Enhancing Security and Flexibility with Combined RBAC and ABAC Access Control Models

P. M Jyosthna
Department of CSE
B V Raju Institute of Technology
Narsapur, Telangana, India
jyosthna.p@bvrit.ac.in

Anirudh Varma Mandapati
Department of CSE
B V Raju Institute of Technology
Narsapur, Telangana, India
21211a05g1@bvrit.ac.in

Matam Surya Teja
Department of CSE
B V Raju Institute of Technology
Narsapur, Telangana, India
21211a05g7@bvrit.ac.in

Sachin Kumar Ray
Department of CSE
B V Raju Institute of Technology
Narsapur, Telangana, India
22215a0519@bvrit.ac.in

B.Yashwanth Sai Kumar
Department of CSE
B V Raju Institute of Technology
Narsapur, Telangana, India
21211a05k5@bvrit.ac.in

2024 10th International Conference on Communication and Signal Processing (ICCSP) | 979-8-3503-5306-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCSP60870.2024.10543482

Abstract— **Organizations have started using the feature known as remote data access in recent years. Although it has benefits for the organization's economic development, it also creates several security risks to the protection of its resources. A "Hybrid Access Control Model" is being proposed to address the issues related to access control on an organization's resources. It has integrated both the properties of Attribute Based Access Control (ABAC) And Role Based Access Control (RBAC). RBAC dictates organization roles and their access permissions whereas ABAC dictates attributes of the user who is requesting access. According to user roles, it can be determined what tasks they are responsible for inside the company, and according to user factors like time and location, it can be determined if they are accessing from home or the office. It uses Two-factor authentication to create an additional layer of security to verify the identity and attributes of users before granting access.**

Keywords— Remote Access, Access Control, RBAC, ABAC

I. INTRODUCTION

Access control refers to the process of granting or denying access to resources or information based on the identity of the user and their level of authorization. It is a security measure that helps organizations to protect sensitive data and prevent unauthorized access. There are three main types of access control: Mandatory Access Control (MAC): This type of access control is typically used in high-security environments, such as government agencies or military installations. In MAC, access to resources is granted or denied based on a set of rules defined by the system administrator. These rules are based on factors such as security clearance, job role, and need-to-know. Discretionary Access Control (DAC): This access control type lets the resource owner decide who can use it. The owner can say yes or no to particular users or groups based on who they are, what they do, or other reasons. DAC is often used in smaller organizations where super-high security isn't the main worry. Role-Based Access Control (RBAC): This type of access control is based on the concept of assigning roles to users and granting or denying access to resources based on their assigned roles.

RBAC is commonly used in large organizations where there are many users with different levels of access. It simplifies the access control process by allowing system administrators to manage access based on roles rather than individual users. Attribute Based Access Control (ABAC) presents itself as a viable alternative to RBAC, offering a solution to overcome RBAC's limitations. ABAC's superiority lies in its flexibility, as it readily incorporates contextual attributes when defining permissions. However, ABAC also has its drawbacks, such as increased complexity compared to RBAC, particularly concerning policy review and modification visualization. This complexity arises due to the absence of roles in ABAC, making it challenging to identify the user groups affected by policy modifications. As discussed earlier, both RBAC and ABAC possess distinct advantages and disadvantages. They offer complementary features, making the integration of RBAC and ABAC a significant area of research.

The rest of the paper is organized as follows. Section 2 describes the existing works that have been done so far by various researchers. It also mentioned the objective of this proposed model to address the issues identified in the existing works. Section 3 introduced the proposed model and its algorithm to implement it. Section 4 discussed the results obtained from the proposed model. Section 5 concludes the proposed model with its purpose and findings.

II. LITERATURE SURVEY

In recent research endeavors, multiple scholars have delved into the realm of cloud-based data sharing and access control. Jialu Hao in [1] introduced attribute-based access control which enables data users to define search policies based on the data owner's access policy while addressing data confidentiality. However, a notable drawback is that the cloud server gains access to search ciphertext without having attribute information, raising security concerns. Qian Xu et al., in [2] proposed an access control scheme that expanded data sharing capabilities in the cloud with a focus on privacy preservation and offered security features such as fine-grained access control and anonymous authentication. This scheme effectively outsources resource-intensive computations to enhance decryption while maintaining attribute privacy.

Mumina Uddin et al., in [3] introduced a dynamic access control model that blends RBAC and ABAC, emphasizing real-world applications, particularly in the IT sector. This model enhances process and task sequencing, improving OASIS standards with additional repositories and functions. Lan Zhou et al., in [4] proposed a hybrid RBE model that combines role-based access control with encryption to secure cloud-stored information, offering features like constant-size ciphertexts, efficient user revocation, and role hierarchy support. Smriti Bhatt et al., in [5] extended the AWS IoT

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL. Downloaded on February 16,2026 at 03:27:10 UTC from IEEE Xplore. Restrictions apply.

979-8-3503-5306-8/24/$31.00 ©2024 IEEE

access control model with ABAC capabilities for fine-grained access control in the AWS IoT platform, with practical applications in a smart oil refinery, highlighting the growing role of IoT in various industries. Yong Wang et al., in [6] introduced an innovative model focusing on attribute encryption to enhance security in open environments, allowing for more flexible and authorization-independent access control by combining RBAC and ABAC principles.

Ben Attis Hasiba et al., in [7] proposed a hybrid access control model that integrated the best features of RBAC and ABAC, considering roles, attributes, object types, and access modes, offering distinct advantages over traditional models such as RBAC and ABAC. Ni Dan et al., in [8] addressed the challenge of integrating SOA systems across security domains by proposing an ABAC-based cross-domain access control system, which leveraged attributes related to security, subjects, objects, authorities, and environments to facilitate integration within the SOA framework. Ye Lang et al., in [9] introduced an ABE-based access control system aimed to resolve issues such as efficiency, attribute revocation, and third-party attacks in cloud computing, demonstrating the potential to mitigate super privilege problems. Kritika Soni et al., in [10] compared both role-based access control and attribute-based access control models, highlighting the advantages of combining these techniques to simplify authorization and overcome the limitations of each individual approach.

Shantanu Pal et al., in [11] identified limitations in existing access control models, such as RBAC, ABAC, and AERBAC, including issues related to role proliferation, context awareness, policy visualization, and updates. To address these challenges, they proposed a novel access control model that integrates and extends RBAC and ABAC functionalities. The introduced novel approach combines verifiable computation and encryption through a MAC mechanism, this method enables cloud servers to receive a verifiable partial decryption pattern. Built on the k-multi-linear Decisional Diffie-Hellman assumption, it ensures data privacy, fine-grained access control, and provable customizable authorization [12, 13]. Enhancing medical record security, a CP-ABE-based access control policy utilizes attributes for user identification, generating keys through elliptic curve cryptography. AES encryption ensures robust data protection, providing authorized users with access to encrypted data [14]. Implementing a dual-domain security model, this approach divides the security domain into private and public domains, employing Vigenere encryption for the former and the TwoFish algorithm for the latter. This ensures high security, reduced memory size for key storage, and improved efficiency in key generation, encryption, and decryption compared to existing systems [15].

A blockchain-based [16] SCF management system with an attribute-based access control model is proposed for secure storage and auditable access to sensitive financial data. Through distributed consensus and smart contracts, it enables dynamic access policies adaptable to changing business requirements.

HyARBAC, a hybrid access control model for cloud computing, integrates ABAC and RBAC, leveraging environmental data [17] and a Moving Target Defense mechanism for enhanced security. By activating roles based on environmental attributes and employing attribute-based rules, HyARBAC ensures dynamicity, auditability, scalability, and heightened security in cloud environments. From the literature, it has been identified that a single access control model cannot handle large-scale access control scenarios effectively. The continuous practice of creating an additional role and mapping access permissions to that role may lead to an additional burden on the RBAC model. ABAC can only restrict access based on the user attributes and their contextual information. There is no possibility of enforcing access control based on the organizational role hierarchy. A hybrid access control model is proposed in this paper to increase the level of security and to reduce the security threat of unauthorized resource access through the mapping of roles and permissions.

III. PROPOSED WORK

The proposed system considers a hybrid combination of ABAC and RBAC to reduce the risk of internal threats and data Misuse. By limiting the data access to the official authorities and giving required access to the base-level engineers. With the help of the agile model, it shares the data among all the departments so that there will be constant work progress while maintaining the security of the data.

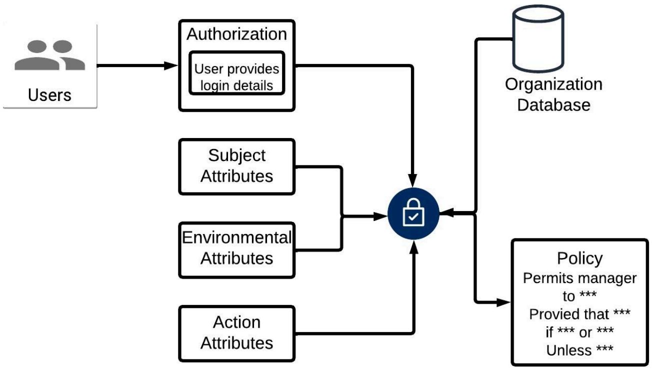


Fig. 1. Architecture Diagram

The high-level architecture of the proposed model is shown in Fig. 1. The primary focus of the proposed model is on user access management and authorization. Users initiate the process by providing their login credentials, which serve as a means of authentication. Once authenticated, a comprehensive evaluation of access rights takes place, considering subject attributes (such as user characteristics and roles), environmental attributes (contextual factors like location or time), and action attributes (specifying the requested action).

The heart of this proposed hybrid model is the Hybrid Engine, a critical component responsible for orchestrating access decisions. This engine integrates seamlessly with the organization's database, where user profiles, roles, and resource information are stored. The model operates based on a set of defined policies, which are flexible and context-driven. These policies may include conditions like "Permits manager to", "Provided that", "If", "Or" and "Unless". These conditions empower administrators to make nuanced access control decisions, taking into account the specific attributes and context of each access request.

By merging the strengths of ABAC and RBAC, this hybrid approach ensures a robust and adaptive access control system. RBAC provides a structured foundation for assigning roles and responsibilities, while ABAC enhances it with fine-grained control based on dynamic attributes and contextual information from that department's manager.

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL. Downloaded on February 16,2026 at 03:27:10 UTC from IEEE Xplore. Restrictions apply.

This hybrid approach leverages RBAC's structured role assignments and ABAC's flexibility in considering a wide range of attributes and contextual factors. Users are assigned roles, and their access is further refined based on attributes such as time, location, or job title. This fusion allows for fine-grained, context-aware access decisions, improving security and adaptability in dynamic organizational environments.

For remote location access, the model ensures that the system can effectively manage access requests from outside the organization's network, taking into account the varying security risks associated with remote locations. Implementing geolocation-based policies and considering contextual attributes like IP addresses can help tailor access permissions dynamically.

Algorithm of Proposed Hybrid Access Control Model

Algorithm 1 enables efficient decision-making processes, allowing systems to automate complex tasks and make intelligent choices, which is essential for scalability and reliability.

```
Algorithm:

Step 1: Credentials Verification

CHECK: if the username and given role match the credentials in the system.
IF match:
Retrieve user_data.
IF role is not valid:
PRINT: "Not a worker of the Organisation"
EXIT.
ELSE:
Proceed to location verification or access control based on role_permissions.

Step 2: Location Verification (Optional, role-based)

IF role requires physical presence (e.g., team leader):
COMPARE: user_data["location"] with office_location.
IF mismatch:
ASK: "Are you doing WFH? [Y/N] "
ELSE:
PRINT: "Have a great day at the office"
Continue your daily routine at the office.

Step 3: Work-From-Home (WFH) Status (optional, role-based)

IF role allows WFH and user_data["WFH_allowed"] is True:
ASK: "Are you working from home (WFH) today?"
IF user_input is "Y":
ASK: "Can you complete the work in 8 hours [Y/N]: "
IF user_input is "Y":
GRANT: WFH access.
ELSE:
DENY: WFH access and suggest alternative arrangements.
ELSE: Proceed to resource access control.
ELSE:
Skip the WFH prompt and proceed to resource access control

Step 4: Resource Access Control

GET: resource_id from user.
CHECK: if resource_id belongs to the user's team based on team_structures.
IF match:
CHECK: if resource_id is allowed for the user's role based on resource_access.
IF allowed:
GRANT: access to the resource.
ELSE:
ASK: "Request access from team leader?"
IF user_input is "Y":
SEND: access request to the team leader.
IF request approved:
GRANT: access to the resource.
ELSE:
PRINT: "Request Denied!!"
ELSE:
PRINT: "Access Denied!!"
ELSE (resource not part of user's team):
CHECK: if the user has temporary access granted for this resource.
IF temporary access is granted:
GRANT: access to the resource.
ELSE:
ASK: "Request access from the resource's project manager?"
IF user_input is "Y":
SEND: access request to the project manager.
IF request approved:
GRANT: temporary access to the resource.
ELSE:
PRINT: "Access request denied."
ELSE:
PRINT: "You are not allowed to access this resource."
```

IV. Result and Discussion

Firstly, the RBAC component evaluates the role-based conditions by checking if the user's assigned roles have the necessary permissions to perform the requested action on the resource. This evaluation relies on the predefined role-permission mappings established within the RBAC framework. If the RBAC evaluation does not yield a conclusive result or additional context is required, the hybrid model proceeds to the ABAC component. Here, the attribute-based conditions come into play, considering attributes associated with the user, resource, and environment. These attributes encompass various factors such as user roles, job titles, data classifications, location, and time of access. The ABAC evaluation assesses whether the attribute values meet the conditions specified in the policies.

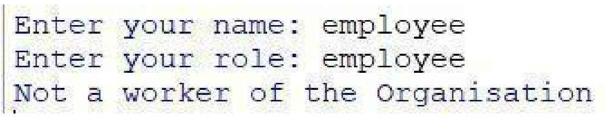
Once the RBAC and ABAC evaluations are complete, the hybrid model combines the results to make the final access control decision. The specific method of combining the results may vary depending on the implementation, but the overall aim is to ensure that the decision aligns with

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL. Downloaded on February 16,2026 at 03:27:10 UTC from IEEE Xplore. Restrictions apply.

both the role-based permissions and the attribute-based contextual information. By incorporating both RBAC and ABAC elements in policy evaluation, the hybrid access control model provides a more comprehensive and adaptable approach to access control. It leverages the strengths of both models, enabling organizations to achieve a fine-grained and context-aware access control system that meets their specific security requirements

Case 1: Employee authentication

To access the system, users are required to undergo a two-step authentication process. Initially, users input their credentials, consisting of a username and role as shown in Fig. 2.



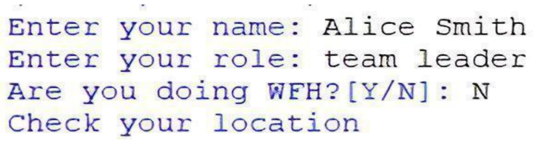
```
Enter your name: employee
Enter your role: employee
Not a worker of the Organisation
```

Fig. 2. Employee authentication

Subsequently, the system engages a location library to determine the user’s current location, cross-referencing it with the specified company location stored in the database. During this process, if the system fails to find corresponding employee details in the company database based on the provided credentials, the outcome is a definitive message stating, ”Not a worker in the Organization”. Consequently, the system terminates the operation, denying access to the user. This stringent verification process ensures that only authorized personnel, whose details align with the company records, are granted entry, reinforcing the security measures of the system.

Case 2: Remote location access

As the user, a pivotal team leader within the organization engages with the system and is asked to provide essential details. After entering the login credentials it verifies whether the user’s location is matched with office location or not. The system then seeks to understand the user’s current work arrangement by inquiring whether he/her currently working from home (WFH), to which he/she responds with the answer ”N” (No) as shown in Fig. 3.. This decision triggers the system to initiate a critical location verification process by asking the user to check their physical location. It also underscores the importance of physical presence for certain roles, such as team leadership, to facilitate effective communication, collaboration, and oversight of team activities.



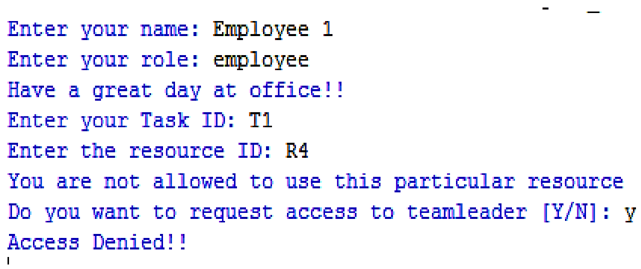
```
Enter your name: Alice Smith
Enter your role: team leader
Are you doing WFH?[Y/N]: N
Check your location
```

Fig. 3. Remote Location Access

Case 3: Verification of user location

In the authentication flow, once the primary login is successfully verified against the company database, the system introduces an additional layer of inquiry. It asks the user the question, “Are you working from home (WFH)?” If the user responds affirmatively, indicating a remote work arrangement, the system proceeds to inquire whether the user can complete their assigned tasks within the allocated time. Then it asks the user whether he can complete the work in 8 hours. If the user confirms their ability to complete tasks remotely, the system grants work-from-home (WFH) access. However, if the user attempts to access tasks assigned to other teams by entering a task ID, an additional authorization step is implemented. The system asks the user to seek permission from the project manager associated with the task team.

Upon entering the task ID of another team, the user is asked to request access permission from the respective project manager. This step ensures a hierarchical and controlled access process. Once the project manager grants permission, the user gains access to the specific resource or task they sought initially. It ensures that remote work permissions are granted judiciously and access to tasks from other teams is regulated through proper channels, contributing to a secure and organized work environment as shown in Fig. 4.

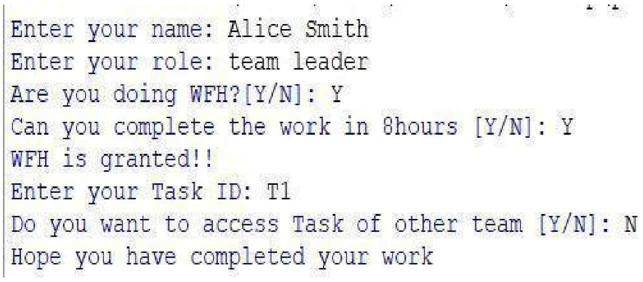


```
Enter your name: Employee 1
Enter your role: employee
Have a great day at office!!
Enter your Task ID: T1
Enter the resource ID: R4
You are not allowed to use this particular resource
Do you want to request access to teamleader [Y/N]: y
Access Denied!!
```

Fig. 4. Verification of user location

Case 4: Task and Resource allotment

The provided scenario in case 3, the user, identified as “Employee1” with the role “Employee” receives a message expressing well wishes for their day at the office. Subsequently, the user is asked to enter a task ID, and upon providing a Resource ID they are informed that they are allowed/ not allowed to use that particular resource. For instance, a software engineer based in the company's headquarters may need access to certain proprietary code repositories based on their role as a member of the development team. RBAC assigns them the appropriate permissions as a "Developer" role. This scenario is shown in Fig. 5. If it is not allowed case, a proactive solution is presented by asking whether the user wants to request access from their team leader. Upon responding affirmatively (Y), the user receives a confirmation message that access has been granted, followed by encouragement to complete the assigned work. The inclusion of a request mechanism to the team leader adds a layer of authorization, ensuring that access permissions are granted in a controlled manner.



```
Enter your name: Alice Smith
Enter your role: team leader
Are you doing WFH?[Y/N]: Y
Can you complete the work in 8hours [Y/N]: Y
WFH is granted!!
Enter your Task ID: T1
Do you want to access Task of other team [Y/N]: N
Hope you have completed your work
```

Fig. 5. Task and Resource Allotment

The proposed hybrid access control model, combining Role-Based Access Control (RBAC) and Attribute-Based

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL. Downloaded on February 16,2026 at 03:27:10 UTC from IEEE Xplore. Restrictions apply.

Access Control (ABAC), presents a compelling solution to address the complexities and evolving security requirements of modern systems. This discussion will delve into the key points and considerations surrounding the implementation and effectiveness of this hybrid model.

1) *Integration of RBAC and ABAC:*

The hybrid model integrates RBAC and ABAC by leveraging their respective strengths. RBAC provides a structured approach to access control through predefined roles, simplifying administration and user role management. On the other hand, ABAC introduces the concept of attributes, allowing for a more dynamic and contextual access control framework. The integration of these two approaches aims to combine the benefits of RBAC's simplicity and scalability with ABAC's flexibility and contextual control.

2) *Flexibility and Adaptability:*

The hybrid model offers flexibility and adaptability, allowing organizations to respond to changing business requirements and evolving security needs. RBAC provides a straightforward approach to access control policy management, making it easy to assign permissions based on predefined roles. However, as systems become more complex and dynamic, additional flexibility is often necessary. ABAC introduces this flexibility by allowing organizations to consider a broader range of attributes and context-specific factors. The hybrid model thus accommodates changes in user roles, resource properties, or environmental conditions, ensuring that access control policies remain effective and aligned with evolving security demands.

3) *Security and Compliance:*

Effective security and compliance measures are critical considerations in access control models. RBAC contributes to security by enforcing the principle of least privilege, ensuring that users have only the necessary permissions for their roles. It also supports the separation of duties, mitigating risks associated with insider threats. ABAC enhances security by considering a wider range of attributes and contextual factors when making access decisions. By incorporating ABAC into the hybrid model, organizations can enforce more stringent security policies and grant access based on relevant contextual information. This comprehensive approach strengthens the overall security posture and helps organizations comply with regulatory requirements.

Table 1. Comparative Analysis of Existing Access Control Models with Proposed Hybrid Model

Set of requirements	RBAC	ABAC	Proposed Hybrid Model
Session Management	NO	YES	YES
Separation of duties	YES	NO	YES
Regular access reviews	NO	NO	YES
Context verification	NO	YES	YES
Two-level authorization	NO	NO	YES

4) *Implementation and Management Considerations:*

Implementing and managing a hybrid access control model requires careful consideration. Organizations need to define and align roles, attributes, and associated policies effectively. This may involve mapping RBAC roles to corresponding ABAC attributes and determining how attributes impact access decisions. Additionally, organizations must establish robust processes for managing and updating access control policies to ensure they remain current and aligned with evolving business needs. Training and awareness programs may also be necessary to familiarize users and administrators with the hybrid model's features and best practices.

V. Conclusion

This Hybrid Access Control Model offers various advantages by guaranteeing that designated individuals with proper authorization are the only ones permitted to access specific resources or execute particular actions within a system. By including various Access Control Models and methods the proposed access control model integrates both RBAC and ABAC properties to ensure that authorization can be performed at two stages for accessing required resources. With RBAC, the model achieves the least privileges principle by verifying the requester's role and its associated permissions, and with ABAC the model achieves granular and adaptable access control by considering multiple attributes (user roles, job titles, location, time of access, data classification) and policies, enhancing security in diverse access scenarios. Finally, the proposed Hybrid Access Control Model meets all the organizational requirements and compliance standards by giving its careful design and implementation.

VI. Acknowledgment

We wish to extend our sincere appreciation to all individuals who played a part in the project's success. Your invaluable support and guidance were integral to our achievement in completing it successfully.

We would like to sincerely thank our guide, Mrs. P. M Jyosthna, Department of CSE, for her insightful advice and inspiring words that helped us finish the project successfully.

REFERENCES

1. Hao, J., Liu, J., Wang, H., Liu, L., Xian, M., & Shen, X.: Efficient attribute-based access control with authorized search in cloud storage. IEEE Access 7, 182772-182783(2019).
2. Xu, Q., Tan, C., Fan, Z., Zhu, W., Xiao, Y., & Cheng, F.:Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption. IEEE Access 6, 34051-34074(2018).
3. Uddin, M., Islam, S., & Al-Nemrat, A.: A dynamic access control model using authorizing workflow and task-role-based access control. IEEE Access 7, 166676-166689(2019).
4. Zhou, L., Varadharajan, V., & Hitchens, M.: Enforcing role-based access control for secure data storage in the cloud. The Computer Journal 54(10), 1675-1687(2011).
5. Bhatt, S., Pham, T. K., Gupta, M., Benson, J., Park, J., & Sandhu, R.: Attribute-based access control for AWS Internet of things and secure industries of the

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL. Downloaded on February 16,2026 at 03:27:10 UTC from IEEE Xplore. Restrictions apply.

future. IEEE Access, 9, 107200-107223(2021).

6. Yong Wang, Yuan Ma, Keyu Xiang, Zhenyan Liu.: ARole-Based Access Control System Using Attribute-Based Encryption. Journal on Big Data and Artificial Intelligence 12, 128-133(1982).
7. Hasiba, B. A., Kahloul, L., & Benharzallah, S.: A new hybrid access control model for multi-domain systems. In: 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), pp. 0766-0771, IEEE, (2017).
8. Dan, N., Hua-Ji, S., Yuan, C., & Jia-Hu, G.: Attribute-based access control (ABAC)-based cross-domain access control in service-oriented architecture (SOA). In: 2012 International Conference on Computer Science and Service System, pp. 1405-1408, IEEE, (2012).
9. Liang, Y., Wang, J., Zhang, L., Ge, Z., Zhai, H., Ge, M., & Jin, H.: Research of access control system based on attribute encryption technology that suitable for dispatching and control the cloud. In: 2019 IEEE 4th International Conference on cloud computing and Big Data Analysis (ICCCBDA), pp. 358-362, IEEE, (2019).
10. Soni, K., & Kumar, S.: Comparison of RBAC and ABAC security models for private cloud. In: 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), pp. 584-587, IEEE, (2019).
11. Pal, S., Hitchens, M., Varadharajan, V., & Rabehaja, T.:Policy-based access control for constrained healthcare resources. In: 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pp. 588-599, IEEE, (2019).
12. Raja, S. K. S., Sathya, A., & Priya, L.: A Hybrid Data Access Control Using AES and RSA for Ensuring Privacy in Electronic Healthcare Records. In: 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), pp. 1-5, IEEE, (2020).
13. Rathod, V., Narayanan, S., Mittal, S., & Joshi, A.:Semantically rich, context-aware access control for OpenStack. In: 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 460-465, IEEE, (2018).
14. Chennam, K., & Muddana, L.: Improving Privacy and Security with Fine-Grained Access Control Policy using Two Stage Encryption with Partial Shuffling in the Cloud. In: 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 686-690, IEEE, (2018).
15. Gunjal, Y. S., Gunjal, M. S., & Tambe, A. R.: Hybrid attribute-based encryption and customizable authorization in cloud computing. In: 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), pp 187-190, IEEE, (2018).
16. Li, D., Han, D., Crespi, N., Minerva, R., & Li, K. C. (2023). A blockchain-based secure storage and access control scheme for supply chain finance. The Journal of Supercomputing, 79(1), 109-138.
17. Houhou, O., Bitam, S., & Hamida, A. (2024). HyARBAC: A New Hybrid Access Control Model for Cloud Computing. International Journal of Computing and Digital Systems, 15(1), 1-11.

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY WARANGAL. Downloaded on February 16,2026 at 03:27:10 UTC from IEEE Xplore. Restrictions apply.