An Improved System for Risk Based Access Control in Cloud Environment

Prateek Bhatia , J.K.Maitra
Rani Durgawati University, Jabalpur ,MP, India
prateek.bhatia2110@gmail.com , jkmrdvv@rediffmail.com , Affiliation

Abstract— Over the past decade, businesses have been increasingly migrating their computer infrastructure with improved cost-efficiency, flexibility and resource use in cloud environments. However, this shift has posed a critical security challenge, especially in data access control. Ensuring sensitive data in a cloud environment remains a critical issue for researchers and industry experts. B. b. Traditional access control models such as discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), task-based access control (TBAC), and attribute-based access control (ABAC) provide a structured mechanism for managing user authentication. However, these models often lack the flexibility needed to tackle the dynamic and complex safety threats of cloud systems. To address this limitation, risk-based access control (risk control) has proven to be an effective solution for security environments at several levels. In this article, we propose advanced risk-based access control methods that increase the security of your cloud environment by evaluating a variety of risk parameters in real time. By including dynamic risk assessment techniques, this approach improves access control guidelines decision-making, reduces the likelihood of unauthorized access, and at the same time reduces operational efficiency. The proposed model contributes to enhanced cloud security by adapting access control mechanisms to the development of threats and organizational requirements.

Keywords— Cloud Security, Access control methods, MAC, DAC, ABAC, RBAC, Risk based access control

I. INTRODUCTION

Cloud computing is a new technology, and its growth is on the rise, spread by a variety of IT conglomerates such as Google, IBM, and Salesforce.com. It combines many technologies such as utility computing, grid computing, and virtualization. Cloud computing uses the benefits of these technologies and offers many advantages, including low investment costs, large memory, faster calculations, virtualization, and more. Cloud service providers use the Multimieto model [24], allowing multiple users to access outsourced data. Therefore, there is a high threat to the security of outsourced data in the cloud. Furthermore, cloud service providers and databases are most likely in a variety of areas.

The purpose of access control is to make access accessible and accessable, and to make information resources accessible as part of the legal realm [20]. Essentially, the access control model has three components: subject, object, and access control guidelines. Subjects are active units creating access requirements and therefore the initiator of the access action. An object is a passive unit that receives access to other companies, and therefore the recipient of an access campaign. Access control guidelines are a set of access rules for objects in an object. Figure 1 illustrates the key factors and decision-making process through access control [12] [8] [17].

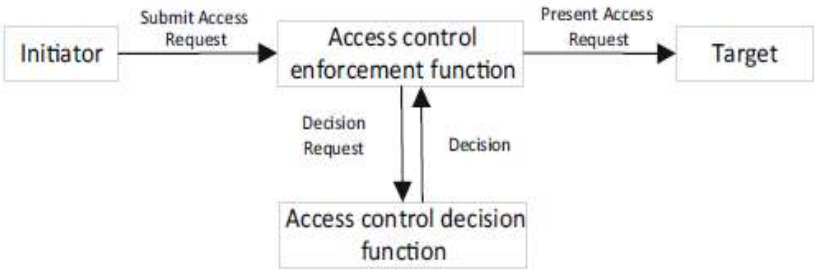

Fig. 1: Process of access control mechanism.[12]

A detailed analysis was performed to determine the basic requirements for access control in cloud computing [2]. They specify dynamic performance and mobility features [15], authentication [22], trust [15], scalability [4], heterogeneity [16], quality of service [11], interoperability [23], attribute management [13], virtualization and sharing of physical

resources [18], ease of allocation and privilege [9], reduction of potential [9], and identifying security taxonomy for cloud services in various fields in Figure 2. The typical organizational security framework provided by IBM indicates that organizational security guidelines should manage one of the key security management and access management for identity and access [29]. Identity and Access Management must ensure that only valid users have access to company data that may be related to the application. Users who access the cloud can have a variety of roles, such as developers, administrators, IT managers, and more quality. Beach [25] presents a governance model based on role-based guidelines (role-based access control) that allows for dynamic changes to the access rights assigned to subjects within the system based on data objects based on activity and responsibility within the virtual enterprise.

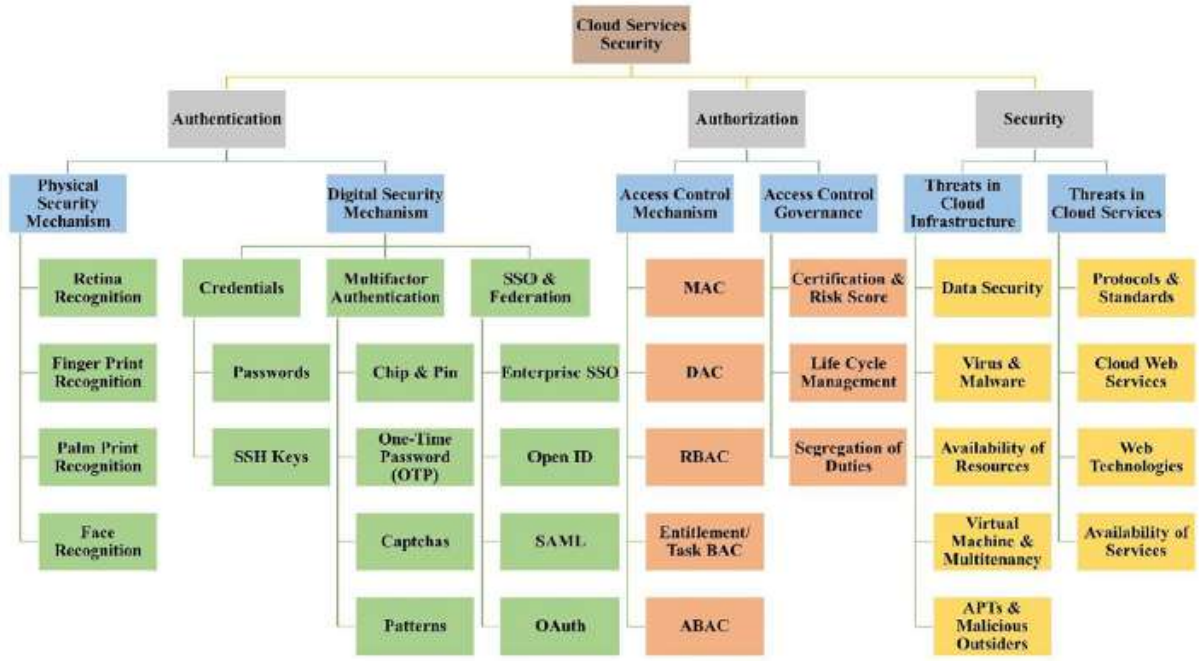

Figure 2: Taxonomy of cloud services security [21]

II. RELATED WORK IN THE FIELD OF ACCESS CONTROL METHODS

Access control is a crucial aspect of cloud computing security, ensuring that only authorized users can access specific resources and data. Over the years, researchers have developed various models to address security concerns in cloud environments. Traditional methods such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Task-Based Access Control (TBAC), and Attribute-Based Access Control (ABAC) have been widely studied and implemented. However, these models often struggle to adapt to the dynamic nature of cloud computing, leading to the development of more advanced techniques such as Risk-Based Access Control (RISK-BAC) and blockchain-based mechanisms.

Several recent studies have explored access control mechanisms in cloud environments. A review by SN Computer Science (2021)[31] examines data access control in mobile cloud computing, emphasizing the limitations of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) due to its high computational costs. Similarly, research published in Mobile Networks and Applications (2021)[32] proposes a secure access control framework that integrates cryptographic techniques with Role-Based Access Control to mitigate privilege abuse and token hijacking[33].

. Advances in Computational Intelligence and Informatics[34] presents an extensive survey on various Attribute-Based Encryption (ABE) schemes, assessing their efficiency and security in cloud-based data access control (Springer). Another study in Internet and Distributed Computing Systems [35] highlights the inefficiencies of traditional models like MAC and RBAC and introduces a new Combinatorial Batch Codes-

Based Access Control (CBCBAC) model that enables secure resource sharing among non-trusted cloud tenants [36].

Guidelines and recommendations for access control have also been explored in policy-driven research. The NIST Special Publication 800-210 [37] provides comprehensive access control strategies tailored for different cloud service models (IaaS, PaaS, SaaS), offering practical implementation guidelines for secure cloud environments (NIST). Similarly, a study in Computer [38] discusses the flexibility of Attribute-Based Access Control (ABAC) and its effectiveness in managing complex access policies in dynamic cloud settings.

Recent advancements also include blockchain-based solutions for access control. Research published in the [39] presents a taxonomy and review of blockchain-based trust management models, highlighting their potential in improving decentralized access control (Journal of Cloud Computing). A study in [40] further explores a blockchain-based data-sharing mechanism, which enhances security and privacy by eliminating central points of failure in cloud access control systems.

Furthermore, research in Sensors [41] examines cloud-native architectures and how access control is implemented in microservices-based systems. The study identifies best practices and emerging challenges in securing cloud-native environments. In a broader review, the International Journal of Computer Science and Mobile Computing [42] compares various access control models and their applications in cloud security, discussing their strengths and limitations.

Cloud computing technology has been developed in detail over the past decade. Most of the organization's computers and data memory was passed to a cloud environment. Researchers conduct extensive research to improve cloud computing environments. They focus on virtualization, cloud security, networking and Qos. Cloud computing is a supply model that provides high availability, flexibility, and services on demand. [3]. Cloud consumers do not need to purchase additional hardware and software. Cloud Service Providers (CSPs) need to ensure the security of the data and services hosted by customers/customers in the cloud. A common technique like this that restricts access to stored data is access control. Access control techniques ensure data confidentiality by restricting access to authorized users only [28].

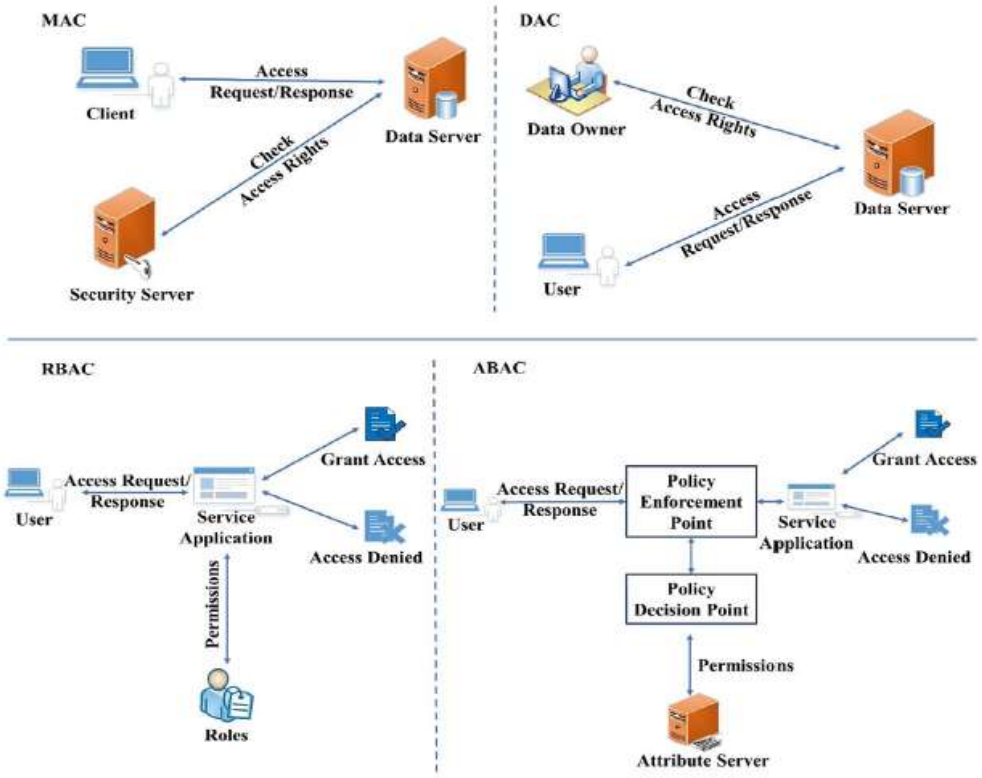

Figure 3: Functional view of main access control methods [21].

Various cloud security issues are represented by [30].

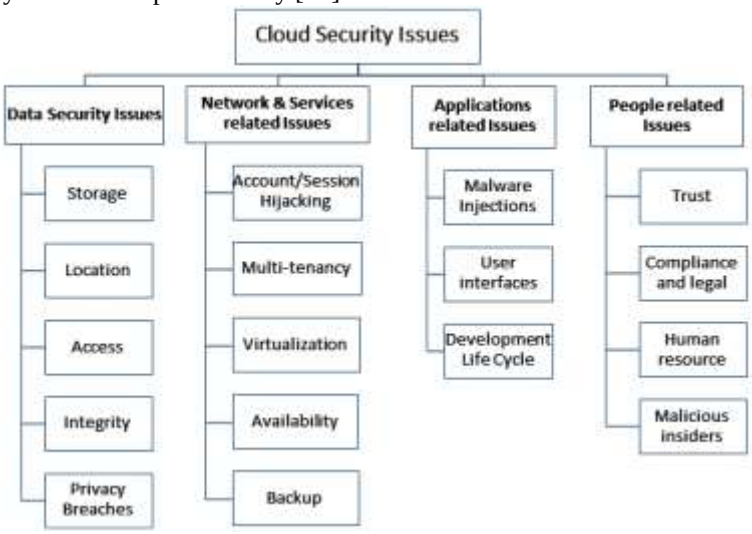

Figure 4: Security issues in cloud [30]

The basic models are not sufficient for the dynamic cloud environment [28][14]. Functional view of MAC, DAC, RBAC, ABAC model is shown in Fig 3. Summary of various access control mechanism, security aspects and their issues are shown in Table 1:

TABLE I
SUMMARY OF VARIOUS ACCESS CONTROL MECHANISM

MODELS	MERITS	DEMERITS
Mandatory access control	It gives more security in accessing the Resources.	It has less flexible environment to process the access rights. It is difficult to implement.
Discretionary access control	The data owner controls the data access policy. Hence it provides more flexibility than MAC.	It provides less security.
Role based access control	1) It is easy to use and simple. 2) The major cloud computing based on RBAC are open stack, AWS and Microsoft Azure. 3) The policies specifications are simple. 4) The manageability is simple. 5) Trust is globally.	1) Role explosion. 2) Without changing the rules the access of a particular entity is not possible. 3) It has administrative, data abstraction issues. 4) No considerations environment attributes. 5) Not well suited for a highly distributed environment.
Attribute access control	1) It has fine grained access control. 2) It is very flexible and expandable with a potential of increasing the higher users. 3) There is no role explosion and role permission explosion problem.	1) The policies specifications are complex. 2) The manageability's are complex. 3) Trust is locally. 4) Sometimes attributes of subjects do not match than those of objects.
Hybrid model (RBAC + ABAC)	1) It is more fine-grained access model. 2) It reduces to number of attributes available in the process. Hence simplify the user – permission relationships.	1) Implementation is complex. 2) Time Consuming.

Attribute-based encryption (ABE) allows users of the model to access the data with the help of user attributes [1]. Private and secret keys are generated with user attributes. The private key is shared with consumers who

meet the database for the purpose of definition of access guidelines. The database defines access directives based on user attributes. Users with private keys can decrypt only the cipher text. The main drawback of ABE is that the database must encrypt data in order to store it in the cloud using the public key of all users. We only discuss a few of them. In the most important guidelines and atrib-based encryption (KP-ABE), many user attributes are assigned to the ciphertext of the access control model, and the private key is assigned to the access structure [1]. In Ciphertext-Policy attribute-based encryption base (CP-ABE), model ciphertext is assigned to access structures, and private keys are assigned to many user attributes [19]. Users can decrypt ciphertext only if the user attribute meets an access structure linked to the ciphertext. For risk-based access control, we deal with risk parameters [7]. Lakshmi et al. [16] Implement risk-based access checks. The customer has considered several parameters that assess the individual's risk. Users can access only if the risk value is lower than the thriller. In this research work, two types of risk were calculated, taking into account risk parameters. H. Current risk values and threshold risk values. This proposed module is of static nature. Dynamic and adaptive risk-based access control modules are the basis of two tasks, and therefore minor changes and improvements to static risk-based access control are required. This model allows for the destruction of unauthorized users based on calculations and updated risk metrics that prevent intrusions on cloud networks. The basic idea behind this model is to improve the security of the access control process in cloud systems. By implementing RBAC in combination with the concept of risk and trust [27]. Table 2 shows contrast results for joint access control methods for various factors [6].

TABLE 2
COMPARISON OF COMMON ACCESS CONTROL METHODS [6]

Factor	MAC	DAC	RBAC	TBAC	ABAC
Security	Y	N	N	N	N
Confidentiality	Y	Y	N	N	N
Flexibility	N	Y	Y	Y	Y
Minimum privilege	Y	N	Y	Y	Y
Duty separation	Y	N	Y	Y	Y
Description	Y	Y	Y	Y	Y
Granularity	Y	Y	N	Y	Y
Constraint	Y	N	Y	N	Y
Dynamic	N	Y	N	Y	Y
Compatible	N	Y	Y	N	Y
Expansibility	N	Y	N	Y	Y
Management	Y	N	Y	N	N

III. PROPOSED METHOD

Proposed research work is a hierarchal system with enhanced risk parameters. It will contains new risk parameter system properties like network, operating system, browser type, type of service used and user access history. Proposed system will calculate risk by accessing user access past behaviour. System parameters play an important role in calculating risk along with parameters like year of experience, designation, defect level, referral index, location index, appraisal factor and probationary period of users. Other attributes like pattern of date and time to access, machine, type of network, operating system, etc. are also important to take risk into account. Proposed system will have a feature of continuous system monitoring. Continuous system monitoring will guide risk engine to learn about users and decides, calculate risk and decide which type of authentication method will use to check user.

The proposed framework is given in figure below:

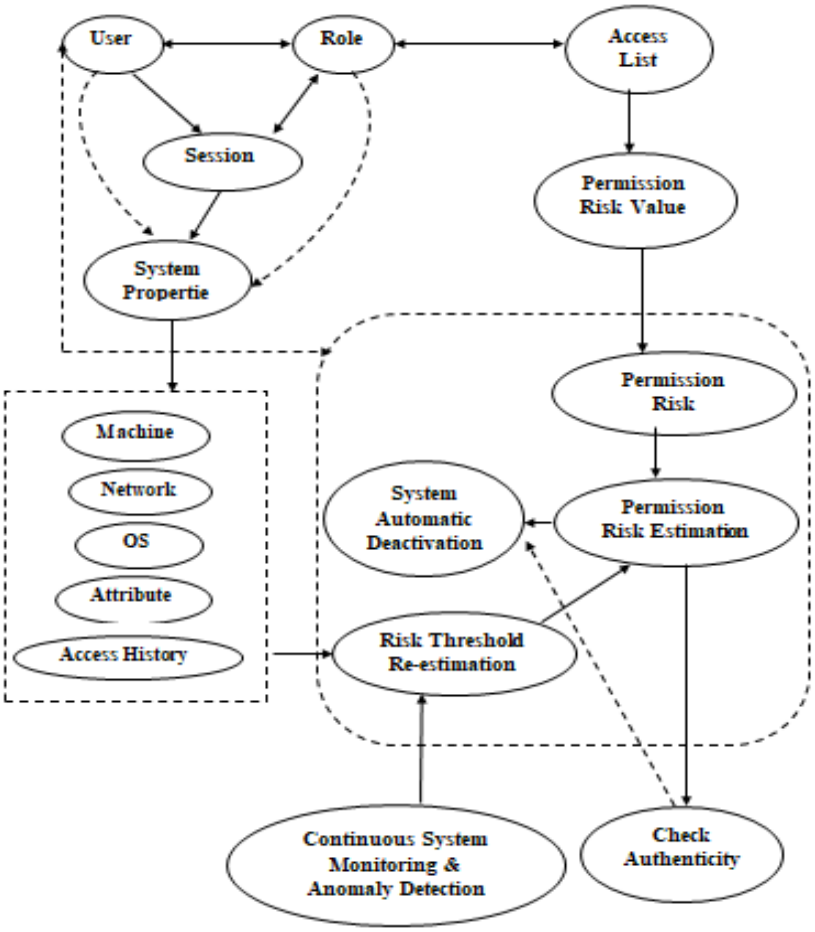

Figure 5: Proposed Model

IV. RESULT

The proposed system uses following parameters to calculate the final risk value:

- Years of Experience
- Designation
- Defect Level
- Referral Index
- Location Index
- Time Index
- Appraisal Factor
- Probationary Period
- System Parameters

For principal role comparison between existing and proposed system is shown below with various attributes, in which different colours lines show different values of attributes generated on login:

Figure 6: Different attributes with existing solution for role principal

Figure 7: Different attributes with proposed solution for role principal

V. CONCLUSIONS

After evaluating the results, it has been shown that improved risk-based access control with improved system attributes contributes to the provision of cloud access control solutions. In particular, these systems are extremely important for businesses and hierarchical cloud organizations. The proposed system is capable of both risk and role-based access control within the cloud. The proposed system is robust and scalable. Administrators can increase both hierarchy and roles as needed. Intrusion prevention access control is the fundamental state of all information systems. It has already become a hot topic in the field of service security.

REFERENCES

[1] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, no. 13, p. 2009, 2009.
[2] Almutairi A, Sarfraz M, Basalamah S. "A distributed access control architecture for cloud computing." Softw IEEE 2012;29(2):36e44. Retrieved from, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber¼6095492.

[3] Aluvalu RajaniKanth and Lakshmi Muddana. "A Survey on Access Control Models in Cloud Computing." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1. Springer International Publishing, 2015.
[4] Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H., "A strong user authentication framework for cloud computing." In: 2011 IEEE Asia-Pacific Services Computing Conference. IEEE; 2011 pp. 110e5. http://dx.doi.org/10.1109/APSCC.2011.14.
[5] Crago S, Dunn K, Eads P, Hochstein L, Kang D-I, Kang M, et al., "Heterogeneous cloud computing." In: 2011 IEEE International Conference on Cluster Computing. IEEE; 2011. pp. 378e85. http://dx.doi.org/10.1109/CLUSTER.2011.49.
[6] Fangbo Cai, Nafei Zhu, Jingsha He, Pengyu Mu, Wenxin Li, Yi Yu, "Survey of access control models and technologies for cloud computing" Springer 2018 https://doi.org/10.1007/s10586-018-1850-7
[7] Ferraiolo DF, Barkley JF, Kuhn, "A role-based access control model and reference implementation within a corporate intranet." ACM Trans Inf Syst Secur 1999;2(1):34e64. http:// dx.doi.org/10.1145/300830.300834.
[8] Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006, October. "Attribute-based encryption for fine-grained access control of encrypted data". InProceedings of the 13th ACM conference on Computer and communications security (pp. 89-98). Acm.
[9] Han, D.J., Gao, J., Zhai, H.L., et al., "Research progress of access control model." Comput. Sci. 37(11), 29–33 (2010)
[10] Hasebe K, Mabuchi M, Matsushita A., "Capability-based delegation model in RBAC." In: Proceeding of the 15th ACM symposium on Access control models and technologies e SACMAT '10. New York, New York, USA: ACM Press; 2010. pp. 109e18. http:// dx.doi.org/10.1145/1809842.1809861.
[11] Hu VC, Kuhn DR, Ferraiolo DF., "The computational complexity of enforceability validation for generic access control rules." In: IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing e Vol 1 (SUTC'06)vol. 1. IEEE; 2006. pp. 260e7. http://dx.doi.org/10.1109/SUTC.2006.1636184.
[12] I. Indu a, P.M. Rubesh Anand, Vidhyacharan Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges" Engineering Science and Technology, an International Journal 21 (2018) 574–588 elsevier
[13] Jin X, Krishnan R, Sandhu R., "A unified attribute-based access control model covering DAC, MAC and RBAC." In: DBSec'12 Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, vol. 7371; 2012. pp. 41e55. Retrieved from, http://www.springerlink.com/index/V7Q168247006164H.pdf; 2012.
[14] Karthick, A. V., E. Ramaraj, and R. Ganapathy Subramanian. "An efficient multi queue job scheduling for cloud computing." Computing and Communication Technologies (WCCCT), 2014 World Congress on. IEEE, 2014.
[15] Keromytis AD, Smith JM., "Requirements for scalable access control and security management architectures." ACM Trans Internet Technol 2007;7(2):22. http://dx.doi.org/10.1145/1239 971.1239972.
[16] Lakshmi Hi, Namitha S, Seemanthini, Satheesh Gopalan, Dr.Sanjay H N, Chandrashekaran K, Atul bhaskar"Risk Based Access Control In Cloud Computing", 2015 IEEE
[17] Lampson, B.W., "A scheduling philosophy for multiprocessing systems." Commun. ACM 11(5), 347–360 (1968)
[18] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y-. Lee, H. Lee, "Enforcing access control using risk assessment", in Proc. 4th European Conference on Universal Multiservice Networks (ECUMN '07), Washington DC., IEEE Computer Society, 2007, pp. 419-424.
[19] Oh S, Park S., "Task role-based access control model." Inf Syst 2003;28(2002):533e62. Retrieved from, http://www. sciencedirect.com/science/article/pii/S0306437902000297.
[20] Patil V, Mei A, Mancini L., "Addressing interoperability issues in access control models." In: ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security, vol. 389e391; 2007. Retrieved from, http://dl.acm.org/citation.cfm?id¼1229337; 2007.
[21] R. Sandhu, P. Samarati, "Access control: principles and practice", IEEE Communications Magazine, vol. 32(9), 1994, pp. 40-48.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[22] RajaniKanth Aluvalu, Lakshmi Muddana, "A Survey on Access Control Models in Cloud Computing", Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Emerging ICT for Bridging the Future – Vol. 1, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_73 pp. 653
[23] Shen, H.B., Hong, F., "Review of access control model." Appl. Res. Comput. 22(6), 9–11 (2005)
[24] Sun, P.J., "Security and privacy protection in cloud computing: Discussions and challenges", Journal of Network and Computer Applications (2020), doi: https://doi.org/10.1016/j.jnca.2020.102642.
[25] Thomas Beach, Omer Rana, Yacine Rezgui, Manish Parashar, "Governance Model for Cloud Computing in Building Information Management", IEEE TRANSACTIONS ON SERVICES COMPUTING, 2013

[26] Wang W, Han J, Song M, Wang X., "The design of a trust and role based access control model in cloud computing." In: 2011 6th International Conference on Pervasive Computing and Applications. IEEE; 2011. pp. 330e4. http://dx.doi.org/10.1109/ ICPCA.2011.6106526.
[27] Wided Ben Daoud, Amel Meddeb-Makhlouf, Faouzi Zarai, " A Model of Role-Risk Based Intrusion Prevention for Cloud Environment", IEEE 2018
[28] Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing," Journal of Information Security and Applications (2014)Elsevier , http://dx.doi.org/10.1016/j.jisa.2014.04.003
[29] https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-policy-governance-risk-compliance/
[30] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z.,"Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey". *Electronics*, *11*(1), 16. https://doi.org/10.3390/electronics11010016
[31] A. K. Das, P. Saha, S. Chatterjee, and M. Conti, "A review on data access control schemes in mobile cloud computing: State-of-the-art solutions and research directions," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–18, May 2021, doi: 10.1007/s42979-021-00917-w.
[32] Y. Wang, J. Yu, and M. Guo, "A secure access control framework for cloud management," *Mobile Netw. Appl.*, vol. 26, no. 3, pp. 1106–1115, Jun. 2021, doi: 10.1007/s11036-021-01839-w.
[33] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394, Feb. 2014, doi: 10.1109/TPDS.2013.180.
[34] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 2010*, San Diego, CA, USA, Mar. 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5462174.
[35] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-145, Sep. 2011.
[36] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS '06)*, Alexandria, VA, USA, Oct. 2006, pp. 89–98, doi: 10.1145/1180405.1180418.
[37] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc. 14th Eur. Symp. Res. Comput. Secur. (ESORICS 2009)*, Saint-Malo, France, Sep. 2009, pp. 587–604, doi: 10.1007/978-3-642-04444-1_35.
[38] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. 2007 IEEE Symp. Secur. Privacy (SP '07)*, Berkeley, CA, USA, May 2007, pp. 321–334, doi: 10.1109/SP.2007.11.
[39] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proc. 33rd Int. Conf. Very Large Data Bases (VLDB '07)*, Vienna, Austria, Sep. 2007, pp. 123–134, doi: 10.14778/1325851.1325870.
[40] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014, doi: 10.1109/TPDS.2013.180.
[41]M. S. Rahaman, S. N. Tisha, E. Song, and T. Cerny, "Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study," *Sensors*, vol. 23, no. 7, p. 3413, Mar. 2023, doi: 10.3390/s23073413. MDPI
[42] A. Venčkauskas, D. Kukta, Š. Grigaliūnas, and R. Brūzgienė, "Enhancing Microservices Security with Token-Based Access Control Method," *Sensors*, vol. 23, no. 6, p. 3363, Mar. 2023, doi: 10.3390/s23063363.