NATIONAL LAW INSTITUTE UNIVERSITY BHOPAL

Master of Cyber Law and Information Security

BATCH 2024-26

FUNDAMENTALS OF SECURITY ARCHITECTURE, MODELS AND IDENTITY MANAGEMENT

Project Assignment On

"EVOLUTION OF SECURITY MODELS: FROM MAC TO ABAC"

Under the Supervision of

Dr. SATYA PRAKASH

Assistant professor

Ph.D., M.S. C.L.I.S., LL.B.

Submitted By

MEENAKSHI PUNDHIR
2024MCLIS27

I semester

ACKNOWLEDGEMENT

I would like to express my heartfelt appreciation to everyone who supported me throughout my project on "*Evolution of security models: From MAC to ABAC.*"

First and foremost, I am incredibly thankful to Dr. S. Suryaprakash, our Vice Chancellor. His constant support and encouragement helped me tackle challenges and push for excellence in my research.

I am also deeply grateful to Mr. Vivek Bakshi, our Registrar, for his guidance and readiness to assist, ensuring I had the necessary resources and confidence to progress.

A special thanks goes to my professor, Dr. Satya Prakash, whose mentorship was invaluable. His insightful guidance and advice helped keep me focused and significantly enhanced the quality of my work.

I would also like to acknowledge the library staff at the National Law Institute University, Bhopal, for their crucial help in providing access to essential resources, which greatly contributed to the completion of my project.

I truly appreciate the support and encouragement I received from everyone involved. Thank you all.

Meenakshi Pundhir

Roll No. 2024MCLIS27

I Semester

CONTENTS

ABSTRACT

Access control models play a vital role in protecting sensitive information and ensuring that only the right people can access specific resources. As organizations grow and systems become more complex, it's important to have effective mechanisms in place to manage who gets access to what. This paper explores how these models have evolved over time, starting with early approaches like Mandatory Access Control (MAC), which strictly defines permissions, and moving through more flexible systems like Discretionary Access Control (DAC) and Role-Based Access Control (RBAC). The focus is on Attribute-Based Access Control (ABAC), a modern approach that adapts to today's dynamic environments, such as cloud and hybrid systems, providing better security and more control. Key concepts like least privilege, real-time decision-making, and adaptable authorization are also discussed to show how access control continues to advance in response to new challenges.

Keywords: Access Control Models, Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Least Privilege.

CHAPTER 1: INTRODUCTION

Access control is the process of regulating who can access an organization's data, systems, and resources, ensuring that only authorized individuals are granted entry. This system typically involves authentication, where a user's identity is verified (such as through passwords or biometrics), followed by authorization, which assigns specific access rights based on that identity. Many organizations enhance this process with two-factor authentication (2FA) for added security. Additionally, regular audits are conducted to ensure that users have only the necessary access, preventing any potential misuse. Access control covers both physical environments, like office keycard systems, and digital platforms, such as secure logins to devices. It's essential for complying with regulatory standards like PCI DSS, HIPAA, and ISO 27001, which safeguard sensitive information and physical assets. In an era of rising cybersecurity threats, a strong access control system is fundamental to maintaining both security and trust.[1]

Access control aims to minimize the risk of unauthorized access to physical and digital systems, protecting sensitive data like customer information and intellectual property. It is essential for ensuring compliance with security regulations by implementing policies that restrict access to networks, applications, and files. To address this, vendors are moving from single sign-on systems to unified access management, which secures both environments. Access control identifies and verifies users or applications, then grants appropriate access based on credentials. Protocols like LDAP and SAML help authenticate and authorize access to resources. Organizations choose different access control models based on their compliance needs and security requirements.

In the early days of computing, during the 1950s and 1960s, access control focused on physical security for mainframe computers. Multics in the 1960s introduced "rings" for different access levels, paving the way for modern access models. Discretionary and Mandatory Access Control emerged in the 1970s, followed by Role-Based and Attribute-Based Access Control in later decades.

The purpose of this study is to throw light on the evolution of access control models from mandatory access control (MAC) to attribute based access control (ABAC) and emerging technologies in this arena.

[1] 'What Is Access Control? - Network Cybersecurity Systems' (*Fortinet*) <https://www.fortinet.com/resources/cyberglossary/access-control> accessed 30 September 2024.

1.1 REVIEW OF LITERATURE

- ***Pierangela Samarati and others, "Access Control: Policies, Models, and Mechanisms" (2000):*** This research focuses on the importance of access control in safeguarding systems by regulating who can access data and resources according to specific policies. It highlights a structured approach, from defining the rules to creating models and implementing mechanisms that enforce these controls. By separating the rules from the enforcement process, the research shows how systems can adapt more easily, ensuring data remains secure, accessible only to authorized users, while protecting its integrity and availability.
- ***Maile McCarthy and others, "The Definitive Guide to Role-Based Access Control (RBAC)" (2024):*** This work on Role-Based Access Control (RBAC) underscores its efficiency in streamlining access management by assigning permissions according to specific roles. Studies show that RBAC improves security, cuts down administrative efforts, and helps organizations meet compliance requirements. By organizing access around roles, companies can better protect their networks while ensuring flexible and scalable permission management.
- ***Keith Casey, "What Is Attribute-Based Access Control (ABAC)?" (2020):*** Attribute-Based Access Control (ABAC) is gaining recognition for its versatility and security, enabling organizations to regulate access by assessing specific attributes related to users, resources, actions, and the environment. Research highlights ABAC's development and endorsement for enhancing information sharing, especially within federal organizations, positioning it as an effective solution for modern access management issues.
- ***Travis Rodgers, "What is MAC (Mandatory Access Control)?" (2023):*** Mandatory Access Control (MAC) is a security framework that applies established rules to regulate user access to resources, which is particularly important in secure environments like government agencies and healthcare facilities. Studies highlight MAC's strong security features, as it restricts individual users from changing access permissions, thus improving data protection and ensuring regulatory compliance.

1.2 STATEMENT OF PROBLEM

The increasing information security risks and cyber threats have heightened the vulnerability of critical data, access control models have had to evolve to meet these challenges. It's essential to grasp the unique features and functions of each model, particularly from Mandatory Access Control (MAC) to Attribute-Based Access Control (ABAC).

1.3 HYPOTHESIS

The integration of access control models into a broader cybersecurity strategy, along with their continuous monitoring and regular advancements can significantly reduce risks to critical data and information security.

1.4 RESEARCH QUESTIONS

1. How have the principles and frameworks of access control evolved from MAC TO ABAC in response to the changing landscape of cybersecurity threats?
2. What are the differences between Discretionary Access Control (DAC) and Non-Discretionary Access Control (NDAC)?
3. In what way do different access control models work?
4. What are some future strategies and models for improving access control?

1.5 RESEARCH OBJECTIVES

1. To analyse the evolution of access control principles and frameworks from Mandatory Access Control (MAC) to Attribute-Based Access Control (ABAC) in response to contemporary cybersecurity threats.
2. To compare and contrast the features and applications of Discretionary Access Control (DAC) and Non-Discretionary Access Control (NDAC) models.
3. To investigate the operational mechanisms of various access control models and their effectiveness in enhancing information security.
4. To explore innovative strategies and emerging models for improving access control systems in the context of evolving cybersecurity challenges.

1.6 SCOPE AND LIMITATION

This project will examine the development and comparison of various access control models, such as MAC, DAC, and ABAC, and assess future strategies for their improvement. Limitations include a concentration on established models, contextual constraints, and the fast-evolving landscape of

cybersecurity threats, which may influence the findings' applicability. Furthermore, resource limitations may hinder access to particular case studies and data.

1.7 RESEARCH METHODOLOGY

This research has chosen the doctrinal method of research to investigate the topic of evolution of security models: from MAC to ABAC.

CHAPTER 2: ANALYSIS & DISCUSSION.

As cloud-based technologies continue to grow, managing access to sensitive organizational data has become increasingly complex. Businesses that operate across multiple locations now need real-time access to critical information, all while implementing robust security measures to prevent breaches. Access control is a key component of cybersecurity, determining who can access and use specific resources within a system. By limiting access to authorized users, it reduces risks and protects sensitive data, applications, and networks. Proper access control also ensures compliance with data privacy regulations like PCI DSS and HIPAA, lowering the likelihood of data breaches. Following the principle of least privilege, it provides users with only the permissions necessary for their roles, minimizing the chances of unauthorized access. Real-time authorization further enhances security, particularly for organizations with distributed teams, by enabling secure, immediate access to essential resources.

2.1 KEY ELEMENTS OF ACCESS CONTROL

Access control involves several key components: identification, authentication, and authorization.

1.Identification determines who a user is and ensures they are uniquely recognized within the system. This is typically done through user IDs, which track individual activities, and badges, which serve as physical identifiers for access to secure areas.

2.Authentication verifies the user's identity after identification. Common methods include passwords, which should be strong and secure, and biometrics, such as fingerprints or facial recognition, which offer higher security but require specialized equipment. Multi-factor authentication adds an extra layer of security by combining these methods.

3.Authorization defines what a user can access once authenticated. It can be managed through access control lists (ACLs), which assign specific permissions to users, or role-based access control (RBAC), where users are granted permissions based on their role within the organization. ACLs offer flexibility but can be complex, while RBAC simplifies user management but requires careful role definition.[2]

[2] bcsadmin, 'The Three Elements of Access Control' (*BCS Consultants*, 21 September 2023) <https://www.bcsconsultants.com/blog/the-three-elements-of-access-control/> accessed 2 October 2024.

2.3 ACCESS CONTROL PRINCIPLES

1. Accountability and Reliable Input: Accountability in access control ensures that actions can be traced back to individual users, holding them responsible for their activities within the system. Access control decisions must be based on reliable data, with proper user authentication as a prerequisite.

2. Least Privilege: Users should only have the minimal level of access required for their tasks. This principle reduces the risk of accidental or malicious misuse by limiting access rights both statically (in policies) and dynamically (during operation).

3. Separation of Duty: To prevent fraud or abuse, no user should be able to carry out conflicting tasks that would allow them to misuse the system. This principle is enforced through role-based restrictions and historical checks on prior actions.

4. Conditional Authorizations: Access permissions can be contingent on conditions like time, location, or data type. The system must evaluate these factors dynamically, granting or denying access based on specific requirements.

5. Administrative Policies: These policies govern who can modify access control rules. They can be centralized under a privileged user, hierarchical, or ownership-based, depending on the system's structure and needs.

6. Conditional Authorizations: Access permissions can be contingent on conditions like time, location, or data type. The system must evaluate these factors dynamically, granting or denying access based on specific requirements.

7. Multiple Policies and Exceptions: Access control should support both "closed" (deny by default) and "open" (allow by default) policies, allowing for exceptions where specific rules permit or deny access in different situations.

8. Policy Combination and Conflict-Resolution: When multiple policies apply, the system should resolve conflicts, prioritizing denials or specific permissions based on the scenario. This ensures clarity in how rules are applied.[3]

[3] Sabrina De Capitani Di Vimercati, Stefano Paraboschi and Pierangela Samarati, 'Access Control: Principles and Solutions' (2003) 33 Software: Practice and Experience 397.

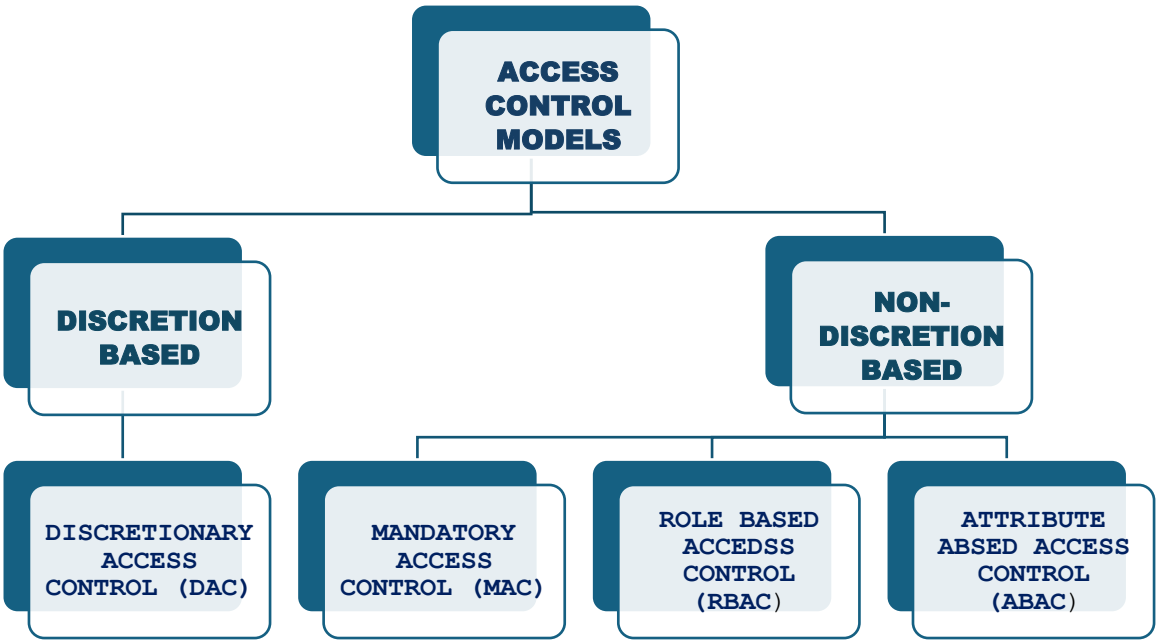

FIGURE 1: *Access Control Models (Types)*

2.4 EVOLUTION OF SECURITY MODELS: FROM MAC TO ABAC.

Access control models have progressed from Identity-Based Access Control (IBAC), which governed access based on user identity, to more sophisticated systems. As managing individual permissions became overwhelming, Role-Based Access Control (RBAC) was introduced, associating access rights with roles. However, RBAC encountered difficulties in multi-domain scenarios, prompting the development of Attribute-Based Access Control (ABAC), where access decisions are based on specific user attributes like clearance levels. These models, collectively known as Authentication-Based Access Control (NBAC).

2.4.1 MANDATORY ACCESS CONTROL (MAC): Mandatory Access Control (MAC) is a security model that enforces a strict set of predetermined rules or labels to control access to resources. These rules are defined by an administrator and enforced by the system, restricting the ability of individual users or resource owners to grant or revoke access to files or objects. This approach differs from models like Discretionary Access Control (DAC), where users have the freedom to manage access to their own data. MAC is mainly employed in highly secure environments such as government institutions, where access is determined by clearance levels, or healthcare settings where patient data sharing needs to be restricted. For instance, in a government system, files might be classified as unclassified, restricted, confidential, secret, or top secret. Every file is assigned a classification label, and when a user requests access, the system compares the security label of the file with the user's clearance to decide if access should be granted. MAC is hierarchical in nature.

This means that users with higher clearance levels automatically have access to lower-level data, according to the enforced rules and labels.[4]

LEVELS OF SECURITY UNDER MAC.

1.Multilevel Security

Multilevel Security (MLS) involves classifying people, information, and systems into different levels of trust and sensitivity. These levels follow a hierarchy: Unclassified → Confidential → Secret → Top Secret. A person's clearance level dictates the highest classification of information they can handle, while a classification level indicates how sensitive information is, reflecting the potential harm if disclosed. "Security level" refers to either clearance or classification level.

The Bell-LaPadula Model proposed by Bell and LaPadula in 1973 for safeguarding confidentiality in time-sharing systems, this widely used model focuses on confidentiality. It has two main rules:

1.No read up: Subjects can only read objects of the same or lower classification.

2.No write down: Subjects can only write to objects of the same or higher classification. This prevents sensitive information from being unintentionally written to lower-security areas, guarding against Trojan horse attacks.

The Biba Model Developed by Ken Biba, this model prioritizes integrity and ignores confidentiality. It uses integrity levels to prevent unauthorized data modification. Key rules include:

1.No write up: Subjects with lower integrity cannot modify higher integrity data.

2.No read down: Higher integrity subjects cannot read lower integrity data. This ensures that data cannot be inappropriately altered by less trusted sources.

2.Multilateral Security

Multilateral Security focuses on restricting access across vertical boundaries, ensuring information separation between entities like competing businesses or intelligence agencies.

The Chinese Wall Model designed by Brewer and Nash for consultancy firms, this model prevents conflicts of interest. It ensures that analysts do not access data from competing clients by enforcing two rules:

[4] Teleport, 'What Is MAC (Mandatory Access Control)? | Teleport' <https://goteleport.com/learn/what-is-mac/> accessed 4 October 2024.

1.Read Rule: A subject can only read data from the same dataset or a conflict-of-interest (CoI) class that has not been accessed before.

2.Write Rule: A subject can only write if they can read the object, and they cannot write to a dataset from a different company. This prevents indirect information flow between competing clients.[5]

FIGURE 2: *Typical clearances under MAC.*[6]

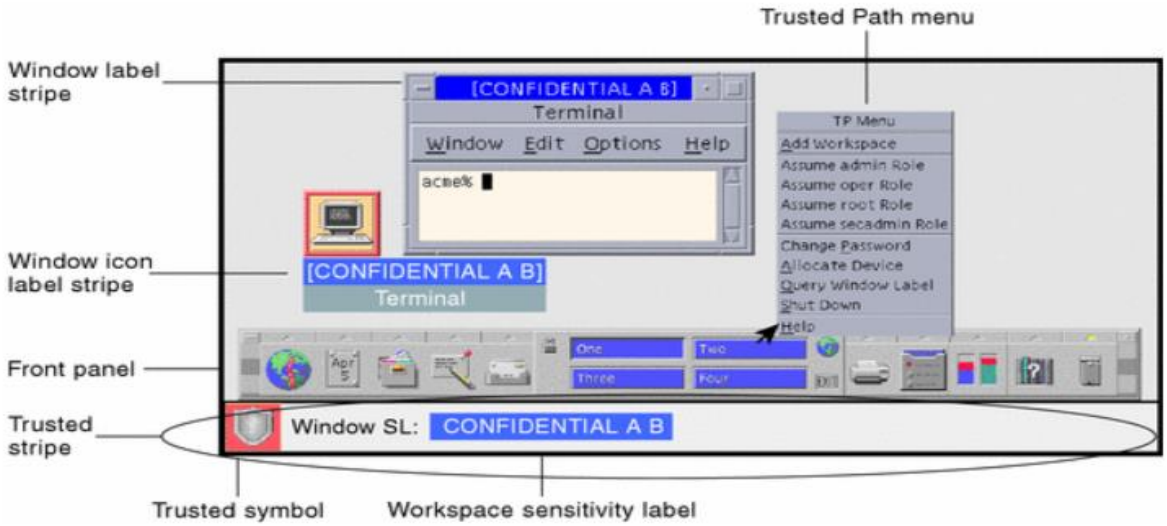

FIGURE 3*: Labelling under MAC.*[7]

2.4.2 DISCRETIONARY ACCESS CONTROL (DAC)

Discretionary Access Control (DAC) is a decentralized model that allows users to manage access to resources. It is commonly found in smartphone applications, Google Docs, and various operating

[5] 'MAC'.
[6] <https://docs.oracle.com/cd/E19109-01/tsolaris8/816-1041/uguide1-32763/index.html> Accessed 4 October 2024.
[7] ibid.

systems, enabling users or user groups (subjects) to control who can access specific resources (objects), such as applications or data. In DAC systems, users can share information and grant access privileges to others. They also have the ability to modify object attributes and determine which attributes are associated with newly created objects, all without needing centralized approval. This flexibility contrasts with Mandatory Access Control (MAC), where access policies are established by a central authority using mechanisms like clearance levels.

DAC relies on two key concepts:

1.Subjects: Users or groups seeking access to resources protected by DAC.

2.Objects: System resources, such as applications or data stored on a network.

Access control in DAC depends on identifying subjects. Users must provide authentication information to verify their identity before the system grants access. The access control system then evaluates whether the subject possesses the necessary rights to access a specific object. DAC systems are primarily classified into two types:

1.Access Control Lists (ACLs): These documents list authorized users, allowing administrators to implement rule-based access for each object. ACLs detail the identities of users and their associated privileges and can be linked to user groups within role-based access control.

2.Capability Systems: Unlike ACLs, these decentralized systems associate access rights directly with the object being accessed. For example, cryptocurrency holders can access their assets only if they possess the corresponding private key, while Imgur users can edit images if they have the unique URL.

Both types of DAC enable object owners to adjust ACLs to regulate access and modify user privileges. For instance, certain groups may have write access, while others may only be permitted to read a database.

Discretionary Access Control (DAC) provides several advantages, making it a popular choice for organizations. Its flexibility allows users to set specific permissions for individual objects, facilitating quick information sharing without the need for complex user profiles or clearance levels. DAC also reduces administrative burdens since object owners manage access, simplifying policy management for administrators. These benefits make DAC ideal for smaller organizations or those handling limited sensitive information.

However, DAC also presents challenges, including security risks, as it is generally less secure than Mandatory Access Control (MAC), potentially exposing systems to malware and privilege creep. The decentralized nature can lead to confusion and inadequate oversight, making it hard for security teams to monitor access to sensitive resources. Additionally, maintaining up-to-date access control lists (ACLs) can become cumbersome as networks grow, and DAC may not provide sufficient protection for highly sensitive data, such as health or financial information.[8]

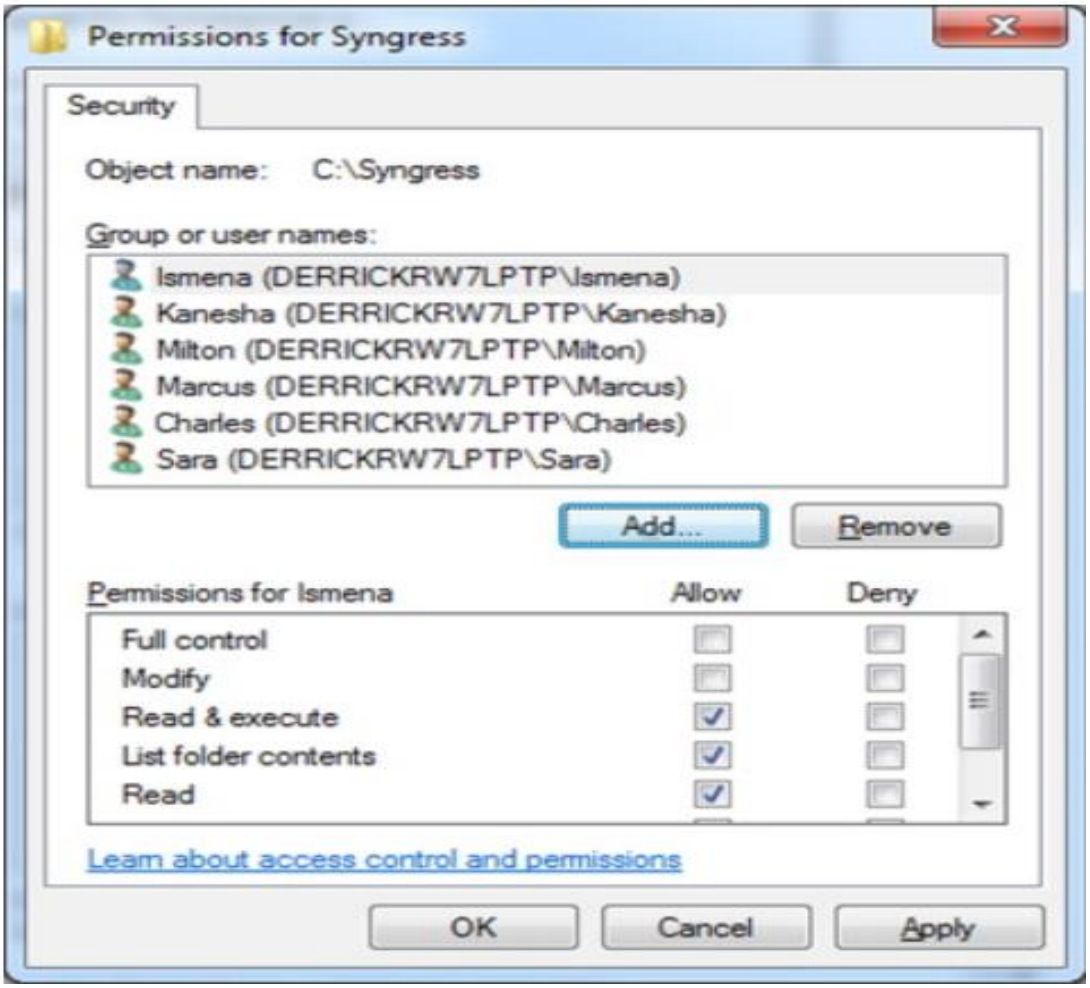

FIGURE 4: *An example of access control list in Windows 7.*[9]

[8] 'What Is Discretionary Access Control (DAC)?' <https://nordlayer.com/learn/access-control/discretionary-access-control/> accessed 5 October 2024.

[9] 'Discretionary Access Control - an Overview | ScienceDirect Topics' <https://www.sciencedirect.com/topics/computer-science/discretionary-access-control> accessed 5 October 2024.

2.4.3 ROLE-BASED ACCESS CONTROL (RBAC)

Role-based access control (RBAC) has been employed for managing access to commercial computer systems since the 1970s, although the initial approaches were often makeshift. It wasn't until 1992 that the American National Standards Institute (NIST) started to formalize RBAC, largely due to the work of researchers *Ferraiolo and Kuhn,* who introduced a foundational paper on the topic. In the following years, particularly throughout the 1990s and early 2000s, the model underwent further development, emphasizing its economic advantages and establishing separation of duties. By 2004, NIST officially recognized RBAC as an industry standard.

Role-based access control (RBAC) is a security model that manages user access to systems based on their specific roles within an organization. This approach ensures that employees can access the data and applications necessary for their job functions while minimizing the risk of unauthorized users accessing sensitive information or carrying out prohibited actions. RBAC also allows for tailored interactions with data, such as granting read-only or read/write access to specific roles, thereby limiting users' ability to execute commands or delete information. Implementing an effective RBAC system is vital for large organizations that work with numerous contractors, vendors, and customers. It helps protect essential data, enhances operational efficiency, and facilitates compliance with regulatory requirements.

The RBAC Framework

RBAC consists of three main types of access control: core, hierarchical, and constrained.

1. **Core RBAC:** The core model encompasses the fundamental aspects of any RBAC system. While it can function on its own, it also serves as the foundation for the hierarchical and constrained models. Core RBAC is governed by three primary rules:

- *Role Assignment:* A user can perform an action only if they have been assigned a role.
- *Role Authorization:* The user’s active role must be approved.
- *Permission Authorization:* A user can only perform actions that are permitted for their current role.

2. **Hierarchical RBAC:** This model allows for a structured hierarchy of roles, offering more precise control over permissions according to the organizational structure.
3. **Constrained RBAC:** This variation introduces the concept of separation of duties into the core model, divided into static and dynamic categories:

- **Static Separation of Duty (SSD):** A single user is prohibited from holding conflicting roles, which helps ensure that one individual cannot both initiate and approve a transaction.
- **Dynamic Separation of Duty (DSD):** A user can hold conflicting roles but may not function in both roles simultaneously during a session. This model helps mitigate internal security risks by enforcing rules like the two-person rule, which requires two different users to authorize a particular action.

Role-Based Access Control (RBAC) provides several advantages, including increased security by limiting user access to essential permissions, simplified workflows that lessen reliance on IT for access requests, and better compliance through effective access tracking. However, it also comes with challenges, such as the requirement for comprehensive business understanding to accurately define roles, possible inflexibility in adjusting to evolving organizational demands, and the risk of "role explosion," where an overabundance of roles creates management difficulties and potential security vulnerabilities.[10]

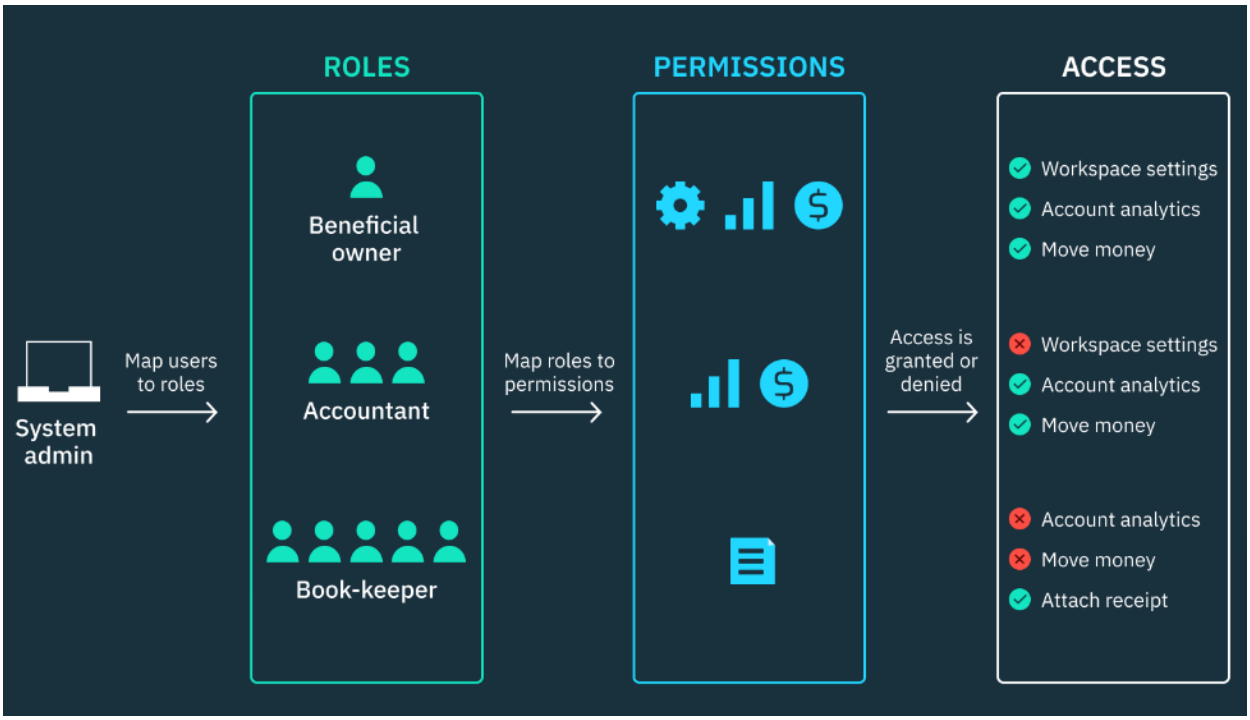

FIGURE 5: *Role-based access control.*[11]

[10] 'The Definitive Guide to Role-Based Access Control (RBAC) | StrongDM' <https://www.strongdm.com/rbac> accessed 5 October 2024.
[11] 'What Is Role-Based Access Control (RBAC)?' <https://stytch.com/blog/what-is-rbac> accessed 5 October 2024.

2.4.4 RISK BASED ACCESS CONTROL (RBAC)

Risk-Based Access Control (RBAC) is an adaptive approach to managing user access, focusing on real-time risk evaluation rather than relying solely on predefined roles or attributes. Instead of using fixed rules, it looks at the situation surrounding an access request, considering factors like user behaviour, location, and device security to make decisions. The core of RBAC is its ability to assess risks dynamically. Every access attempt is evaluated by analysing multiple factors, which collectively contribute to a risk score. For instance, a user trying to log in from their usual office computer might be considered low-risk, while the same user trying to access the system from an unrecognized device in a foreign country could trigger a higher risk level. Risk-based systems continuously monitor and adjust access rights based on these contextual factors.

Various real-time factors are taken into account when determining risk, including:

1. **User behaviour:** Monitoring for unusual activities, such as login attempts at odd hours or from locations not typically associated with the user.
2. **Location:** The geographic location of the access attempt is checked, especially if it originates from unfamiliar or high-risk regions (e.g., logging in from a known cybercrime hotspot may trigger more scrutiny).
3. **Device security:** The system verifies whether the device being used is recognized, secure, and up-to-date. Devices with outdated software or without security patches are flagged as high risk.
4. **Network conditions**: Access attempts over secure, private networks are considered less risky compared to public or unsecured Wi-Fi networks.
5. **Data sensitivity:** The system evaluates the sensitivity of the data being accessed. For instance, accessing confidential company files or financial records might require a lower risk score compared to accessing less critical information.

Risk-Based Access Control (RBAC) adapts access rights in real time based on assessed risk levels. In low-risk scenarios, users can access resources without extra checks, while medium-risk situations may prompt multi-factor authentication (MFA). High-risk cases could restrict access to certain files, and very high-risk situations may lead to a complete denial of access. The system calculates a risk score based on factors like location, behaviour, and device security, continuously updating it as conditions change. Additionally, modern RBAC systems use automation and

machine learning to analyse past behaviours, enabling proactive security measures to address potential threats before they escalate.

2.4.5 ATTRIBUTE BASED ACCESS CONTROL (ABAC)

Attribute-Based Access Control (ABAC) is an authorization model that determines access based on specific attributes or characteristics instead of predefined roles. The main goal of ABAC is to safeguard resources like data, network devices, and IT systems from unauthorized users or actions—essentially those that lack the "approved" attributes outlined in an organization's security policies. In the last decade, ABAC has gained traction as a logical access control method, evolving from earlier systems like access control lists and Role-Based Access Control (RBAC). In 2011, the Federal Chief Information Officers Council recognized the importance of ABAC in enhancing access control frameworks for federal organizations and endorsed it as the recommended model for safely sharing information.

Attribute-Based Access Control (ABAC) is a system that manages access to resources based on various attributes related to the subject (the user), the resource (the asset), the action (what the user wants to do), and the environment (the context of the access request).

- ***Subject:*** This is the user trying to gain access, characterized by attributes such as their ID, job role, and security clearance, usually pulled from HR systems or authentication methods.
- ***Resource:*** This refers to the asset the user wants to access, including details like its creation date, owner, and sensitivity level. For instance, in online banking, the specific resource could be identified by the account number.
- ***Action:*** This describes the specific operation the user intends to perform, such as "read," "edit," or "delete."
- ***Environment:*** This encompasses the overall context surrounding the access request, considering factors like the time of the request, the user's location, and the security of their device.

"Whenever an access request happens, the ABAC system analyses attribute values for matches with established policies. As long as the above policy is in place, an access request with the following attributes should grant access:

Subject's "job role" = "communications"

Subject's "business unit" = "marketing"

Action = "edit"

Resource “type” = “media strategy document”

Resource “business unit” = “marketing”[12]

ABAC evaluates these attributes against established rules to decide whether to grant access. For example, a policy might allow users in certain job roles to access specific documents. This approach allows for flexible and precise control over access permissions based on a variety of attribute combinations.

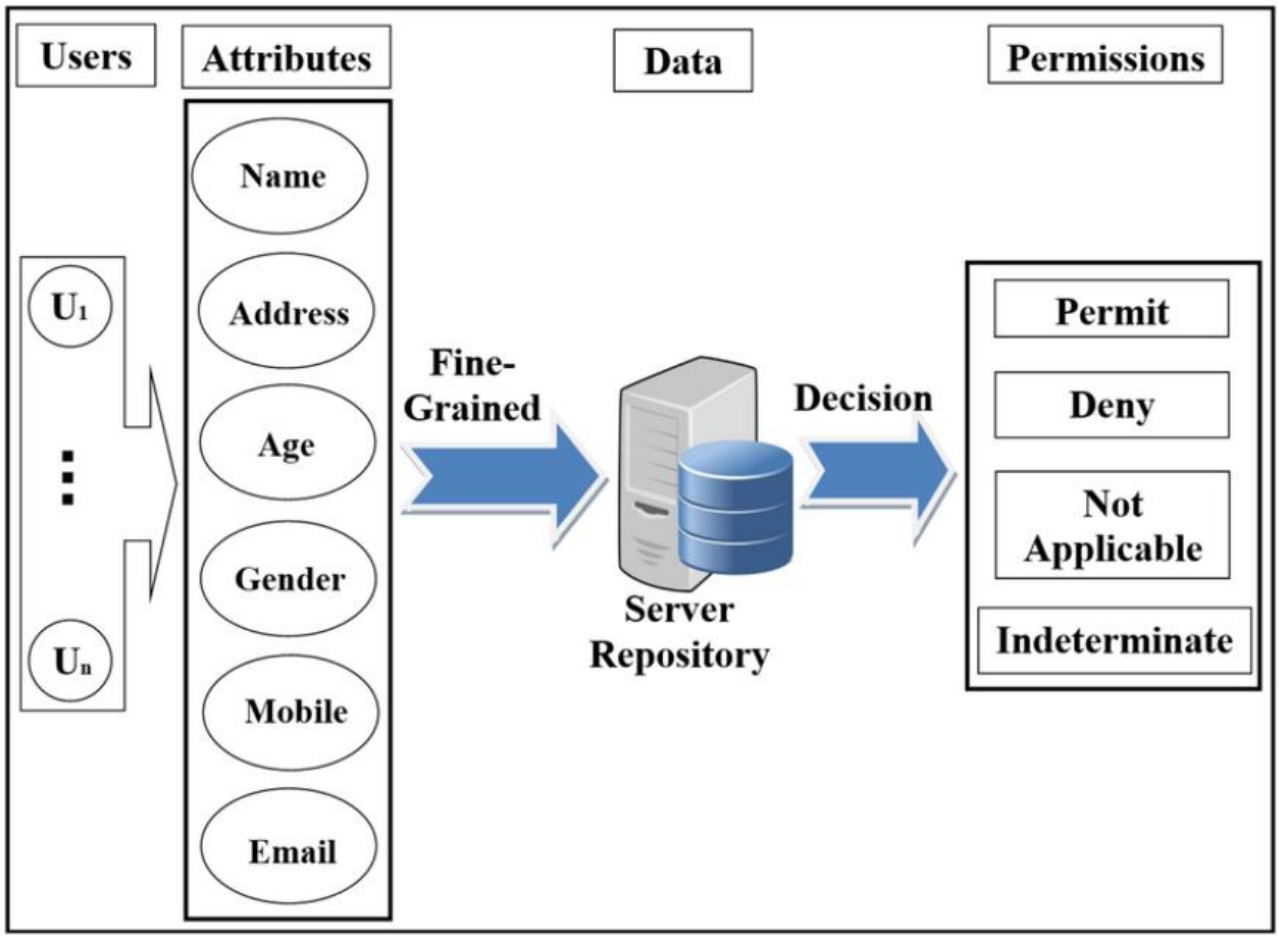

FIGURE 6*: Attribute based access control (ABAC)*[13]

[12] ‘What Is Attribute-Based Access Control (ABAC)?’ <https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/> accessed 6 October 2024.

[13] ‘Scheme of Attribute-Based Access Control (ABAC) Model.’ (*ResearchGate*) <https://www.researchgate.net/figure/Scheme-of-attribute-based-access-control-ABAC-model_fig2_332732675> accessed 6 October 2024.

CHAPTER 3: CONCLUSION AND SUGGESTIONS.

Access control is essential for safeguarding sensitive information by ensuring that only authorized individuals can access vital resources. This study examines various access control models, including Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Risk-Based Access Control, and Attribute-Based Access Control (ABAC). Each model addresses unique security challenges in today's complex IT environments, especially with the growth of cloud technologies. By implementing principles such as least privilege and separation of duty, organizations can enhance their security. Ultimately, an effective access control strategy not only protects against breaches but also fosters accountability and trust in a dynamic cybersecurity landscape.

Some suggestions for futuristic security models based on the research work done for this project are as follows:

1. **Multi-Factor Authentication (MFA):** MFA has evolved into a cornerstone of access security by providing innovative and user-friendly mechanisms, combining passwords, biometric data, and one-time codes sent to personal devices.
2. **Zero Trust Security Model:** The Zero Trust model operates on the principle that threats can arise from both outside and inside the network. The motto is "*never trust, always verify*," which ensures that access is granted only after thorough checks.
3. **Blockchain for Secure Access Management:** Blockchain technology can revolutionize how we manage identity verification and enhance transparency by creating decentralized and tamper-resistant records of who has access to what
4. **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML can analyse user behaviours to identify unusual activities and potential security threats. By using these technologies, access controls can adapt in real-time, adjusting permissions based on current risk assessments to bolster security further.
5. **Context-Aware Access Control:** Context-aware systems take into account various factors like a user's location, device security, and the time of access to make informed decisions about granting access. This ensures permissions are only given when all security conditions are satisfied.

BIBLIOGRAPHY

1. bcsadmin, 'The Three Elements of Access Control' (*BCS Consultants*, 21 September 2023) <https://www.bcsconsultants.com/blog/the-three-elements-of-access-control/> accessed 2 October 2024

2. De Capitani Di Vimercati S, Paraboschi S and Samarati P, 'Access Control: Principles and Solutions' (2003) 33 Software: Practice and Experience 397

3. 'Discretionary Access Control - an Overview | ScienceDirect Topics' <https://www.sciencedirect.com/topics/computer-science/discretionary-access-control> accessed 5 October 2024

4. 'MAC'

5. 'Scheme of Attribute-Based Access Control (ABAC) Model.' (*ResearchGate*) <https://www.researchgate.net/figure/Scheme-of-attribute-based-access-control-ABAC-model_fig2_332732675> accessed 6 October 2024

6. Teleport, 'What Is MAC (Mandatory Access Control)? | Teleport' <https://goteleport.com/learn/what-is-mac/> accessed 4 October 2024

7. 'The Definitive Guide to Role-Based Access Control (RBAC) | StrongDM' <https://www.strongdm.com/rbac> accessed 5 October 2024

8. 'What Is Access Control? - Network Cybersecurity Systems' (*Fortinet*) <https://www.fortinet.com/resources/cyberglossary/access-control> accessed 30 September 2024

9. 'What Is Attribute-Based Access Control (ABAC)?' <https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/> accessed 6 October 2024

10. 'What Is Discretionary Access Control (DAC)?' <https://nordlayer.com/learn/access-control/discretionary-access-control/> accessed 5 October 2024

11. 'What Is Role-Based Access Control (RBAC)?' <https://stytch.com/blog/what-is-rbac> accessed 5 October 2024

12. <https://docs.oracle.com/cd/E19109-01/tsolaris8/816-1041/uguide1-32763/index.html> Accessed 4 October 2024