I. J. Education and Management Engineering, **2023, 3, 39-46**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2023.03.05

Exploratory Analysis of Access Control Mechanisms for Cloud-Based IoT

Keerti Naregal*
Research Scholar, Jain college of engineering, Computer Science, Belagavi 590014, India
E-mail: keertinaregal@gmail.com
ORCID iD: https://orcid.org/0000-0002-3072-3803
*Corresponding Author

Vijay Kalmani
Research Supervisor, Jain college of engineering, Computer Science, Belagavi 590014, India
E-mail: vijaykalmani@hotmail.com
ORCID iD: https://orcid.org/0000-0003-0738-3211

Received: 23 December, 2022; Revised: 21 January, 2023; Accepted: 06 March, 2023; Published: 08 June, 2023

Abstract: Computing as a utility has been possible with cloud computing technology. Another technology that has evolved with the internet and has become an inseparable part of our lives is the internet of things (IoT). With the growing use of IoT devices, the data generated and used by them is increasing tremendously, and resource-constrained IoT devices can make use of the cloud for data and computing needs. When IoT and cloud converge there are security and privacy issues as the cloud is a shared resource. Access control mechanisms play an important role in maintaining the security of users' data. Attribute-based encryption provides fine-grained access to data, thus ensuring selective access to data. We review the literature on access control mechanisms for cloud-based IoT and provide an analysis of their strengths and weaknesses. We present a comparison of the mechanisms, highlighting the challenges and open research questions in the field of cloud-based IoT access control and provide suggestions for future research and development. Our findings contribute to the understanding of access control mechanisms for cloud-based IoT and provide insights for their selection and deployment in real-world scenarios.

Index Terms: Cloud based-IoT, Attribute-based Encryption, lightweight, access control mechanism, privacy

1. Introduction

This paper explores and analyses the access control mechanisms for cloud-based IoT, we have come across review articles for access control in IoT [1,2] or for the cloud alone. This paper for the first time performs the study of access control mechanisms for cloud-based IoT and identifies the suitable security mechanisms for the cloud-based IoT environment, the possible issues, and the open challenges. This paper provides a comprehensive survey and comparative analysis of access control mechanisms for cloud-based IoT. The survey covers the most widely used and established access control mechanisms, including role-based access control (RBAC), attribute-based access control (ABAC), discretionary access control (DAC), and mandatory access control (MAC). The study aims to evaluate the strengths and limitations of each mechanism and provide insights into their performance in the context of cloud-based IoT. The paper also proposes a comparative analysis framework and metrics to facilitate the evaluation of the access control mechanisms. The outcomes of the study can help decision-makers and practitioners in choosing the most appropriate access control mechanism for their specific IoT applications, based on their security requirements and resource constraints. The contents of the paper are put up as follows, in section 2 basic concepts of the cloud, IoT, and cloud-based IoT are discussed, section 3 reviews the classical access control mechanisms, in section 4 we discuss the Attribute-based encryption, in section 5 we discuss the methodology, in section 6 we analyze the ABE mechanisms for cloud-based IoT and in section 7 we discuss results.

2. Cloud, IoT, and Cloud-based IoT

This section provides the basics of cloud computing, IoT (Internet of Things), and cloud-based IoT.

2.1. *Cloud*

Cloud computing provides services on demand, the services range from resources like memory, servers, software applications, and so on. Cloud computing provides computing as a utility [3]. With the usage of cloud services, the initial cost of establishment is saved and the ‘pay as per use’ feature, helps users and businesses. The cost and time for establishment are greatly reduced with the use of cloud computing services. Maintenance of hardware and software infrastructure requires trained professionals, maintaining regular backups, and timely servicing is a must. With the use of the cloud, everything is taken care of by the cloud service providers and it is not a headache for the users. Scaling of resources is possible and easily done with cloud computing. Thus, cloud-based systems ensure the provision of scalability, flexibility, availability, sustainability, and cost-effectiveness.[5]

The commonly agreed cloud computing classification has 3 major services defined, namely SaaS, or Software as a Service; PaaS, Platform as a Service; and IaaS, Infrastructure as a Service.[4]

Software as a Service: With this cloud service users can run software applications on the cloud. The applications can be accessed by the users via a web interface. Data and network security, where exactly the data is placed (its locality), the web interface used, and data integrity are some of the security issues that can arise with SaaS. Most importantly providing restricted access to the applications needs to be focused on.

Platform as a Service: This cloud service enables users to develop and deploy applications by providing a suitable platform. Unlike a traditional standalone system used for application development, where access to the system is defined by the user and data is stored locally, PaaS stores data on the cloud and could be owned by a third party. Users are dependent on the security features employed by the cloud service provider. Network intrusion and security breaches are a major threat in PaaS and suitable encryption and authorization methods need to be used.

Infrastructure as a Service: This cloud service provides users with different resources like storage, virtual machines, etc. using which users can develop and host applications. The user has control over the operating system and the resources used. Security of the virtual machines is a major botheration here.[5]

Four deployment models are specified for the cloud:

Public cloud: As the name suggests the cloud services are available to the public, they can use the services through a suitable web interface. Usually, large companies or a group of companies are public cloud owners and service providers. It is the most commonly used deployment model with features of scalability, reliability, etc. Security issues are an important concern in this model.

Private cloud: Cloud services are provided for a private organization. The cloud may be owned by the organization itself or by a third party. Its working is similar to the intranet; security features are greatly enhanced as access is restricted to the organization. These features of course come at an enhanced cost.

Community cloud: A community is formed by multiple organizations that have commonalities over say security policy, compliance, etc. Like the private cloud, the organizations could own the cloud or maybe outsourced to a third party.

Hybrid cloud: It is formed by a mix of public, private, or community clouds, though they remain separate entities, the combination in conjunction enables data movement. For example, data processed on a community cloud could be moved to a private cloud for storage. Cloud bursting moving data to another cloud when resources run short is another example. [7]

2.2. *IoT*

We have come across the term internet of things (IoT) very often in our day-to-day life. In IoT, embedded systems are connected with sensors to sense various events, this data is shared across the network infrastructure using the internet. In the last twenty years, we have seen a highly increasing use of mobile phones and their applications. With advancements in IoT, soon we may find things like clothes, household items like a refrigerator, TV, etc. talking to each other on the internet, and it is already partly started. We can find data transfer through things like smart glasses, smart watches, etc. Data can also be transferred by devices located in nomadic environments. The evolution of IoT with the internet is explained in Fig.1.[9]

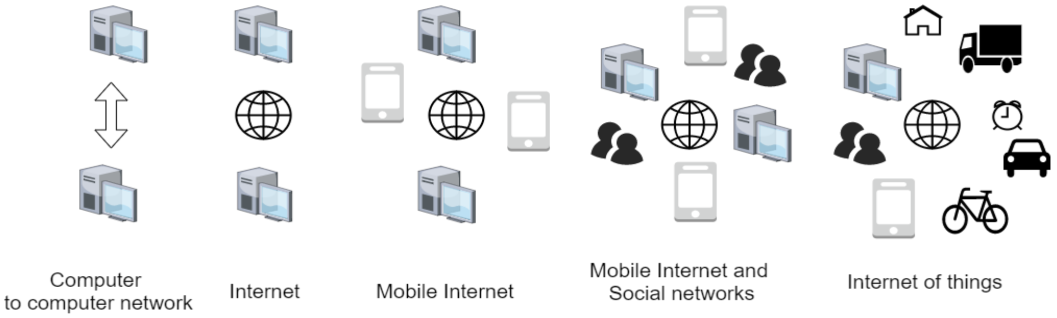

Fig. 1. Evolution of IoT.

Different architectures are defined for IoT, one is 3 layered another is 5 layered, and so on. Efforts are being made by different organizations to standardize the protocols used for IoT. Some of the organizations working for standardization are the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE),3rd Generation Partnership Project (3GPP). [10] Various categories of IoT applications are identified, some of them are listed below [1]:

Smart home: In a smart home application various objects like TV, refrigerator, music system, doorbell, and lights are all smart and are monitored by the owner of the house. Thus, there is machine-to-machine and human-to-machine interaction.

Healthcare: In this application patients are monitored by various devices like BP, Sugar level, heart rate, etc. monitors and suitable actions are taken. Also, health-supporting devices like pacemakers and insulin pumps could be used.

Smart Buildings: Lightning, heating, air conditioning, fire alarm, such tasks are automated and controlled using applications.

Connected Vehicles: Vehicles share information such as speed, location, etc with other vehicles, helping in traffic management.

Similarly, Smart Energy, Smart City, Smart agriculture, Industrial internet, and many other IoT applications are defined.[8]

2.3. Cloud-based IoT

With each passing day the number of IoT devices is increasing, and so is the variety of applications they are used for. As we get accustomed to devices, it is difficult to imagine life without these smart objects. An important point to be noted and of concern is that IoT devices are resource-constrained devices. Most of them have limited power as they are usually battery-operated for portability or the nomadic environments, they are placed in. The memory used for data storage is also limited. When we consider IoT applications like Healthcare, Smart homes, etc., the data generated or in transit in these applications is increasing and with limited storage resources, it is difficult to cater to the needs of the applications. Cloud on the other hand is resource-rich and has huge storage capacity and the capability to manage the huge data generated by IoT devices.[11]

Also, the cloud has sufficient computing resources for data processing. So IoT devices can use the cloud for data storage or processing. The term cloud-based IoT is used when cloud and IoT converge. Fig.2. shows an example of cloud-based IoT architecture.[12] With growing IoT applications and devices, cloud usage with IoT is going to be the norm.

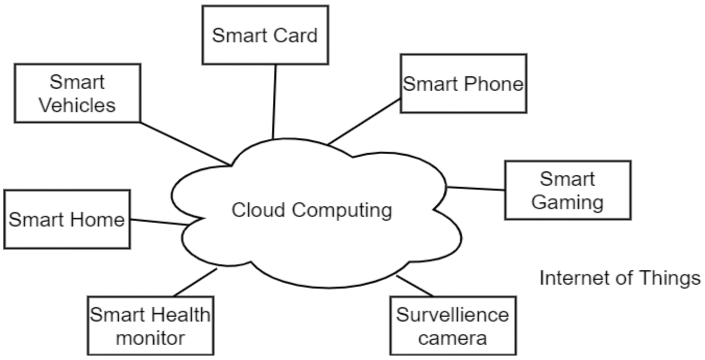

Fig. 2. Cloud-based IoT architecture.

When cloud and IoT converge, the data of the users are at risk. Suitable security mechanisms are to be used to ensure the privacy of the users. Concerning this, we discuss the access control mechanisms.

3. Review of Access Control Mechanisms

Whenever data or any digital resource is shared among entities, access control becomes a necessity. With data being shared on the cloud by IoT devices, access control becomes very important. Access control mechanisms can be effectively provided if they satisfy the security requirements of confidentiality, integrity, and availability (CIA)

Three functions covered as part of access control are [13]:

Authentication: It is the process of verifying if the user is authentic. Passwords, pins, and biometrics are the different ways of verifying the user’s identity.

Authorization: Deciding on whether to grant or deny permission for a specific object is done through authorization. Access control policies have to be defined and suitable mechanisms have to be used to apply them.

Accountability: It involves maintaining a log of actions performed by the user to help in auditing later.

A range of access control models and mechanisms have been developed in the literature to secure cloud-based IoT systems.

DAC- Discretionary access control: In this method of access control, the owner of the resources has complete control of the resources and decides who has what access to the resources. In this model, an access matrix is used to find the access permissions of the users. The sample access matrix is shown in Table 1. below

The object owner may define groups of users and define the access permission for the group instead of allotting permissions to individual users. The main problem with the DAC model is that there is a lack of control over copying. Information may be copied from one object to another and may lead to unauthorized access by using the copy.

Table 1. Access Matrix

	Object1	Object2
User1	Read	Execute
User2	Read/Write	

MAC- Mandatory access control: In this model unlike DAC, a system administrator assigns access permissions to all the users of the system. Data owners do not have control, instead, everything is taken care of by the system administrator. All the security policies are defined by the administrator and they are enforced by the operating system. This model is simple as it uses a single authority and at the same time highly secure as information flow among users

The main issue with MAC is that it does not provide fine-grained access control. The pricing of the MAC systems is also high as they use trusted components. Scalability is a problem in MAC as it is centrally managed.

RBAC- Role-based access control: In this model users in an organization are given access permission defined by their roles. The roles are based on the duties assigned to the employees. So, access to resources is based on the roles and not on people. When an employee working in an organization changes his department or his designation changes, his role and access permission also change accordingly. The main difference between DAC and RBAC is unlike DAC here users have no control over the access permissions and they cannot pass the permission to other users like in DAC. RBAC provides a great deal of flexibility. If a new employee joins an organization, based on his nature of work, his role is defined and his access rights are defined by the system administrator. When his job changes or the nature of his work changes, he is assigned a new role. In the hierarchical RBAC, there is a parent role which can include its descendant roles [14], for example, the role of doctors in an electronic health record (EHR) system can include physicians, pediatricians, surgeons, urologists, gynecologists, and so on. We can find multiple implementations of the RBAC model for different applications.

There are many advantages of using the RBAC model some of them are:

Implementation is simple: Defining different roles for an organization is a one-time task and requires initial research and understanding. Once the roles are defined, moving the user from one role to another is not difficult. If a user leaves an organization his role gets disassociated, and even if his account is active, his access permissions are lost.

Provides Scalability: RBAC allows scalability, new roles can be added and corresponding users can also be updated.

Hierarchy supported: RBAC supports hierarchical roles which enable association between roles and results in enhanced functionality concerning the end user.

There are a few disadvantages as well associated with the RBAC model:

The RBAC does not provide fine-grained access control, in large organizations management of RBAC becomes difficult, the model is static i.e., it does not support the use of user location, time, etc to restrict access to resources, and an administrator is likely to create permission errors, especially during role changes or an employee quitting an organization.

ABAC-Attribute-based access control: In this model, the user is provided access to the resource by verifying the attributes associated with the user and the attributes of the resource. Access policies are defined that are based on attributes, such as location, time, user id, etc. In ABAC each user is associated with attributes that are the characteristics of the user like the project they are associated with, their role, department, etc. ABAC has several advantages, access policies are defined and updated dynamically. There is flexibility in the updating of policies. Using the larger set of attributes and defining corresponding policies, fine-grained access control is possible. Unlike RBAC system administrator is not the only person responsible and in charge of the whole system.

Though ABAC has several advantages, there are shortcomings as well, authorization requirements are gathered and implemented as policies. In ABAC the ownership of authorization is distributed across IT teams, analysts, etc, and is complex. It is difficult to determine who has access to a specific resource in ABAC, hence auditing becomes difficult. Separation of duties is also not possible whereas in RBAC it can be done by the admin easily.

Access control in cloud-based IoT environments requires an understanding of the characteristics and requirements of IoT devices and services. For example, some IoT devices may have limited processing power, memory, and energy resources, which require lightweight access control mechanisms. Additionally, some IoT services may require real-time access control decisions, which require fast and efficient access control mechanisms.

4. Attribute-based Encryption

Data is stored on the cloud by a third party and the security of the data is at stake. Many IoT applications also store data in the cloud and the privacy of such data is important. To protect the data, it can be stored in an encrypted form, but when the data stored is huge, and access to a small subset of the large data is needed, decryption of the whole data might be difficult and unnecessary. As a solution to this problem, Sahai Waters [15] proposed attribute-based encryption (ABE), a public key encryption technique that uses attributes of users for encryption and decryption.

The basic ABE model is shown in Fig.3.

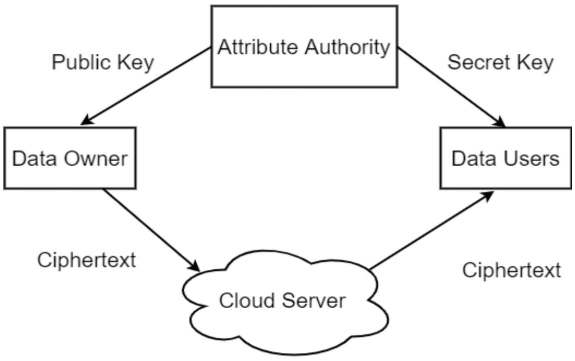

Fig. 3. Basic Attribute-Based Encryption.

Three entities are involved in attribute-based encryption namely attribute authority, the data owner, and the data user. The authority is responsible for generating the public key and the master secret key. Based on the attributes, the user's secret key is generated. The data owner encrypts the data using the public key and stores it on the cloud. The data user makes use of the private key distributed by the authority and performs decryption. Decryption is possible only if the requisite number of attributes match the attributes in the secret key. Different ABE schemes have been proposed. In Key policy attribute-based encryption (KPABE), the ciphertext is generated with the attribute set selected by the encryptor and the private key for the users is generated based on an access structure. Decryption is possible when the user attributes match the access structure. In another variation called ciphertext-policy attribute-based encryption (CPABE), unlike KPABE, the ciphertext is generated with the access structure or the policy, and the user's key is generated based on the attributes.[16]

KPABE and CPABE form the basic types of ABE. We have many other ABE variants like multiauthority ABE, based on access structure monotonic and non-monotonic, attribute authority may be hierarchical called Hierarchical ABE, and so on. All of them follow either KPABE or CPABE though.

5. Methodology

Our work involves a search of the literature on access control mechanisms for cloud-based IoT applications. We searched using several academic databases, including Google scholar, IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink. We also searched for relevant conference proceedings and journals, as well as conducted a manual search of reference lists from relevant articles.

The search was conducted using a combination of keywords and phrases related to access control, cloud computing, and IoT. The keywords and phrases used included “access control mechanism,” “access control model,” “role-based access control,” “attribute-based access control,” “cloud computing,” “Internet of Things,” “cloud-based IoT” and “IoT security.” We then applied inclusion and exclusion criteria to the articles retrieved from the search. Suitable articles were selected, reviewed, and analyzed.

6. Importance of ABE for cloud-based IoT and analysis of the ABE mechanisms for cloud-based IoT

When we consider cloud-based IoT, data from the IoT devices are moved to the cloud for storage. Attribute-based encryption proves to be a promising access control mechanism for such data as it provides encryption, which protects the data from privacy, and access control ensures that only requisite data is made available to each user. Table 2. compares the different ABE schemes used for cloud-based IoT.

Table 2. Variant Dependencies

Cloud-based IoT ABE scheme	Data Confidentiality	Fine-grained access control	Attribute Authority	Key features
PU-ABE [17]	✔	✔	Single	Based on KP-ABE, uses constant-size ciphertext
Multiauthority ABE [18]	✔	✔	Multiauthority	Based on CP-ABE, uses constant size key and ciphertext thus giving high scalability
BaDS [19]	✔	✔	Blockchain-based	Uses blockchain-based architecture, attribute-based signature with CP-ABE used
C-KPABE [20]	✔	✔	Single	Collaborative KPABE uses delegation of encryption to cloud servers and trusted nodes, thus helping resource-constrained IoT devices
Anonymous decentralized ABE [21]	✔	✔	Multiauthority	Decentralized multiauthority ABE, outsourced decryption
SEM-ACSIT [22]	✔	✔	Multiauthority	The attribute authority management (AAM) module is used for the storage of keys of users and attribute authorities

It is observed that single attribute authority is suitable and sufficient when the users for the application are limited and manageable by one authority, as the number of devices or users increases and the data increase multiple attribute authority is used. The blockchain method provides a decentralized way of working with attributes. Attribute revocation is another problem that needs to be looked into [23] and suitable solutions are decided considering the application in mind. As we can see there is no single method that proves to be the best for all IoT devices or applications. Depending on the application's needs, a suitable ABE method can be chosen. Research is going on and different methods of ABE for cloud-based IoT are being proposed.

7. Discussion of the Results

Based on the analysis and comparison of the access control mechanisms, we identified some general trends and patterns that can be used to guide the selection of the most appropriate mechanism for a given cloud-based IoT application.

First, RBAC and ABAC are the most commonly used access control mechanisms in cloud-based IoT applications, with RBAC being more prevalent in the literature. This may be due to the simplicity and ease of implementation of these mechanisms, as well as their ability to support different levels of access control.

Second, the choice of access control mechanism depends on the specific requirements and characteristics of the cloud-based IoT application. For example, RBAC may be more suitable for applications that have a relatively simple access control structure, while ABAC may be more suitable for applications that require fine-grained control over access to resources.

Third, the evaluation criteria used in the survey are important factors that should be considered when selecting an access control mechanism. However, they are not the only factors that should be considered, and other factors such as scalability, usability, and compatibility with existing systems should also be taken into account.

Finally, the limitations and strengths of the different access control mechanisms should be carefully evaluated before selecting a mechanism for a given cloud-based IoT application. This evaluation should take into account the specific security requirements and characteristics of the application, as well as the limitations and strengths of the available mechanisms.

In conclusion, the results of the survey provide valuable insights into the strengths and limitations of different access control mechanisms for cloud-based IoT applications. These insights can be used to guide the selection of the most appropriate mechanism for a given application and can inform the development of new access control mechanisms that address the limitations of the existing mechanisms.

8. Conclusions

In this paper, we presented a survey of access control mechanisms for cloud-based IoT applications. We identified and discussed the evaluation criteria for access control mechanisms and evaluated popular access control mechanisms using these criteria. Our evaluation showed that each mechanism has strengths and weaknesses, and the choice of mechanism will depend on the specific requirements of the application. Attribute-based encryption is a suitable mechanism for providing fine-grained access control for IoT devices using the cloud for storage. As IoT devices are resource constrained, designing a lightweight mechanism is important and equally challenging. Based on the application needs, an appropriate mechanism with single or multiple attribute authority can be chosen. CPABE is preferred in many cases as the data owner can decide the access rights. Our future work focuses on providing a lightweight attribute-based encryption mechanism for cloud-based IoT for healthcare applications.

We hope that this survey will provide useful insights for researchers and practitioners working in the area of access control for cloud-based IoT applications. In the future, we plan to extend this work to include a more detailed evaluation of the mechanisms in the context of specific IoT use cases.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Access Control in Internet-of-Things: A Survey(Sowmya Ravidasa,∗ , AlexiosLekidisa , Federica Pacib , Nicola Zannonea)

[2] Namasudra, S., & Roy, P. (2016). Secure and efficient data access control in cloud computing environment: A survey. Multiagent and Grid Systems, 12(2), 69-90.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski et al., A view of cloud computing, Commun of the ACM 53(4) (2010), 50–58

[4] L. Savu, "Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges," 2011 International Conference on Computer and Management (CAMAN), 2011, pp. 1-4, DOI: 10.1109/CAMAN.2011.5778816.

[5] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J NetwComput Appl. 2011;34(1):1-11.

[6] Dimitrios Zissis, Dimitrios Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, Volume 28, Issue 3,2012,Pages 583-592,ISSN 0167-739X,https://doi.org/10.1016/j.future.2010.12.006

[7] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.

[8] Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT security. IoT security: advances in authentication, 27-64.

[9] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. IEEE communications surveys & tutorials, 16(1), 414-454.

[10] Liyanage, M., Braeken, A., Kumar, P., & Ylianttila, M. (Eds.). (2020). IoT security: Advances in authentication. John Wiley & Sons.

[11] Babu, S. M., Lakshmi, A. J., & Rao, B. T. (2015, April). A study on cloud-based Internet of Things: CloudIoT. In 2015 global conference on communication technologies (GCCT) (pp. 60-65). IEEE.

[12] Naregal, K., &Kalmani, V. H. (2022). Need for Lightweight Attribute-Based Encryption (ABE) for Cloud-Based IoT. In Handbook of Research of Internet of Things and Cyber-Physical Systems (pp. 265-278). Apple Academic Press.

[13] Suhendra, V. (2011, December). A survey on access control deployment. In International conference on security technology (pp. 11-20). Springer, Berlin, Heidelberg.

[14] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), 4(3), 224-274.

[15] Sahai, A., & Waters, B. (2005). Advances in Cryptology-EUROCRYPT 2005. Lect Notes in Comput Sci, 3494, 457-473.

[16] Kumar, P., & Alphonse, P. J. A. (2018). Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. Journal of Network and Computer Applications, 108, 37-52.

[17] Belguith, S., Kaaniche, N., & Russello, G. (2018, July). PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 924-927). IEEE.

[18] Banerjee, S., Roy, S., Odelu, V., Das, A. K., Chattopadhyay, S., Rodrigues, J. J., & Park, Y. (2020). Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment. Journal of Information Security and Applications, 53, 102503.

[19] Zhang, Y., He, D., & Choo, K. K. R. (2018). BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. Wireless Communications and Mobile Computing, 2018.

[20] Touati, L., &Challal, Y. (2016, May). Collaborative kp-abe for cloud-based internet of things applications. In 2016 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE.

[21] Nasiraee, H., &Ashouri-Talouki, M. (2020). Anonymous decentralized attribute-based access control for cloud-assisted IoT. Future Generation Computer Systems, 110, 45-56.

[22] Xiong, S., Ni, Q., Wang, L., & Wang, Q. (2020). SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage. IEEE Internet of Things Journal, 7(4), 2914-2927.

[23] Kalmani, V. H., Goyal, D., & Singla, S. An Efficient and Secure Solution for Attribute Revocation Problem Utilizing CP-ABE Scheme in Mobile Cloud Computing. International Journal of Computer Applications, 975, 8887.

Authors' Profiles

Keerti Naregal is working as Assistant Professor, in the Department of Computer Science and Engineering at Graphic Era University, Dehradun, India. She received her M.Tech. and B.E. degrees from Visvesvaraya Technological University in 2012 and 2006. She has thirteen years of Academic and Teaching experience and three years of industry experience. Currently, she is pursuing research in the area of cloud security and is a research scholar at Jain College of Engineering, Belagavi.

Vijay Kalmani is a Research Supervisor at the Jain College of Engineering, Belagavi, affiliated with Visvesvaraya Technological University, Belagavi, India. He received his Ph.D. in Computer Science & Engineering from Suresh Gyan University, Jaipur, India. His research interests include cloud computing, network, and information security, AI & ML, etc. He is the author of many research studies published in national and international journals as well as conference proceedings.

How to cite this paper: Keerti Naregal, Vijay Kalmani, "Exploratory Analysis of Access Control Mechanisms for Cloud-Based IoT", International Journal of Education and Management Engineering (IJEME), Vol.13, No.3, pp. 39-46, 2023. DOI:10.5815/ijeme.2023.03.05