Journal of Information Systems and Informatics

Vol. 6, No. 3, September 2024 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

DOI: 10.51519/journalisi.v6i3.863 Published By DRPM-UBD

Enhancing Network Security in Mobile Applications with Role-Based Access Control

Ezichi Mpamugo[1] , Godwin Ansa[2]

[1,2]Department of Computer Science, Akwa Ibom State University, Nigeria
Email: [1]mpamugo.ezichi@abiastateuniversity.edu.ng , [2]godwinansa@aksu.edu.ng

Abstract

In today's dynamic networking environment, securing access to resources has become increasingly challenging due to the growth and progress of connected devices. This study explores the integration of Role-Based Access Control (RBAC) and OAuth 2.0 protocols to enhance network access management and security enforcement in an Android mobile application. The study adopts a waterfall methodology to implement access control mechanisms that govern authentication and authorization. OAuth 2.0, a widely adopted open-standard authorization framework, was implemented to secure user authentication by allowing third-party access without exposing user credentials. Meanwhile, RBAC was leveraged to streamline access permissions based on predefined user roles, ensuring that access privileges are granted according to hierarchical role structures. The main outcomes of this study show significance towards the improvements in security enforcement and user access management. Specifically, the implementation of multi-factor authentication, session timeout mechanisms, and user role-based authorization ensured robust protection of sensitive data while maintaining system usability. RBAC proved effective in controlling access to various system resources, such as database operations which was presented in scenario of physical access to doors, while OAuth 2.0 provided a secure communication channel for authentication events. These protocols, working in tandem, addressed key issues like unauthorized access, data integrity, and scalability in network security policy enforcement. This research deduces that combining RBAC and OAuth 2.0 protocols in mobile applications enhances security posture, simplifies access management, and mitigates evolving threats.

Keywords: Role-Based Access Control (RBAC), OAuth 2.0, Network Security Access Management, Multi-Factor Authentication, Authorization Protocols

1. INTRODUCTION

Network Access Control (NAC) serves as a security measure that imposes regulations on devices seeking network entry, thus enhancing network transparency and mitigating potential security threats [1]. NAC restricts network resource availability solely to endpoint devices and users who align with a predetermined security protocol. The NAC mechanism has the ability to disallow entry to noncompliant devices, impound them in a confined zone, or allocate limited access to computing assets. This effectively safeguards the network against potential adulteration by insecure nodes [2].

NAC solutions enable organizations to exercise authority over network access, featuring functionalities like managing security policies by creating profiles and enhancing transparency, offering guest network access, and conducting security posture assessments [3]. Consequently, the role of NAC in the realm of enterprise security extends to the management of security policies, which is a pivotal component. It curtails network resource accessibility to endpoint devices and individuals adhering to a specified security protocol. A holistic security policy encompassing privacy and security prerequisites is imperative for mitigating the challenges. In this domain, there exists a demand for continued exploration and enhancement of policy methodologies and strategies within the scope of NAC where security policy management plays a crucial part.

In Network Access Control, the significance of Security Policy Management lies in its pivotal role of simplifying the creation and implementation of security policies [4]. Security policies are the custodians of network integrity and safety, dictating regulations for network entry, internet connectivity, device and service adjustments, and other crucial aspects. Yet, the effectiveness of these rules becomes evident only when they are put into action. Therefore, Network Security Policy Management (NSPM) serves as the backbone, aiding organizations in maintaining compliance and safeguarding their assets by ensuring that their policies are streamlined, coherent, and actively upheld [5]. Hence, the application of security policy management to enforce network access control entails the adoption of measures to oversee and protect the access to organization network infrastructures. It is imperative for organizations to safeguard themselves against unauthorized access, malware infiltrations, data breaches, and various security risks. This can be achieved by implementing a blend of technological tools and administrative strategies, guaranteeing the network's security and adherence to regulatory standards.

Nevertheless, this study addresses specific challenges in the domain of mobile network security, focusing on the vulnerabilities inherent in modern mobile environments and the complexities associated with securing network access. One of the critical issues is the need for a robust mechanism to enforce network access control in a mobile context, where devices and users frequently interact with sensitive resources across diverse and potentially insecure networks [22]. Traditional Network Access Control (NAC) systems, though effective in restricting access based on security policies, often face limitations in mobile environments due to the dynamic nature of device mobility, varying security barriers, and the growing sophistication of mobile-based cyber threats [23]. This study tackles these challenges by exploring how NAC systems can be optimized and enhanced through the application of Role-Based Access Control (RBAC) and OAuth 2.0 in mobile network security. The contribution of this research lies in advancing the implementation of RBAC and OAuth 2.0 for mobile security. This study seeks to fill that gap by tailoring RBAC to meet the dynamic security demands of mobile networks, ensuring that only authorized users and devices can access network resources.

1.1 Background

Networks are in a constant state of evolution, albeit at varying rates. The approach to managing these networks has also undergone changes over time. An integral aspect of network management involves safeguarding against alterations that could adversely affect the network's security stance. Consequently, in the face of a growing array of devices connecting to corporate networks, it is crucial to establish a resilient and streamlined implementation of network access control through the management of security policies. This entails tackling the surge in mobile and computing devices, along with the accompanying security challenges they introduce [6]. Furthermore, the integration of network access control with various security measures, the automation of incident response, and the guarantee of scalability and adaptability in policy management are imperative to adeptly confront evolving threats and the changing demands of the organization [7].

Nevertheless, navigating these challenges hinges significantly on formulating and executing effective security measures. As indicated by the National Center for Education Statistics (NCES), security policies are instrumental in governing access, safeguarding information, and fortifying systems. It is imperative that these policies stem from a thorough risk assessment, offering a precise understanding of an organization's unique security requirements [8]. Although, enforcing network access control via security policy management poses intricate challenges, necessitating all-encompassing security policies, approaches founded on risk assessment, and the deployment of effective enforcement mechanisms. These measures are imperative to tackle the dynamic outlook of network security threats.

1.1.2 Network Access Control

NAC is a mechanism that act as a computer networking remedy by employing a suite of protocols to articulate and execute a strategy detailing the process of securing of an entry to network endpoints by devices during their initial endeavor to connect to the network [9]. The core purpose of NAC solutions is to validate that solely sanctioned and compliant devices gain entry to the network, thereby fortifying the overall security of the network infrastructure. Also, Administrators overseeing networks employ NAC solutions to oversee and govern computing devices, verifying adherence to the specific security prerequisites established by the corporation. Prior to allowing access to corporate network assets, devices undergo updates encompassing operating system service packs, patches, antivirus and antispyware updates, along with necessary software patches [10]. Within the realm of NAC mechanisms, there exist two distinct evaluation facets: authentication of users and scrutiny of device compliance. The structural framework of NAC solutions encompasses functions such as authentication (focused on identity verification), endpoint compliance, remediation processes, and policy enforcement. These elements collectively validate both the identity of the user and the security status of host devices as prerequisites for granting access to the network. Nevertheless, the indispensability of NAC solutions lies in their ability to enforce security protocols and guarantee the alignment of devices with the security prerequisites set by corporations.

1.1.3 Kinds of Network Access Control

Network Access Control (NAC) serves as a strategic approach to enhance the security, transparency, and administration of a private network. It regulates the accessibility of network assets, permitting entry exclusively to endpoint devices and users adhering to a specified security protocol. There are two types of NAC:

a) Pre-Admission NAC

Pre-entry Network Access Control (NAC) stands as a security protocol that assesses access endeavors prior to permitting entry into a network. By implementing NAC policies in advance of device access, it guarantees that only sanctioned devices and users who adhere to security protocols gain admission [11]. This specific form of NAC plays a pivotal role in upsetting unauthorized access and upholding the integrity of network security. It empowers organizations to stipulate prerequisites for access, such as adherence to security protocols, prior to allowing entry into the network. Typically integrated at either the data link (layer two) or network layer (layer three) of the open standards interconnection model, pre-admission NAC involves the evaluation, validation, and admission of users as they attempt to connect with corporate networks everything unfolding before users gain actual access [12]. This proactive strategy aids organizations in mitigating the potential for security breaches, ensuring that only devices that comply with regulations and possess authorization gain network access. The significance of pre-admission NAC extends to maintaining the security, transparency, and access control of an exclusive network. It introduces automated functionalities that streamline the authentication and authorization processes, thereby reducing the time and associated expenses. Through the implementation of pre-admission NAC, organizations can exercise effective control over network access, bolstering overall security measures [13].

b) Post-Admission NAC

Post-Access Network Access Control (NAC) emerges as a pivotal element in ensuring network security, encompassing the re-verification of users and devices subsequent to their initial entry into the network. This feature holds significance due to the potential shifts in a device's security status following network access, and the device's conduct within the network might warrant imposition of restrictions [14]. The Post Admission Network Access Control is another method for implementing NAC that involves the deployment of a dedicated appliance tasked with enforcing comprehensive policies dictating the permissible actions of devices seeking entry into the network. Situated strategically between access switches and distribution switches, these post-access NAC devices execute a blend of internal firewalling and intrusion prevention measures [15]. Their functionality extends to discerning instances where endpoints seek access to unauthorized resources and promptly taking measures to curtail such access.

1.1.4 Security Policy Management

Security policies management is an indispensable facet of information security, encompassing the creation, execution, and reinforcement of protocols and guidelines aimed at safeguarding an organization's information assets [16]. The management of security policies encompasses a diverse set of actions. These include the careful selection of policy components, the drafting of policy content, the presentation of the draft to pertinent stakeholders for their input, review, and approval, and the subsequent compilation of the comprehensive security policy document. The team responsible for policy development meticulously chooses specific policy elements tailored to address the unique security requirements of the organization. Following its creation, the policy undergoes scrutiny by relevant stakeholders, inviting their feedback, comments, and eventual approval. The finalized security policy document is then compiled, incorporating the valuable insights garnered from stakeholders during the review process [17]. Nevertheless, overseeing security policies stands out as a essential dimension within information security.

1.1.5 Conceptual framework for Security Policy Management

A structured method for developing and implementing security policies, a conceptual framework for security management policy is a systematic approach aimed at safeguarding an organization's information and systems. It is possible to formulate such a framework by drawing insights from the sources presented in search results [18] hence we present the key components of this framework below;

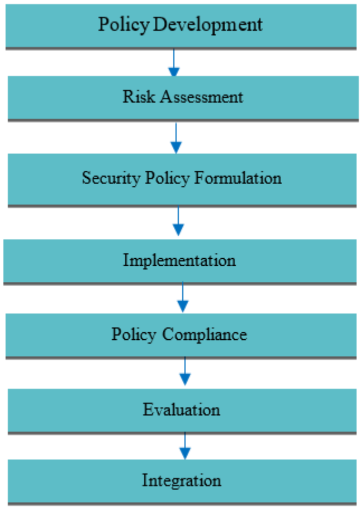


Figure 1. Conceptual framework for Security Policy Management

1. **Policy Development**: This stage requires the recognition of the necessity for a security protocol, delineating its extent, and specifying the policy's goals.
2. **Risk Assessment**: Evaluate the risk environment of the organization, taking into account both internal and external elements, to ascertain the extent of security needed.
3. **Security Policy Formulation**: Derived from the risk evaluation, create a thorough security protocol that tackles the recognized risks and delineates the essential actions to alleviate them.
4. **Implementation**: this design and execute the security protocol, guaranteeing its efficient dissemination to all staff and stakeholders. This might encompass delivering training, offering guidance, and providing resources to assist employees in comprehending and adhering to the policy.
5. **Policy Compliance**: Supervise and uphold adherence to the security protocol, confirming its compliance among all employees and stakeholders. This could include routine audits, inspections, and assessments of the policy's efficacy.
6. **Evaluation:** Consistently assess the efficacy of the security protocol and implement essential updates or revisions in response to shifts in the organization's risk environment, technological progress, and regulatory demands.
7. **Integration:** Incorporate the security protocol into other organizational policies, including information systems strategy, IT strategy, and overarching business strategy, to guarantee a unified and thorough approach to managing security.

1.1.6 Network Security Threats

Network security vulnerabilities may emerge from diverse origins, encompassing both internal and external assailments. The significance of internal attacks, despite their potential for substantial losses, is frequently underestimated. Delving deeper into the intricacies of network security threats enables a nuanced evaluation of their risks, facilitating the identification of indispensable defense mechanisms [19].

1.1.7 Types of Network Security Threat

The classification of network security threats predominantly revolves around two primary categories: internal and external attacks.

1) Internal Network Security Threats

Internal dangers can wield substantial influence, impacting both the magnitude and frequency of losses. These perils manifest from diverse origins, including:

a) Unauthorized Access: Gaining entry to sensitive data or systems without proper authorization can result in data breaches and security incidents.
b) Insider Threats: Employees or other individuals with authorized access to confidential information or systems become potential risks if they misuse their privileges or harbor malicious intentions.
c) Inadequate Security Practices: Insufficient security measures, such as feeble passwords, unpatched software, or a dearth of employee training, can give rise to vulnerabilities exploitable by internal threats.

2) External Network Security Threats

External threats encompass malevolent activities directed at a network from an external vantage point. A few prevalent instances include:

a) Viruses and Malware: Nefarious software, encompassing viruses, worms, or ransomware, can permeate a network, instigating damage or disruption.
b) Phishing Attacks: Adversaries employ deceptive strategies, such as phishing emails or counterfeit websites, to deceive users into divulging sensitive information or conferring unauthorized access.
c) Application-Specific Hacks: Attackers may target specialized software or services, exploiting vulnerabilities or deficiencies in their design or implementation.

1.1.8 Key component of Network Security

The CIA Triad serves as a widely embraced framework within information security, representing the core principles of Confidentiality, Integrity, and Availability in figure 2. This framework is strategically devised to assist organizations in formulating security policies and procedures aimed at safeguarding their information systems and data [20].

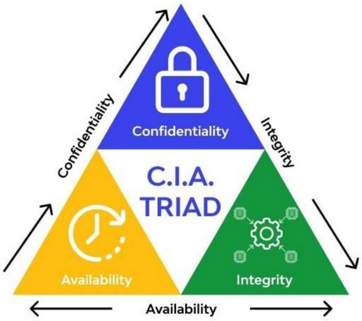


Figure 2. CIA TRIAD Security framework

Nevertheless, we present the three components of the CIA Triad which are:

a) Confidentiality: This centers on shielding confidential data against unauthorized entry. It entails the implementation of measures to restrict access to information, guaranteeing that solely authorized individuals can reach sensitive data.

b) Integrity: Soundness guarantees the reliability, completeness, and accuracy of information. It acts as a deterrent against unauthorized alterations to data, ensuring the preservation of data integrity.

c) Availability: Accessibility ensures that sanctioned users enjoy dependable and prompt access to essential information and systems. This entails the deployment of measures to sustain the continuity and integrity of information systems, encompassing strategies like backups and disaster recovery plans.

From this CIA framework, this study adopts this model in order to achieve the set-out goals of this research.

1.1.9 Security policy management in mobile Application

Effectively managing security policies within mobile applications holds paramount importance for enterprises aiming to safeguard sensitive data and adhere to regulatory mandates [21]. The ensuing insights outline key factors and optimal approaches for the integration of security policies into mobile applications:

a) Develop a mobile security Policy: Craft a comprehensive mobile security policy delineating the regulations and directives governing the utilization of mobile devices and applications within the organizational framework. This policy should encompass aspects like device enrollment, compliance, and data protection.

b) Mandate passcodes: The implementation of robust passcode policies stands as a fundamental measure in fortifying mobile devices. Passcodes play a pivotal role in thwarting unauthorized access to sensitive data and applications.

c) Integrate anti-virus software: Ensure the installation of anti-virus software on mobile devices to provide a defense against malware and various cyber threats.
d) Enforce updates: Make it obligatory for mobile devices and applications to undergo regular updates, safeguarding against security vulnerabilities and ensuring the sustained protection of devices.
e) Restrict rooted devices: Acknowledge the significant security risks posed by rooted devices, necessitating their restriction within the organizational infrastructure.
f) Permit only trusted applications: Authorize solely trusted applications on mobile devices, implementing a Mobile Device Management (MDM) policy to guarantee compliance with established security standards.
g) Deploy Mobile Application Management (MAM): Employ MAM solutions enabling IT administrators to govern the usage of company apps and the storage of company data on devices, ensuring alignment with security policies.
h) Regularly monitor and audit compliance: Consistently scrutinize and audit mobile devices and applications to pinpoint policy infringements and affirm adherence to the mobile security policy.

2. METHODS

In this study, the waterfall methodology is applied to ensure a structured and sequential development process for implementing security measures, particularly Role-Based Access Control (RBAC) and OAuth 2.0 protocols. The Waterfall methodology supports the implementation of these protocols through sequential development step in 2.1.

2.1 Waterfall Methodology Application

2.1.1 Requirement Analysis

a) **OAuth 2.0**: Defined as the standard for secure authorization, OAuth 2.0 facilitates safe third-party access to user resources without exposing credentials. The requirement analysis outlines the need for OAuth 2.0 to handle authentication securely.
b) **RBAC**: Identified as a mechanism for managing user permissions based on roles, RBAC is essential for enforcing access control policies.

2.1.2 System Design

a) **OAuth 2.0**: The system design phase details the architecture for integrating OAuth 2.0, specifying how the protocol will be used to manage authorization flows and secure access.
b) **RBAC**: The design phase includes the RBAC framework, defining roles, permissions, and access control policies to enforce security measures effectively.

2.1.3 Implementation

a) **OAuth 2.0**: Involves coding the authentication process using OAuth 2.0 to ensure secure communication between the client and server.

b) **RBAC**: Implements role-based permissions in the backend, ensuring that users can only access resources according to their assigned roles.

2.1.4 Testing:

a) **OAuth 2.0**: Testing verifies the proper implementation of OAuth 2.0 for secure authorization and error handling.

b) **RBAC**: Tests the enforcement of role-based permissions to confirm that access controls are correctly applied and functioning as intended.

2.2 Choice of Security Protocols and Frameworks

a) **OAuth 2.0**: Chosen for its robust framework that allows secure third-party access to resources without exposing user credentials. It is widely adopted for its security and ease of integration.

b) **RBAC**: Selected for its simplicity and effectiveness in managing user permissions. By assigning roles to users and resources, RBAC provides clear and manageable access control, which is crucial for the study's secure access and policy enforcement requirements.

Nevertheless, we present this study propose framework for Access Control through security policy management in Figure 3.

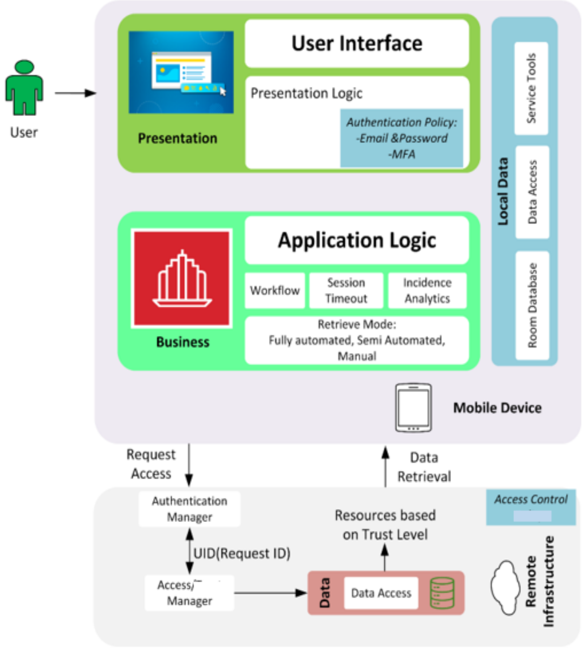


Figure 3. Mobile Network Access Control Through Security Policy

2.3 Description of Key Components the proposed System Framework.

a) **User**: User in the proposed system refers to the Android based mobile user devices. Each User in the system architecture consists of Android mobile device. The functionality of the proposed system can be extended to other platform including desktop and server endpoints. The node provides and endpoint interface to users for interacting with the network application. The interface consists of an Android mobile application.

b) **Authentication/Authorization Policies**: This refers to set of rules and specification on interaction of different components with each other in other to enforce user authentication and authorization in the network. The main components of authentication policy used in this research is the email and password and multi-factor authentication (MFA). This policy outlined the communication protocol used to achieve user authentication and authorization when and during network access. MFA uses Open Authorization (OAuth). The OAuth is one of the most common authentication and authorization protocol used in authentication policy. The OAuth used in the research is known as OAuth 2.0 which enable node to sign up into the network using email/password-based authentication. The OAuth 2.0 also support identity providers such as Google, Facebook, etc. At the completion of the authentication process for each node, a unique identifier (UID) is generated for each authenticated user. This UID is associated with the user account and can be used to manage and secure access to the network resources.

c) **Access Control**: The main aim of access control policy used in this study is to manage and regulate nodes (users) access to resources in order to ensure security, confidentiality, integrity and availability of the resources. As highlighted in the proposed system framework, entities that request access to resources in the network are known as subjects which refers to the user devices. Objects are the resources the users attempt to access. In this research, object incudes reading of user data from database, cloud network services and access to functionalities that requires protection. In addition to entity and object segments, the access control policy used in this work define specific activities each subject(user) is allowed or denied concerning resources. These specific activities are create, read, update and delete (CRUD). The access/trust manager specify the level of access each node have to access resources. The trust manager defined whether a user is allowed to or denied for each action of CRUD on a particular subject. The authentication manager of the access control policy on the other hand specifies rules and conditions under which circumstances access is granted or denied. Such rules include current user location, time of day and user group. Finally, the enforcement mechanism used in the access control policy in this research is based on the role base access control (RBAC) model. In this model, roles represent responsibilities, functions or set of operation with an organization. Each role is assigned with set of permissions that define each action assigned to the role are allowed to perform. In this work, there are two main roles: administrative and regular roles. RBAC adheres to the principle of least privilege, which means that users are granted the minimum level of access necessary to perform one operation or the other. This helps reduce the risk of unauthorized access and potential security breaches. Role authorization is enforced by the trust manager when a user attempts to perform an action within the system. The system checks whether the user's assigned role have the necessary permission to carry out that action. If such permission is denied, an incidence report is made, as outlined in the auditing section of the proposed system.

d) **Session**: Session timeout is a security policy mechanism used to reduce the risk of unauthorized access to network, functionalities or sensitive information in case a user forgets to logout when the session is left unattended to. Session timeout security policy involves automatically terminating a user's session in a network or application after a period of inactivity.

e) **Auditing/Incidence Analytics**: Auditing involves the monitoring and recording of events and activities in a network or within an application.

3. RESULTS AND DISCUSSION

3.1 Authentication Policy Implementation

The authentication policy in this study is implemented on top of the popular Open Authorization 2.0 (OAuth 2.0) protocol. OAuth 2.0 is an open standard authorization protocol that provides a framework for secure third-party access to resources, such as user data, without exposing user credentials. Key components of OAuth 2.0 are shown in Figure 4.

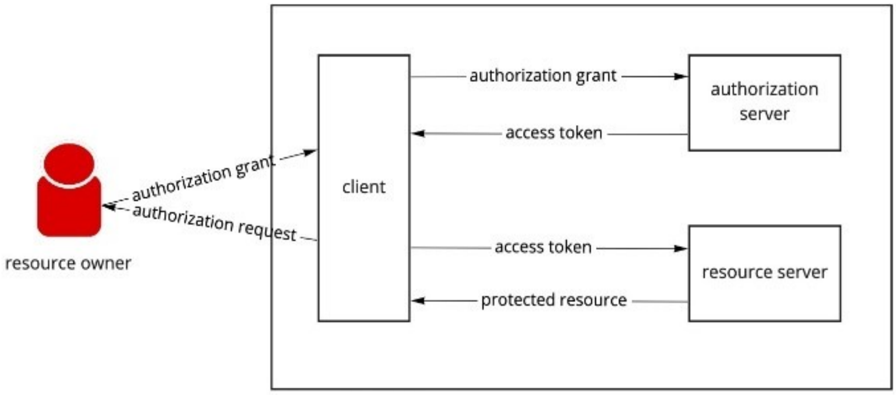


Figure 4. OAuth 2.0 Authentication Security Protocol API

From Figure 4 the key component is described as follow;

a) Resource Owner is the entity that owns the resource. This is typically the end user of the software or application.
b) The Client entity refers to the software of the application that is requesting the resource on behalf of the resource owner. In this research, the client is the android application named Secure Access used to demonstrate the design implementation and enforcement of security policies.
c) The Authorization server is the entity responsible for authentication the resource owner and granting the authorization to the client.
d) The Resource server host the protected resources and is capable of accepting and responding to protected resource requests.
e) Tokens: Two types of tokens are used in conjunction with the OAuth 2.0: Access token and Refresh token. As noted in (2), access token represents the authorization granted to the client. is used to access the protected resources while the refresh token is used to obtain a new access token without requiring re-authentication from the user.

Furthermore, a sequence of diagrams shown in Figure 5 is used to demonstrate the implementation of the authentication security policy based on the OAuth 2.0 framework.

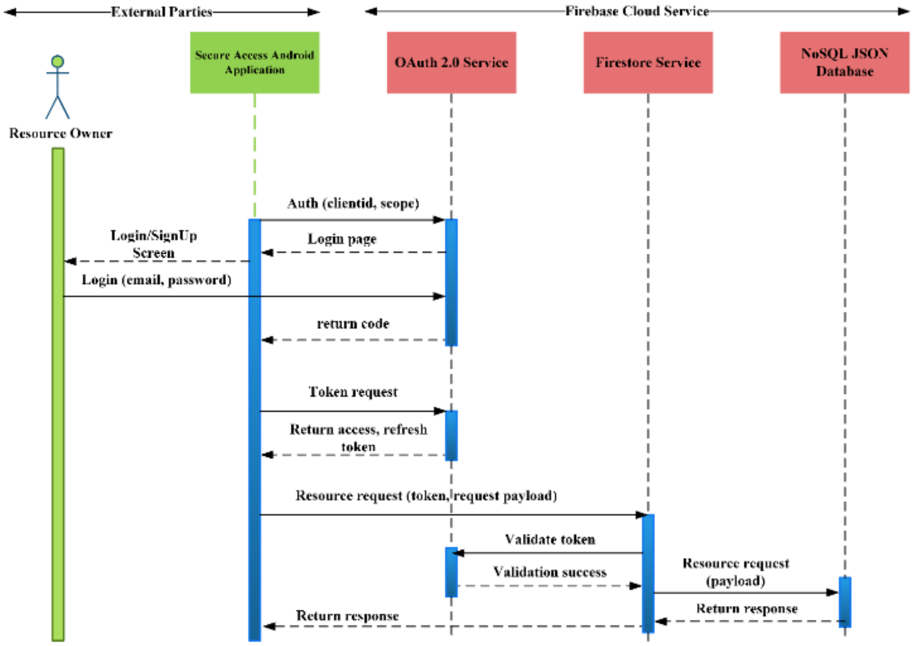


Figure 5. Authentication Policy Implementation

3.2 Role-Based Access Control (RBAC) Design and Implementation

In this study, role-based access control can be demonstrated in the case of secure door access cards. The general architectural framework of RBAC is shown in Figure 6.

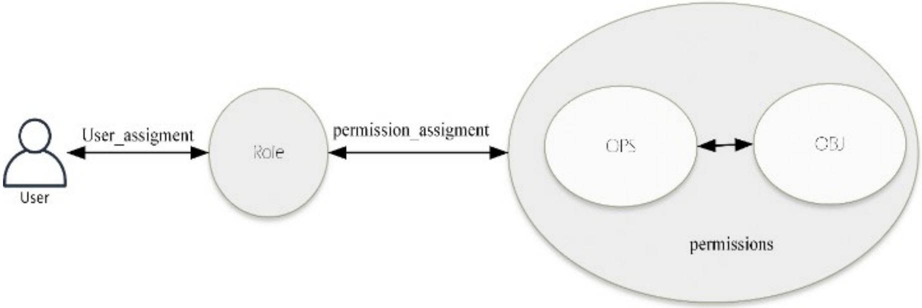


Figure 6. Basic RBAC

As indicated in Figure 7, five elements are associated with RBAC. The five elements are further illustrated in Figure in 6 below.

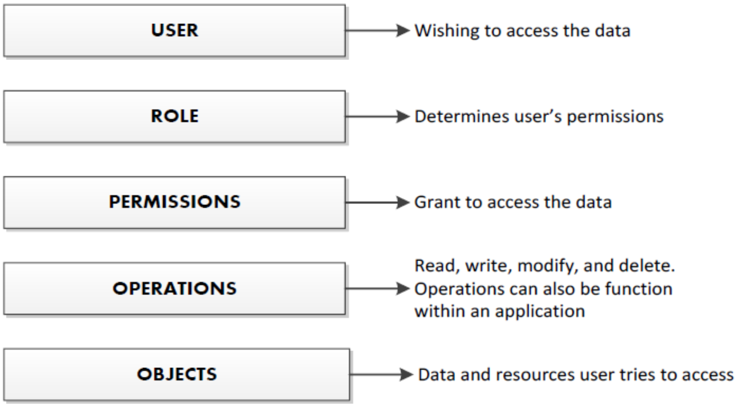

USER
Wishing to access the data
ROLE
Determines user's permissions
PERMISSIONS
Grant to access the data
OPERATIONS
Read, write, modify, and delete. Operations can also be function within an application
OBJECTS
Data and resources user tries to access

Figure 7. Elements of RBAC

In RBAC users are granted access to resources based on the assigned role. When a user is assigned a role, all the privileges and access associated with that role are automatically granted to users with such role. In this research, resources are defined for each role. The resources adopted in this work entails access to database. Four basic operations can be performed on database object which include: create, read, update and delete. The proposed RBAC architecture used in this work is presented in Figure 7.

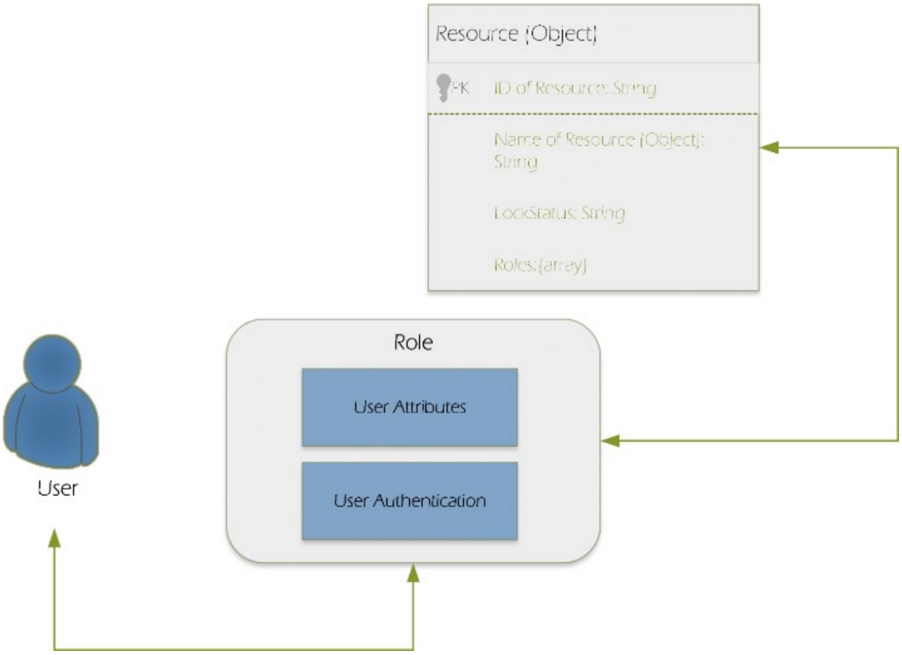


Figure 7. Proposed RBAC Architecture

In Figure 7, a resource object is created as a document in the firestore database. As depicted in the proposed RBAC architecture, each of the resource (object) which is a document in the database is associated with user assigned roles. The user attributes are extracted from the database of users created when a new user registered using the application. The attributes include the first and last name of the user, the unique identification code for each user and the default assigned role. These attributes are used for making requests through the authentication manager and for role assignment.

3.3 User Role-Based Authorization

The authorization of access to resources is based on the user assigned roles and the roles assigned to each of the resources. The role authorization architecture is shown in Figure 8.

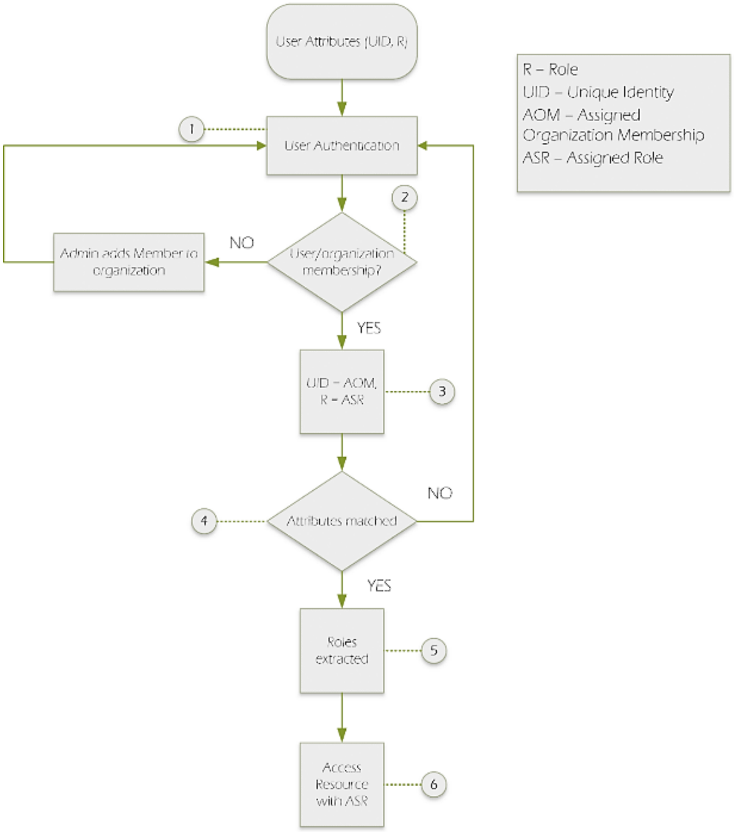


Figure 8 Role authorization

3.4 Application of RBAC in Access Control Policy Enforcement using Secure Door Access as A Case Study

This section describes the application of RBAC in the development and enforcement of access control security policy.

3.4.1 Role Creation

Three levels of roles are defined in the proposed system based on the case study. At the root of the hierarchy of roles is the student, followed by lecturer and hod. The hierarchical structure reflects the inheritance rule in which ‘lecturer’ inherits all the permissions and access associated with ‘student’. The hod being the parent role inherits both the lecturer which in turns inherits the student role. For example, a student has access to all the classes in a particular block and general offices while lecturer inherits all the access of the student as well access to lecturers’ offices. The hod have access to hod office as well lecturers and student accesses. These are the main roles of the case study. Set of roles are associated with different objects, in essence, a hod has access to his office, lecturers offices and all the access that a student may have whereas a lecturer does not have access hod offices but can access lecturers offices and student classrooms. Students on the other hand have access to all the classrooms and general offices and but cannot access the lecturers and hod offices. Table 1 shows the roles and roles designate used in the enforcement of RBAC for one organization.

Table 1. Roles, Objects and Operation in RBAC

Resources / Roles	Object 1 (General Office Door)	Object 2 (Lecturers' office door)	Object 3 (HOD office door)
Student	**OPS:** Read ✓, Update ✓	**OPS:** Read ✓, Update X	**OPS:** Read ✓, Update X
Lecturer	**OPS:** Read ✓, Update ✓	**OPS:** Read ✓, Update ✓	**OPS:** Read ✓, Update X
HOD	**OPS:** Read ✓, Update ✓	**OPS:** Read ✓, Update ✓	**OPS:** Read ✓, Update ✓

As shown in Table 1, RBAC enforced hierarchical rule enforcement. For instance, user whom is assigned the role of hod has inherits all the permission of student and lecturer roles. Likewise, lecturer role inherits all the permissions assigned to student role. Each of the resources (objects) contained list of roles which provide the permissions to access them. However, roles are unsecure and is derived from the client application side. In other to enforce an airtight secure access policy, reliance on user given role is insufficient to secure access to protected data if there is any possibility that roles can be reassigned or misappropriated. This challenge is identified in RBAC in many literatures. in other to overcome such limitation, the implementation and application of sever security rules on the server side which completely control each of the operation on the object was implemented and is discussed in the subsequent section.

3.5 Secure Access Application Design and Development

This section covers the design and development of android mobile applications for the demonstration of enforcement of security access policy in authentication and access control.

3.5.1 System Design Requirements

The Secure Access application software consists of multi-tenancy front end for user interaction, authentication and access to resources. The second part of the application include the backend used for authentication of users and access control policy enforcement using RBAC. Each component of the system has some set of requirements and is presented in the following sections.

3.5.2 Front End Mobile Application Requirements

a) Record personal information of users including the user's full name, email, username, and password.
b) Allow user to sign in and sign out and update user personal information
c) Allow user to access registered list of organizations and interact with the components of each of the organization.
d) Read and update data to and from cloud database using assigned roles and permission.

The mobile application used by admin is required to:

a) Performed all the functions of a regular user as stated in the previous section
b) View all registered users for each of the organization.
c) Assigned new users to organization, and specify their corresponding roles
d) Monitor users, modify their access roles and permissions

3.5. 3 Backend

1. Create organization and resources for each of the organization
2. Create roles and for each of the organization and assigned user membership.

3.5.4 Dashboard Screen Design

The dashboard screen of the mobile application contains the list of all the organizations of which a registered user is a member. If the user does not belong to any organization, the dashboard screen will show an empty list notifying the user. The list of organizations that the user belongs to is shown using a card design user interface. Each of the cards contains the name and address of the organization and the thumbnail image of the that particular organization. This is illustrated in Figure 9.

3.6 Authentication Mechanism

The authentication policy mechanism used in this work is based on email, password, one time password (OTP) and biometrics which is a Multifactor authentication rule. The user supplied email and password pair is used to generate an authentication event and is valid for all time use. The authentication generated event is communicated between the android application and the authentication server through the OAuth 2.0 secure channel. A screenshot in Figure 10 shows the result of the authentication server side.

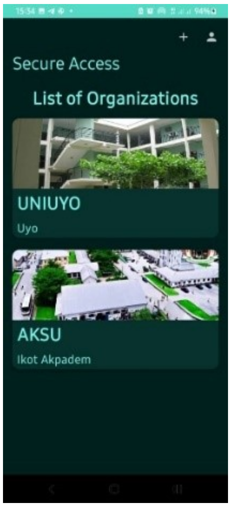
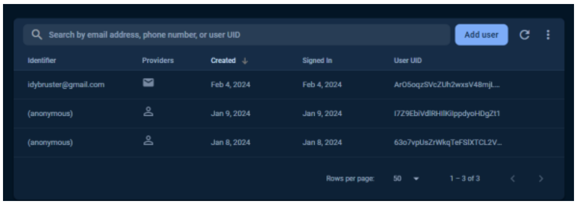


Figure 9. Dashboard



Identifier	Providers	Created ↓	Signed In	User UID
idybruster@gmail.com	✉	Feb 4, 2024	Feb 4, 2024	ArO5oqzSVcZUh2wxsV48mjL...
(anonymous)	👤	Jan 9, 2024	Jan 9, 2024	I7Z9EbiVdlRHIlKilppdyoHDgZt1
(anonymous)	👤	Jan 8, 2024	Jan 8, 2024	63o7vpUsZrWkqTeFSlXTCL2V...

Rows per page: 50 1 – 3 of 3

Figure 10. Authentication Server Page

3.7 Data Integrity and Validation

Data integrity and validation in the context in security policy included the enforcement of strict policies and rules to ensure confidentiality, integrity and available of data collected. Some of the rules and policies used in this work to implement data integrity and validation are input validation, data encryption, access control, authentication and authorization, data masking and audit trailing.

3.7.1 Input Validation and Data Masking

The input validation rule was used to enforce strict validation rules for all the form fields in the user application to ensure that only properly formatted data is accepted from the user. The main purpose of the enforcement of this policy is to prevent injection attacks such as the SQL injection, cross-site scripting and command injection. Figure 10 shows a validation flow graph chart of the input rule validation procedures.

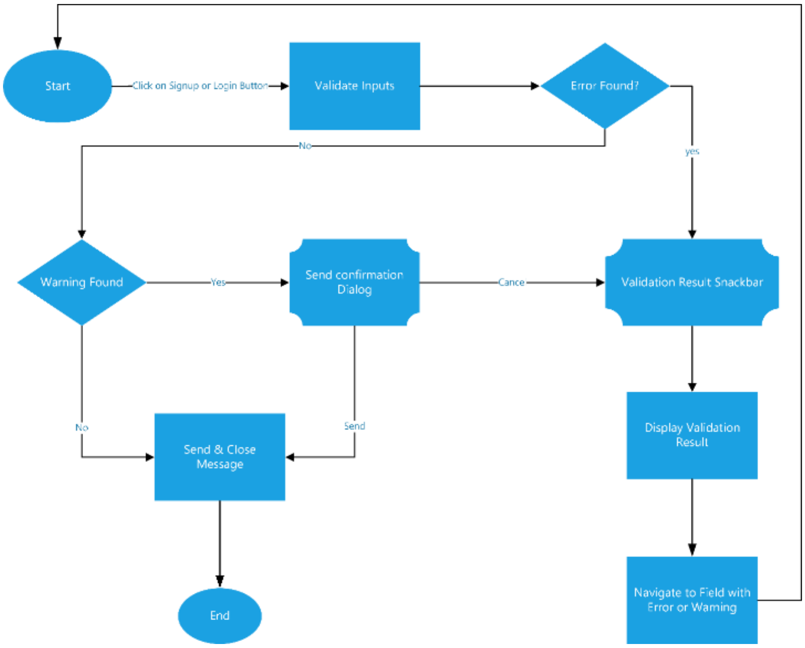
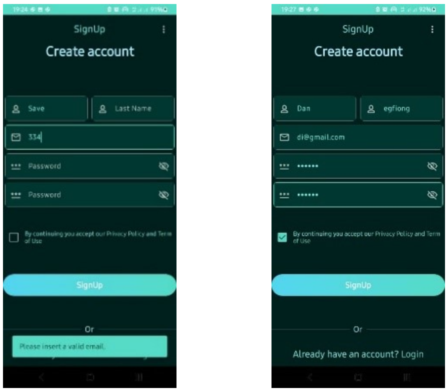

Start
Click on Signup or Login Button
Validate Inputs
Error Found?
No
yes
Warning Found
Yes
Send confirmation Dialog
Cance
Validation Result Snackbar
No
Send
Send & Close Message
Display Validation Result
End
Navigate to Field with Error or Warning

Figure 11. Input Data Validation Flow Graph

Data masking procedure is another data integrity and validation rules implemented. Data masking is used to mask sensitive information such as credit card numbers, and passwords to prevent an unauthorized disclosure of information during the when the user is entering data into the forms. The implementation of the input rules and data masking were done on the user interface of the application layer of the software development. Figure 12 a and b show the result of implementation of the input validation and password masking respectively.


SignUp
Create account
Save
Last Name
334
Password
Password
□ By continuing you accept our Privacy Policy and Term of Use
SignUp
Or
Please insert a valid email.

(a)

SignUp
Create account
Dan
egfiong
di@gmail.com
••••••
••••••
☑ By continuing you accept our Privacy Policy and Term of Use
SignUp
Or
Already have an account? Login

(b)

Figure 12. a and b: Input Validation and Data masking rules

3.8 Access Control

The access control policy of this study was designed using the method of role-based access control. The set of roles were defined and assigned to different subjects. Each subject is assigned some permissions over protected resources. The design and implementation of Android Secure Access application was used to illustrate the effectiveness of enforcement of the access control policy. The application consisted of a basic organization hierarchical structure whereby each organization consist of resources accessible to members only. Each member is an end user who has been preassigned by the admin of each organization. A basic illustration using security access doors was adopted to highlight the access policy implementation. Each member of the organization is assigned specific roles, and each role are assigned specific permissions for specific operations that can be carried out on each of the protected resource. Figure 13 illustrate the enforcement of the access control security policy showing the different access to protected resources.

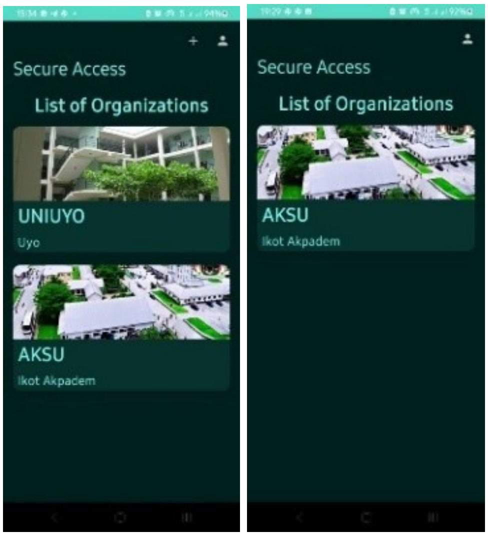
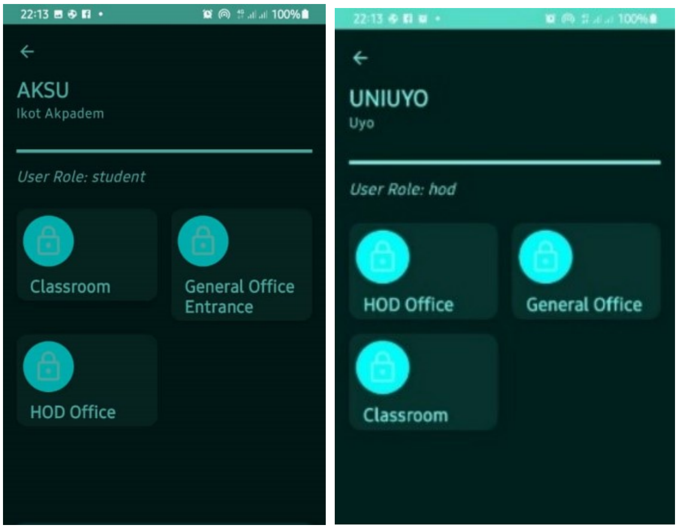


Figure 13: Dashboard for two users

From Figure 13, one user is a member in two organizations (UNIUYO and AKSU) while the other is a member in only one organization (AKSU). It is impossible for a user of to have access to organizational resources which he/she is not a member as clearly detailed in the Figure 5.6 above. This guaranteed enforcement of secure access control over protected resources. Furthermore, in Figure 13, two protected doors (resources) are shown. Each door has access, open and closed operations, however, only users with specific roles and permissions can access (read), open and close (update) each of the security. This is illustrated in Figure 14.



22:13 100%

AKSU
Ikot Akpadem

User Role: student

Classroom

General Office Entrance

HOD Office

22:13 100%

UNIUYO
Uyo

User Role: hod

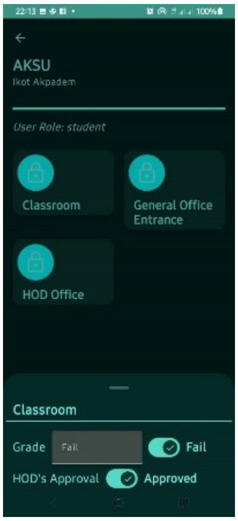
HOD Office

General Office

Classroom

Figure 14. Access to Resource

From Figure 14, User with student role read all the resources available to the registered organization, however, can only open and close the security door tagged General Office. The user with student role despite having access (read operation) to the two office doors (resources) can only update one that access and write permissions while Hod have all read operations and can open all office but restrict on update based on the read write operations. Again Figure 15 shows a student having access to view the classroom but cannot modify what was approved by hod and the grade which was updated by a lecturer.



22:13 100%

AKSU
Ikot Akpadem

User Role: student

Classroom

General Office Entrance

HOD Office

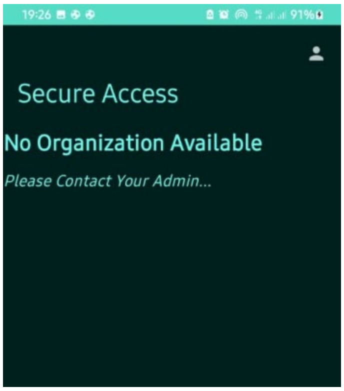
Classroom

Grade Fail Fail

HOD's Approval Approved

Figure 15. Access to Resource

Nevertheless, a user can register to the secure access application but will not be able to perform any action unless an admin assign role to the use at this point the user remains on a read mode but to the resources only to the homepage for further access privilege to be assigned hence, we present this scenario in Figure 16.



Secure Access

No Organization Available

Please Contact Your Admin...

Figure 16. No Access to security doors

Figure 17 depicts the admin section where the admin can assign roles to users and be able to view incidence logs of different activities carried out by users.

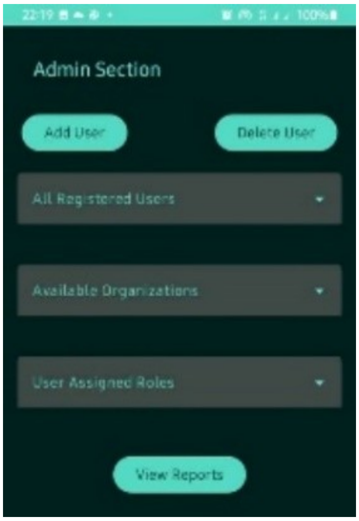
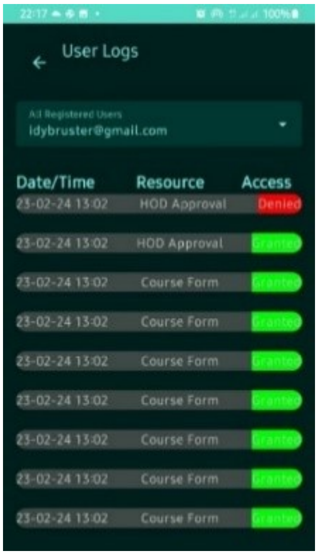


Figure 17. Admin Section

Nevertheless, Figure 18 depicts the incidence log that tracks each user activity on the application and also shows the different access the user had and access it was denied when trying to get to it.



idybruster@gmail.com

Date/Time	Resource	Access
23-02-24 13:02	HOD Approval	Denied
23-02-24 13:02	HOD Approval	Granted
23-02-24 13:02	Course Form	Granted
23-02-24 13:02	Course Form	Granted
23-02-24 13:02	Course Form	Granted
23-02-24 13:02	Course Form	Granted
23-02-24 13:02	Course Form	Granted
23-02-24 13:02	Course Form	Granted
23-02-24 13:02	Course Form	Granted

Figure 18. Incidence logs

Nevertheless, the practical implications of the findings from this study emphasize significant improvements in mobile application security through the use of OAuth 2.0, Role-Based Access Control (RBAC), and multi-factor authentication (MFA). OAuth 2.0 enhances security by enabling secure authorization without exposing user credentials, using access and refresh tokens to protect sensitive data. RBAC provides granular control over resource access based on predefined roles, ensuring users have the minimum required permissions and simplifying administrative tasks. MFA further strengthens authentication by requiring multiple forms of verification, thus reducing the risk of unauthorized access. Data integrity and validation are maintained through strict input validation and data masking, which prevent common security threats such as SQL injection and cross-site scripting. Additionally, the implementation of incidence logs and monitoring features enables effective tracking of user activities and detection of potential security breaches. By comparing RBAC with other security frameworks like Attribute-Based Access Control (ABAC) and Discretionary Access Control (DAC) highlights its strengths and limitations. While RBAC offers a straightforward approach to managing roles and permissions, ABAC provides more dynamic and context-aware access control, and DAC allows users to control access to their own resources, potentially leading to inconsistent policies. Overall, the study demonstrates that the combination of OAuth 2.0, RBAC, and MFA effectively enhances mobile application security, with each framework offering different benefits depending on the specific needs of the environment.

3.9 Discussion

The findings of this study underscore the substantial enhancements in mobile application security achieved through the integration of OAuth 2.0, Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA). The OAuth 2.0 protocol plays a pivotal role by facilitating secure authorization without the need to expose user credentials directly. This is accomplished through the use of access and refresh tokens, which provide a secure method for accessing protected resources while ensuring that user credentials remain confidential. The implementation of OAuth 2.0 in this study demonstrates its effectiveness in mitigating risks associated with unauthorized access to sensitive data, making it a crucial component of modern mobile security frameworks.

Role-Based Access Control (RBAC) further enhances security by providing a structured approach to managing access to resources based on predefined roles. This approach simplifies the administration of user permissions by ensuring that each user is granted only the access necessary for their role. The hierarchical nature of RBAC, as implemented in this study, allows for efficient permission inheritance, reducing administrative overhead while maintaining strict access control. The case study involving secure door access cards exemplifies how RBAC can be effectively applied to real-world scenarios, ensuring that users have appropriate access to resources based on their roles within an organization.

The addition of Multi-Factor Authentication (MFA) significantly bolsters the authentication process by requiring users to provide multiple forms of verification before gaining access. This added layer of security reduces the likelihood of unauthorized access, even in cases where user credentials may be compromised. The use of MFA in this study, which includes methods such as email, passwords, one-time passwords (OTP), and biometric data, highlights its effectiveness in enhancing the overall security posture of mobile applications. By combining MFA with OAuth 2.0 and RBAC, the study illustrates a comprehensive approach to securing sensitive data and protecting against potential threats.

The study also emphasizes the importance of data integrity and validation as critical components of security policy enforcement. Strict input validation and data masking techniques are employed to protect against common security threats, such as SQL injection and cross-site scripting. These measures ensure that only properly formatted data is accepted and that sensitive information, such as passwords and credit card numbers, is obscured from unauthorized access. The implementation of these techniques on the user interface layer of the Secure Access application demonstrates their effectiveness in maintaining the confidentiality, integrity, and availability of data.

While the study showcases the strengths of RBAC, it also acknowledges its limitations when compared to other security frameworks, such as Attribute-Based Access Control (ABAC) and Discretionary Access Control (DAC). RBAC offers a straightforward approach to managing roles and permissions, making it suitable for environments where roles are well-defined and static. However, ABAC provides a more dynamic and context-aware approach, allowing for more granular access control based on attributes such as user identity, resource type, and environmental conditions. DAC, on the other hand, gives users the ability to control access to their own resources, which can lead to inconsistencies in policy enforcement. These comparisons highlight the importance of selecting the appropriate access control framework based on the specific needs and context of the environment.

The combination of OAuth 2.0, RBAC, and MFA, as demonstrated in this study, provides a robust and effective approach to enhancing mobile application security. Each framework offers unique benefits that contribute to a comprehensive security strategy, addressing different aspects of authentication, authorization, and data protection. The practical application of these security measures in the Secure Access application illustrates their effectiveness in real-world scenarios, ensuring that sensitive resources are protected against unauthorized access and potential security breaches.

4. CONCLUSION

The integration of Role-Based Access Control (RBAC) and OAuth 2.0 in mobile security represents a significant advancement in safeguarding network resources and user data. RBAC streamlines access management by assigning permissions based on user roles, thereby enhancing data security and operational efficiency. OAuth 2.0 complements this by providing a robust framework for secure, token-based authorization, which mitigates the risks associated with credential exposure. Together, these technologies ensure a well-rounded approach to security, addressing critical aspects such as confidentiality, integrity, and availability of data. The broader implications of using RBAC and OAuth 2.0 for mobile security are substantial. These frameworks not only improve the effectiveness of access controls but also enhance the overall security stance of mobile applications by minimizing the risk of unauthorized access and data breaches. The adoption of these technologies supports scalable and adaptable security solutions that can evolve with changing network environments and threat landscapes. Future research should focus on exploring alternative security models that could complement or enhance RBAC and OAuth 2.0. Areas of interest include the investigation of decentralized identity management systems and the development of more adaptive access control mechanisms. Additionally, testing these systems in diverse environments, such as different organizational settings or varying threat conditions, will provide valuable insights into their effectiveness and potential areas for improvement. This will help ensure that security measures remain robust and relevant in the face of emerging challenges.

REFERENCES

[1] B. Carroll, *Cisco Access Control Security: AAA Administrative Services*. Cisco Press, 2004.

[2] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 566-600, 2017.

[3] S. Parhi, "Attacks due to flaws of protocols used in Network Access Control (NAC), their solutions, and issues: A survey," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 3, pp. 31-42, 2012.

[4] G. L. Kim, J. S. Jang, and S. W. Sohn, "The implementation of policy management tool based on network security policy information model," *KIPS Trans. PartC*, vol. 9, no. 5, pp. 775-782, 2002.

[5] I. J. Umoren and S. J. Inyang, "Methodical performance modelling of mobile broadband networks with soft computing model," *Int. J. Comput. Appl.*, vol. 174, no. 25, pp. 7-21, 2021.

[6] C. L. Bowser, "Enforce network access control through security policy management process and enforcement," SANS Institute, 2004.

[7] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and solutions survey," *Sensors (Basel)*, vol. 22, no. 19, p. 7433, 2022. doi: 10.3390/s22197433.

[8] J. Matias, J. Garay, A. Mendiola, N. Toledo, and E. Jacob, "FlowNAC: Flow-based network access control," in *2014 Third European Workshop on Software Defined Networks*, 2014, pp. 79-84.

[9] A. Lakbabi, G. Orhanou, and S. E. Hajji, "Network access control technology—Proposition to contain new security challenges," *arXiv preprint arXiv:1304.0807*, 2013.

[10] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79-101, 2019.

[11] E. Johnson, G. Ansa, H. Cruickshank, and Z. Sun, "Access control framework for delay/disruption tolerant networks," in *Personal Satellite Services: Second International ICST Conference, PSATS 2010, Rome, Italy, February 2010 Revised Selected Papers*, vol. 2, Springer Berlin Heidelberg, 2010, pp. 249-264.

[12] C. A. Berrick, "Homeland security: DHS's progress and challenges in key areas of maritime, aviation, and cybersecurity (GAO-10-106)," Government Accountability Office, 2009.

[13] O'Reilly, *Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control*, 2023.

[14] C. Fisher, "Network access control: Disruptive technology?" Regis University Student Publications, 2007.

[15] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "Information security policy: A management practice perspective," *arXiv preprint arXiv:1606.00890*, 2016.

[16] S. Ramachandran, C. Rao, T. Goles, and G. Dhillon, "Variations in information security cultures across professions: A qualitative study," *Commun. Assoc. Inf. Syst.*, vol. 33, no. 11, pp. 163-204, Dec. 2012.

[17] M. Kamariotou and F. Kitsios, "Information systems strategy and security policy: A conceptual framework," *Electronics*, vol. 12, no. 2, p. 382, 2023. doi: 10.3390/electronics12020382.

[18] G. Kumar and K. Kumar, "Network security—An updated perspective," *Syst. Sci. Control Eng.*, vol. 2, no. 1, pp. 325-334, 2014.

[19] S. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity, and availability in security," *J. Inf. Syst. Secur.*, vol. 10, no. 3, 2014.

[20] H. Dwivedi, C. Clark, and D. V. Thiel, *Mobile Application Security*. New York: McGraw-Hill, 2010.

[21] E. J. Smith, D. A. Robinson, and S. Elphick, "DER control and management strategies for distribution networks: A review of current practices and future directions," *Energies*, vol. 17, no. 11, p. 2636, 2024.

[22] Y. Mowafi, I. Dhiah el Diehn, A. Zmily, T. Al-Aqarbeh, M. Abilov, and V. Dmitriyevr, "Exploring a context-based network access control for mobile devices," *Procedia Comput. Sci.*, vol. 62, pp. 547-554, 2015.