed the powerful multi-copy, large-universe, policy-based encryption method for multi-copy authority. Any string can be used as attribute of the device in a large-universe ABE scheme, which are not usually specified during set-up. There is no central authority distributing the keys to the users in a multi-authority ABE structure.

Xhafa, Fatos, et al [11] developed a secure cloud-based EHR system, which guarantees protection and privacy of the cloud medical data stored in the cloud, depending upon the cryptographic primitive, but not the full confidence of cloud servers, to allow the efficient storage and sharing of PHRs and also eliminate patient privacy concerns.

Ngo, Canh, Yuri Demchenko, and Cees de Laat [12] analyzed Cloud providers provide use cases and provide multi-tenant cloud providers with access control models, and use an attribute-based access control model. The Intercloud models are also extended with the tokens exchange approach. We apply an efficient mechanism to turn complex logical expressions into compact policy decisions diagrams in order to promote an assessment of attributes and enforce the proposed model.

Zhang, Peng, et al [13] proposed the first user revocability and upgrade attribute control (CP-ABE) scheme. Specifically, in the identity-based sense, the revocation of users is decided and does not clash with our attributes. The cost of the attribute update is effective in that we only focus on updating the ciphertexts relevant to the modified attribute.

Zhang, Yinghui, et al [14] proposed the new technique known as match-then-re-encrypt, in which a matching step before re-encryption is additionally implemented. It uses special proxy re-encryption components and the cypher texts to secretly verify whether a proxy re-encryption can be done by the proxy.

Ren, Wei, et al [15] proposed a F2AC-based framework for the control of in-mobile cloud file storage is lightweight, fine-grained, and versatile. In addition to iterative permission, custom-tailored policy authentication and access control, F2AC can provide access privilege transfer and revoke for dynamically-changing access classes.

Hemdi, Marwah, and Ralph Deters [16] to give the system the ability to enforce policies for the detection of unauthorised entry, an attribute-based access control mechanism (ABAC) is implemented. A prototype was eventually produced to test the solution proposed.

Odelu, Vanga, et al [17] proposed Latest CP-ABE pairing scheme with the CSCTSK expressive AND gate access structure offering both constant-sized and secret key (CSCTSK) ciphertexts. We then demonstrate that in the Selective Protection Model the proposed CP-ABE-CSCTSK system is safe from the selected contestant text and provides a comparative description to illustrate the usefulness of the system.

Li, Fagen, Bo Liu, and Jiaojiao Hong [18] proposed a new control system for data access that can simultaneously achieve confidentiality and cloud authentication. Users store encrypted data in the cloud under this system. The data owner delegates the cloud to re-encrypt the information when a user wants to access the data, and the approved user alone can decrypt the data. The cloud does not receive any plaintext data.

Qiu, Meikang, et al [19] proposed approach is referred to as a Proactive Dynamic Protected Data Scheme (P2DS), designed to ensure the data are not open to unanticipated parties. The proposed framework has two main algorithms which are the Semantic Access Control (A-SAC) and the Determinative Access (PDA) algorithms for Attributes.

Wang, Hao, and Yujiao Song [20] used ABE and Identity-Based Encryption (IBE) for encrypting medical data and using ID (IBS) for introducing digital signatures. We are implementing a new primitive cryptography, known as Combined attribute / identity-based Encryption and Signature (C-AB / IB-ES) to incorporate various functions of ABE, IBE and IBS in one cryptosystem.

Seol, Kwangsoo, et al [21] proposed a cloud-based EHR model that uses an extensible markup language to carry out attribute-based access control. With a security focus, our EHR model partially encrypts and uses electronic signatures when a patient documents are submitted to a requester. We use digital signature technology for XML and XML encryption.

Zhong, Hong, et al [22] proposed a more realistic CP-ABE access control decentralised multi-authority regime in favour of user revocation. This scheme can also secure the privacy of data and privacy of access with cloud storage policies. In this case, the access policy introduced by the use of the linear secret sharing method.

Jiang, Yinhao, et al [23] introduced a new CP-ABE improvement system offering defence against this problem of the harassment of the main delegation. For such a property, we officially define the security requirements and then develop a CP-ABE system which fulfils the new safety requirements.

5. ISSUES AND CHALLENGES

Considering the problem of accessing distributed (personal) data, collected though multi-cloud infrastructures, the following main challenges could be highlighted:

- Continuous access
- Different regulations
- Dynamic access policies
- User-friendly management
- Continuous control
- Scalability
- Resource sharing and interoperability
- Validation and verification of access control policies
- On line tracing of access control polices execution
- Testing of access control systems

5. CONCLUSION

Access control remains a continuous task since it is one of the earliest computer security issues. The Access Control aspect specifies whether requests are granted for access to resources. The requesting entity is commonly referred to as a subject, normally a programme or a process that operates on behalf of a user. A user is a machine communicating object and accessing services. The large-size use of the classical models in several different areas will prevent users from implementing Attribute-based Access Control (ABAC), an ABAC model that cannot configure these models. This ABAC system can simulate classical models with sufficient specifications.

REFERENCE

[1] Pandey, S., Dwivedi, A., Pant, J., and Lohani, M. (2016). Security enforcement using TRBAC in cloud computing. In International Conference on Computing, Communication and Automation (ICCCA), 2016 (pp. 1232–1238).

[2] Chatterjee, S., Gupta, A. K., Mahor, V. K., and Sarmah, T. (2014). An efficient fine-grained access control scheme based on attributes for enterprise class applications. In International Conference on Signal Propagation and Computer Technology (ICSPCT), 2014 (pp. 273–278).

[3] Charanya, R., and Aramudhan, M. (2016). Survey on access control issues in cloud computing. In International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), (pp. 13–4). IEEE.

[4] Sirisha, A., and Kumari, G. G. (2010). API access control in cloud using the role-based access control model. In Trendz in Information Sciences & Computing (TISC), 2010 (pp. 1353–137).

[5] Zhou, L., Varadharajan, V., and Hitchens, M. (2013). Achieving secure role-based access control on encrypted data in cloud storage. IEEE transactions on information forensics and security, 8(12), 1947–1960.

[6] Strembeck, M., and Mendling, J. (2011). Modeling process-related RBAC models with extended UML activity models. Information and Software Technology, 53(5), 456 483.

[7] Chen, S. T., Xu, J. F., Hang, Y. X., and Li, J. W. (2016). Role-based access control for memory security on Network-on-Chips. In 13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT), 2016 (pp. 1422–1424). IEEE.

[8] Yaira K Rivera S´anchez, Steven A Demurjian, and Mohammed S Baihan. Achieving rbac on restful apis for mobile apps using fhir.

[9] Gunti, N., Sun, W., and Niamat, M. (2011). I-rbac: Isolation enabled role-based access control. In Ninth Annual International Conference on Privacy, Security and Trust (PST), 2011 (pp. 79–86).

[10] Chen, H. C., andVioletta, M.A. (2013).Acognitive RBAC model with handover functions in small heterogeneous networks. Mathematical and Computer Modelling, 58(5-6), 1267–1288.

[11] Saenko, I., and Kotenko, I. (2017). Administrating role-based access control by genetic algorithms. In Proceedings of the Genetic and Evolutionary Computation Conference Companion (pp. 1463–1470).

[12] Sergeev, A., and Matulevicius, R. (2017). An Approach to Capture Role-Based Access Control Models from Spring Web Applications. In Enterprise Distributed Object Computing Conference (EDOC), 2017 IEEE 21st International (pp. 159– 164).

[13] YAN, D. F., Yuan, T. I. A. N., HUANG, J. L., and YANG, F. C. (2013). Privacy-aware RBAC model for web services composition. The Journal of China Universities of Posts and Telecommunications, 20, 30–34.

[14] Chuanfan, L. (2010). Research on role-based access control policy of e- government. In International Conference on E-Business and EGovernment (ICEE), 2010 (pp. 714–716). IEEE.

[15] Kwon, J., and Moon, C. J. (2007). Visual modeling and formal specification of constraints of RBAC using semantic web technology. Knowledge-Based Systems, 20(4), 350–356.

[16] Rui-Feng Zhu, Jie Ning, and Pei Yu (2012). Application of role-based access control in information system. In International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP), (pp. 426–428). IEEE.

[17] Habib, M. A., Ahmad, M., Mahmood, N., and Ashraf, R. (2017). An evaluation of role-based access control towards easier management compared to tight security. In Proceedings of the International Conference on Future Networks and Distributed Systems, p. 44. ACM.

[18] Jin, P., and Fang-Chun, Y. (2006). Description logic modelling of temporal attribute-based access control. In First International Conference on Communications and Electronics, 2006. ICCE'06. (pp. 414–418).

[19] Pussewalage, H. S. G., and Oleshchuk, V. A. (2016).An attribute based access control scheme for secure sharing of electronic health records. In IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), (pp. 1–6).

[20] Shen, H. B., and Hong, F. (2006). An attribute-based access control model for web services. In Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. (pp. 74–79).1] Hirra Anwar and Muhammad Awais Shibli (2012). Attribute based access control in dspace. In 7th International Conference on Computing and Convergence Technology (ICCCT), pp. 571–576. IEEE.

[22] Sabbari, M., andAlipour,H. S. (2011). Improving attribute-based access control model for web services. In Information and Communication Technologies (WICT), 2011World Congress on (pp. 1223–1228). IEEE.

[23] Dan, N., Hua-Ji, S., Yuan, C., and Jia-Hu, G. (2012). Attribute based access control (ABAC)-based cross-domain access control in service-oriented architecture (SOA). In International Conference on Computer Science & Service System (CSSS), (pp. 1405–1408).