International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

CRABAC: Combined Role-Attribute Based Access Control Model

Abhimanyu Bansal[1], Dr. C Vinothini[2]

[1]PG Student, Computer Science and Engineering, Dayananda Sagar College of Engineering, Karnataka, India
[2] Professor Computer Science and Engineering, Dayananda Sagar College of Engineering, Karnataka, India

---

Abstract - Access control is one of the techniques to provide accessibility, flexibility and control over the cloud resources. The traditional access control model is no longer sufficient to provide protection of data. Due to the rising data breaches, it is important to evolve our data security mechanisms. Therefore, it is better to combine several techniques to bring out the most efficient technique. Thus, this paper introduces custom access control model where Role-Based Access Control (RBAC) model and Attribute-Based Access Control (ABAC) model is combined to give a single hybrid model. This technique brings out the best qualities of both models. It provides both flexibility and dynamicity. The assignment of attributes provides better security.

Key Words: *Access Control, Role-Based Access Control, Attribute-Based Access Control, Cloud Computing*

1. INTRODUCTION

Cloud computing is the availability and accessibility of different cloud resources over the internet. The benefits provided by cloud computing is enormous. The main benefit provided by cloud computing is storage, computing power and cost-effective as compared to physical infrastructures. Due to rising data generation, demand of cloud resources has risen significantly. However, with such benefits, also comes huge security issues and resource management problems. Therefore, access control mechanisms provide security and resource management. It focuses on authorization of users accessing some cloud resource. This mechanism provides continuous verifying of users which enables better security.

The cloud offers a digital arena to host servers, platforms, and services, delivering resources through models like SaaS, PaaS, and IaaS. While cloud computing provides notable advantages, from cost savings to deployment agility, its efficacy hinges on top-tier security and consistent accessibility. Safeguarding access—through both authentication and authorization—is pivotal, especially when sensitive information from individuals and businesses is stored. The public cloud demands rigorous security measures. A unique challenge arises from the sharing of cloud resources among potentially untrusted users, underscoring the need for comprehensive access control methods. If these controls falter, it opens doors for unauthorized access. Hence, a robust system must be in place, which encrypts data, checks user identities when they request access, and only then grants access permissions.

The digital revolution has thrust cloud computing to the forefront, positioning it as a linchpin in the modern technological ecosystem. At its core, the cloud acts as a sophisticated repository, offering not just storage but also computation capabilities across models like SaaS, PaaS, and IaaS. This flexible framework provides businesses with unparalleled scalability, allowing them to adapt dynamically to ever-changing market conditions.

Yet, this flexibility doesn't come without its challenges. In a world where data breaches and cyber-attacks have become the norm, the security of cloud infrastructures is paramount. It's not just about protecting data in transit, but also ensuring its sanctity when it's at rest. The inherent structure of the public cloud, which hosts multiple users on shared resources, complicates matters. It's akin to a vast digital marketplace, where not every participant might have pure intentions.

To counteract this, rigorous vetting processes for access control become essential. It's not just about knowing who wants access, but also understanding why they want it and what they intend to do with it. Therefore, in this paper, the focus is mainly on the structure of access control model which can provide better security.

2. LITERATURE REVIEW

Authors in [1], conducts an exhaustive analysis of top methods for ensuring secure data sharing within the cloud. It delves into the functionality, potential solutions, workflow, accomplishments, and shortcomings of each technique in data protection techniques. Additionally, it contrasts various methods to determine their suitability for specific needs. The paper also identifies current research gaps and suggests future research directions. The authors anticipate that their work will inspire and guide future research endeavours in cloud domain. It discusses major classification of data protection techniques which are cryptography, access control, differential privacy with machine learning, watermarking and probabilistic techniques. The authors conclude that no single technique is sufficient to provide data protection and security, hence hybridization of various techniques yields better protection and security.

In [2], the authors present a hybrid approach for access control which combines both role-based access control and attribute-based access control models which offers enhances security and adaptability. Through this paper we perform similar approach bringing better stability and robustness.

In [3], authors delve into improving access management in borderless networks, emphasizing real-time decision-making and policy implementation. Three key contributions emerge: 1) It introduces an Authorising Workflow Task Role-Based Access Control that upgrades existing models, like RBAC, by granting user access dynamically while maintaining governance and accountability. 2) The research adapts the

OASIS XACML policy language to cater to dynamic access needs, addressing risks like unchecked privilege escalation and inadequate logging. 3) Utilizing the open-source Balana policy engine, the model is tested on a real-world financial institution scenario. The findings reveal that the AW-TRBAC system can efficiently handle numerous complex requests while upholding dynamic access control standards.

In [4], authors perform a detailed analysis on different access control mechanisms in cloud computing. The study explores access control mechanisms, highlighting that attribute-based controls align well with provenance-based systems with minor adjustments. Meanwhile, traditional role-based controls are ideal for trust-based access. It's crucial to identify unauthorized users to prevent service access. Challenges include encryption complexities, especially key management, and setting trust thresholds based on dynamic user behaviour. The intricacies of managing data provenance databases in the cloud and granting appropriate access to authorized users are pressing concerns. This paper delves into various access control techniques, evaluating their merits and drawbacks, emphasizing the ongoing importance of security, user authentication, and robust access control. Despite enhancements to existing methods, the realm of access control still presents significant research opportunities.

In [5], the article introduces LW-C-CP-ARBE, a system designed for lightweight decryption in collaborative mobile cloud computing that also supports write access for outsourced data. By incorporating proxy-based re-encryption, their approach ensures secure policy sharing for users with write access. One of the primary benefits is reducing computational strain on mobile devices by shifting it to a proxy server, making it suitable for mobile cloud settings. The authors delved into the security facets of their method and contrasted its efficiency with similar systems. Through comprehensive testing, they found LW-C-CP-ARBE to outperform its peers, indicating its readiness for practical application in the mobile cloud domain. Future plans involve more extensive testing, exploring multi-proxy setups, and streamlining the encryption process for mobile users uploading to the cloud.

In [6], the study introduces the EACAS (efficient attribute-based access control with authorized search scheme), designed to address data-sharing needs in cloud storage while safeguarding data confidentiality and attribute privacy. With EACAS, users can create search policies based on the permissions set by the data owner and create related search criteria without the data owner's intervention. Importantly, cloud servers can search encrypted data on users' behalf without accessing attribute details or the actual plaintext. After evaluating EACAS's attributes, security, and performance, the findings show its practicality and efficiency. Future research aims to incorporate anonymous KP-ABE to enhance data sharing and storage, especially in the e-health cloud sector.

In [7], the paper presents the I-RBAC model, a novel security mechanism tailored for the rapidly evolving modern environments. The I-RBAC system offers a solution to security challenges in distributed contexts via intelligent multi-domain access control. Leveraging a multi-agent system built on RBAC, it introduces semantic roles, which are derived from various occupational titles. It further introduces dynamic role activation and deactivation tied to specific user, role, action, and object attributes, and incorporates monitoring agents for role management activities. To ensure adaptability and scalability, knowledge management via ontology is incorporated, enabling the definition and enforcement of dynamic access control rules. This model's agents manage dynamic role assignments within a revamped policy and utilize real-world data sets for role creation. With the ability to reason, these ontologies facilitate access control decision-making and semantic interoperability, enhanced by the business roles class. Practical testing of this model on a large data set, encompassing 100,000 permission assignments across diverse sectors, confirmed its efficacy and efficiency, with promising runtime results. The core knowledge of I-RBAC is grounded in the latest SOC (Standard Occupational Classification) List, which currently enumerates 1300 roles. Future refinement of this list can further optimize the I-RBAC system, and the authors plans to test the model on an even larger scale and in varied scenarios.

3. RESEARCH METHODOLOGY

In this section, various access control mechanisms are discussed. They are Role-based access control, Attribute-based access control, Mandatory access control, Discretionary access control, Rule-based access control, distributed RBAC, Cloud optimized RBAC and Attribute-based encryption model.

Discretionary Access Control (DAC):

Discretionary Access Control (DAC) is an access paradigm where resource owners have the autonomy to specify which users can access their resources and the types of operations allowed. Commonly observed in file systems, DAC's flexibility empowers users to manage permissions based on user identities or group affiliations. However, this model has several disadvantages. Firstly, it can inadvertently introduce security vulnerabilities if users grant permissions too liberally. Secondly, in larger systems, maintaining consistent and accurate permissions becomes a complex challenge. Lastly, DAC can lead to "permission creep," where users accumulate unnecessary permissions over time, increasing potential exposure to security breaches.

Mandatory Access Control (MAC):

Mandatory Access Control (MAC) operates under a central authority, establishing strict security classifications (e.g., Top Secret, Confidential) for resources. Users receive security clearances, and their interactions with resources are governed by these classifications. Common in high-security environments like military systems, MAC prioritizes stringent security protocols. However, its disadvantages include reduced flexibility, as users can't alter their access levels even if their tasks demand it. The rigid nature of MAC can impede day-to-day operations and collaboration. Additionally, setting up and maintaining the classification structure can be intricate, potentially leading to administrative challenges.

Rule-Based Access Control:

Rule-Based Access Control (RBAC) centers on a set of predefined rules that dictate what operations users can and cannot perform on a system's resources. Unlike role assignments, these rules consider specific conditions or contexts, such as time-based restrictions. While RBAC offers a more dynamic way to manage access based on evolving conditions, its disadvantages are noteworthy. Crafting an exhaustive set of rules can become complex, especially for large systems with varied user interactions. Misconfiguration

or overlooking a scenario can inadvertently introduce security loopholes. Additionally, constant monitoring is needed to ensure that the rules remain relevant, adding to the administrative burden. Over-reliance on rules without considering user roles or attributes can lead to inflexible systems that resist efficient workflow changes.

Role-Based Access Control:

Role-Based Access Control (RBAC) organizes users based on their roles within an organization, and permissions are assigned to these roles rather than individual users. This approach streamlines access management, especially in large entities, by categorizing users with similar functions under a single role. However, RBAC has its shortcomings. One major disadvantage is the potential for "role explosion," where slight differences in job functions might necessitate the creation of many granular roles, complicating management. Additionally, RBAC might not always account for exceptional cases where a user needs access outside their designated role. Over time, this can lead to "role creep" where users accumulate roles and the associated permissions, heightening security risks. Moreover, the static nature of roles can sometimes be ill-suited for dynamic environments that require more adaptable access controls.

Attribute-Based Access Control:

Attribute-Based Access Control (ABAC) hinges on the attributes of users, resources, and environmental conditions to make access decisions. This model offers a high degree of granularity, using a combination of attributes (e.g., age, department, location) to determine access rights dynamically. While ABAC provides a more adaptable and fine-grained approach compared to other models, it isn't without pitfalls. Configuring an ABAC system can be intricate due to the vast number of potential attribute combinations, posing challenges in ensuring comprehensive coverage without loopholes. Additionally, maintaining the integrity and accuracy of attribute data is vital; any inaccuracies can lead to erroneous access determinations. Lastly, the computational overhead might be higher in ABAC, especially in systems with numerous attributes and complex policies, possibly affecting system performance.

Distributed RBAC (dRBAC):

Distributed Role-Based Access Control (DRBAC) extends the principles of RBAC across distributed systems or multiple domains. In DRBAC, access control policies and roles are coordinated across a network of interconnected systems, facilitating centralized access management for decentralized environments. This is particularly valuable for large organizations with geographically dispersed operations. However, DRBAC comes with its own set of challenges. Synchronizing roles and permissions across multiple systems can be complex and can introduce inconsistencies if not properly managed. There's also the potential risk of a single point of failure; if the central access control mechanism is compromised, it could have widespread implications. Additionally, ensuring timely updates and role changes across all nodes in a distributed environment can be resource intensive. Lastly, integrating legacy systems or those with distinct security frameworks into a DRBAC model can be challenging and may require significant modification.

Cloud optimized RBAC (coRBAC):

Cloud Optimized Role-Based Access Control (CORBAC) tailors the principles of RBAC for cloud environments, aiming to enhance access management in scalable, on-demand cloud infrastructures. In CORBAC, roles and permissions are designed to cater to the dynamic and flexible nature of cloud services, ensuring seamless integration with cloud-specific features such as elasticity and multi-tenancy. However, while CORBAC offers advantages tailored for cloud platforms, it also brings about unique challenges. Given the distributed nature of cloud services, maintaining consistency in role definitions and permissions across various cloud nodes can be intricate. Data privacy concerns emerge, especially when access control data is stored off-premises, potentially in shared or multi-tenant environments. Integrating CORBAC with existing on-premises RBAC systems can lead to compatibility issues. Furthermore, as with all cloud services, there's a dependency on the cloud provider's uptime and security measures, which might not always align with an organization's specific needs or standards.

Attribute-Based Encryption (ABE):

Attribute-Based Encryption (ABE) is a form of public key cryptography in which the secret key of a user and the ciphertext are dependent upon attributes. In ABE, decryption becomes possible when a user's key matches certain attributes related to the encryption. This allows for more granular control in data access, as policies can be set based on user attributes rather than identities. However, ABE comes with its challenges. The computational overhead increases as the number of attributes grows, potentially slowing down encryption and decryption processes. Managing and updating attributes, especially in dynamic environments, can be complex and may pose scalability issues. Revoking access or changing attributes might necessitate re-encryption of data, leading to potential inefficiencies. Moreover, defining and standardizing attributes across an organization can be challenging, making the initial setup and governance of an ABE system intricate. Lastly, ensuring robustness against collusion attacks, where multiple users combine their attributes to decrypt information they shouldn't access, remains a critical concern.

4. PROPOSED MODEL

Compared to all models, RBAC and ABAC are most common and reliable techniques. However, they suffer from flexibility and simplicity. Therefore, in order to overcome their individual disadvantage, both models could be combined to give more secure and robust model. The strengths of two model are combined and thus simplicity and flexibility are offered.

RBAC will provide different roles which will be easier to assign for users and users will be assigned attributes. Some of the roles will also be assigned attributes to give robustness. The attributes should be unique to their roles and the type of users. This approach is preferred because the attributes assigned are fixed. Once the user satisfies the condition for those attributes, then they are assigned the roles. Various functions are used to check assignment of attributes to roles and users.

Algorithm:

Functions: -

- add_role(role)
- assign_role_to_user(role, user)
- assign_role_to_object(role, obj)
- add_object(obj)

- assign_attribute_to_object(attribute, obj)
- assign_attribute_to_role(attribute, role)
- add_attribute(attribute)
- authorized(user, obj)

Checking authorization:

```
if obj in objects:
    obj_roles = objects[obj]
    user_roles = set()
    user_attributes = set()
    for role in roles:
        if user in roles[role]:
            user_roles.add(role)
    for attribute in attributes:
        if user in attributes[attribute]:
            user_attributes.add(attribute)
    common_roles = user_roles.intersection(obj_roles)
    common_attributes=
        user_attributes.intersection(obj_roles)
    if common_roles or common_attributes:
        return True
  return False
```

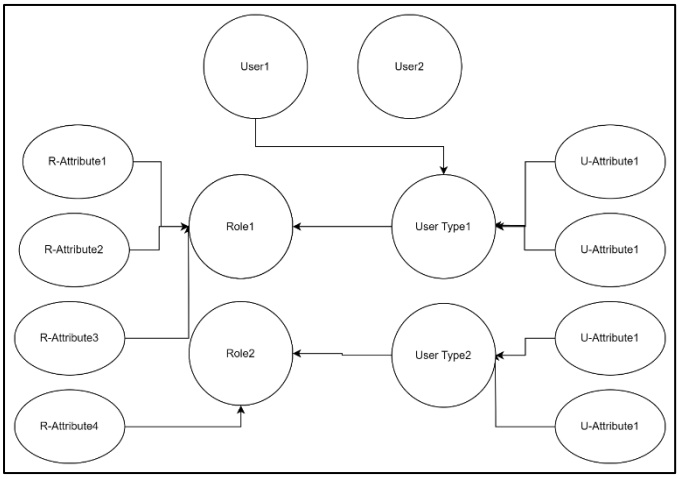

Fig -1: Attributes assignment

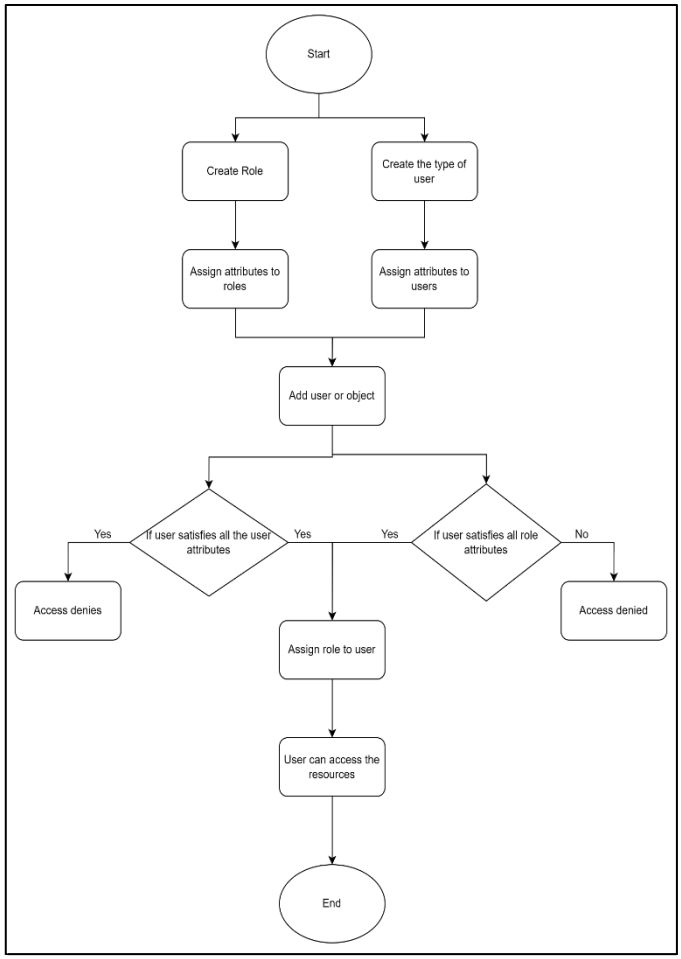

Fig -2: Flow chart for the algorithm

5. CONCLUSION AND DISCUSSION

This new model ensures more robust security by granting access only to users with specific roles, upholding the principle of least privileges. Access control is pivotal for cloud computing, providing essential protection for resources. After analysing existing models and recognizing their advantages and shortcomings, the study underscores the CRABAC's ability to control user data flow and resource usage more effectively by leveraging attribute assignment, ensuring higher security levels not achieved by traditional models.

REFERENCES

1. Ishu Gupta, Ashutosh Kumar Sing, Chung-Nan Lee; Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions, IEEE Access 2022
2. Sara Alayda, Najad.A. Almowaysher, Mamoona Humayn, NZ Jhanjhi; A Novel Hybrid Approach for Access Control in Cloud Computing, International Journal of Engineering Research and Technology 2020
3. Mumina Uddin, Shareeful Islam, Ameer Al-Nemrat; A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control, IEEE Access 2019

4. Mrs. J. Persis Jessintha, Dr. R. Anbuselvi; An Analysis on Access Control Mechanisms in Cloud Environment, International Journal of Engineering Research and Technology 2015
5. Somchart Fugkeaw; A Fine-Grained and Lightweight Data Access Control Model for Mobile Cloud Computing, IEEE Access 2020
6. Jialu Hao, Jian Liu, Huimei Wang, Lingshuang Liu, Ming Xian, Xuemin Shen; Efficient Attribute-Based Access Control with Authorized Search in Cloud Storage, IEEE Access 2019
7. Rubina Ghazal, Ahmad Kamran Malik, Nauman Qadeer, Basit Raza, Ahmad Raza Shahid, Hani Alquhayz; Intelligent Role-Based Access Control Model and Framework using Semantic Business Roles in Multi-Domain Environments, IEEE Access 2019