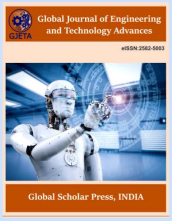
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(RESEARCH ARTICLE)

Check for updates

ENHANCED PROTECTION OF BANK CUSTOMER RECORDS USING ACCESS CONTROL AND HEURISTIC INTRUSION DETECTION TECHNIQUES

Helen T. Godwin [1,*], Godwin O. Ansa [1] and Uduak A. Umoh [2]

[1] Department of Computer Science, Akwa Ibom State University, ikot Akpaden.
[2] Department of Computer Science, University of Uyo, Uyo.
* Corresponding Author

ORCID Details
Helen T. Godwin: https://orcid.org/0009-0001-2614-1990

Global Journal of Engineering and Technology Advances, 2026, 29(02), 034–050

Publication history: Received on 21 September 2026; revised on 02 November 2026; accepted on 04 November 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.29.2.0312

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The advent of digital banking services has created a great need to provide better protection for the confidential records of customers from any form of unauthorized access, misuse of privilege, insider attacks, and any suspicious behavior of the user. While traditional access control policies may limit users according to certain rights, they might not be able to identify any unusual behavior by the user who is an authorized entity of the system. In this regard, this research project seeks to develop a secure banking information system that uses RBAC with IDS. The design of the system was carried out as an intranet web application based on PHP, MySQL, HTML, CSS, JavaScript, Bootstrap, and Apache using XAMPP/WAMP. The RBAC architecture was employed using authentication, session handling, role assignment, and permission validation, whereas heuristic IDS was carried out by analyzing system traces, which comprised logging activities, access pattern of resources, failed access requests, abnormal access time, retrieval of records, and escalation of privileges. Risk scoring approach was also adopted to identify any suspicious activity based on certain heuristic rules and criteria. The results suggest that combining RBAC and heuristic intrusion detection resulted in the successful prevention of any unauthorized access and detecting any abnormal behavior which might happen despite the fact that the user had a valid account. Hence, the system developed is an efficient method to secure the private data of banking customers in an intranet banking environment.

Keywords: RBAC, Intrusion, Bank, IDS, IPS, Security.

1 INTRODUCTION

Nowadays, customer records have turned into one of the major resources for banks. Such records contain all sorts of private information, including customer identification data, financial transaction history, account balance information, and private communications between client and institution (Gangele, 2024). With growing concerns about cyber-attacks, hacking, and insider threats, there is a lot of pressure on banks to make sure that such records are adequately protected from potential threats. However, although access control methods remain the norm for many banks today,

they lack sufficient flexibility to deal with emerging security issues (Haryaman et al., 204). Thus, creation of access control and heuristic intrusion detection systems specially designed for bank environment is essential. Customer records include all aspects of client financial activity and can therefore be viewed as very tempting targets for hackers and malicious insiders. The protection of such records is both a legal requirement for the bank and an important element of customer trust (Chattopadhyay, 2024). One violation of client data could result in substantial monetary loss, reputation loss, legal risks, and even in the downfall of a financial organization's reputation. For securing bank customer record information, a multi-faceted strategy should be implemented that combines various aspects of security such as technical security, administrative security, and physical security. The encryption of data both in storage and in transfer is one common method of protection, whereas the firewall, intrusion detection system, and anti-malware software help prevent the external cyber-attack (Irsyad et al., 2024). Nevertheless, technical protection measures are not sufficient, as insider threats – employees with malicious behavior and intentions – are a serious danger for a bank's database. Therefore, banks need to implement rigorous access control policies that will allow authorized individuals to see and alter customer record information (Chattopadhyay, 2024). Access control mechanisms play a central role in safeguarding bank customer records, providing structured methods to control who can access what information, under what conditions, and to what extent (Chattopadhyay, 2024).

This is where heuristic intrusion detection system comes as a solution for these problems since, unlike signature-based IDS that depend on pre-known patterns of attacks, heuristic IDS (Intrusion Detection System) depend on rule-based reasoning, anomaly detection, and behavior analysis to detect attacks. Through learning patterns of normal and abnormal usage, heuristic system can be able to detect any new kind of threats and thus provides an extra security layer.

With the integration of access control systems, heuristic IDS improves the ability of monitoring, adapting, and preventing any actions from occurring. In spite of the developments in digital security, banks still have cases of intrusions and the ability to get access to sensitive customer records because of the weaknesses in their access control systems. Some contextual factors such as place of login, time, security level of the device, or risks associated with the transaction are taken into consideration (Edet et al., 2025). This static and general nature of access control framework makes insider threats, accidental exposure of information, and cyber-attacks very likely.

There is an urgent need for an improved, intelligent and flexible access control system that will allow dynamic analysis of access requests on a basis of certain rules defined. Heuristic rule-based access control system provides the opportunity to use stricter criteria for access control to make sure that customer data is accessed securely and with a proper authorization. Unfortunately, a great number of banks still does not have access control systems that are this sophisticated making their data vulnerable (Udoetor et al., 2024). The proposed access control system will be based on a heuristic intrusion detection and access control system that gives or refuses an access to bank customer data depending on certain security rules. As it does not operate on a basis of predefined roles or password and instead of that, it makes a decision dynamically, for example, the loan officer will be able to get access to customer loan data during working hours and from office computer only. Customer service will have restricted access to the customer's data allowing to see the general information about customers but without the details of transactions. The access to VIP customers will require additional authentication. Temporary rights will expire after a certain period of time or once a particular task is fulfilled.

2 LITERATURE FOUNDATION

According to Table 1.0, the literature review shows that even though there have been many security frameworks and access control approaches proposed and developed for different fields such as digital banking, healthcare, and cloud computing, the majority of those access control models do not possess any dynamism or cannot combine all three access control paradigms in an adequate manner. For example, RuBAC, RBAC, and ABAC models mentioned in a number of studies have been implemented partially or not at all. In addition, some researches only considered identity management or data digitization but not an efficient access control approach (Liao et al., 2022; Subia et al., 2020). Despite the fact that some of the studies used RBAC (Saxena et al., 2023; Ghazal et al., 2024), it was not as dynamic as it should be in order to ensure adequate security in a real-time environment. Moreover, certain research studies, especially ones focusing on encryption or machine learning (Chattopadhyay et al., 2024; Ullah et al., 2020; Happiness et al.,2024) considered the issue of data security or anomaly detection without considering the aspect of access control framework enabling user-based authorization. The lack of such combination of security measures (such as the combination of RBAC and ABAC or intrusion detection systems) makes the current solutions inefficient in critical industries such as digital banking. Thus, the identified gap consists of developing an improved intelligent access control system with the help of heuristics-based intrusion detection technique. In fact, the developed system is needed because of the goal of the current research, which consists of enhancing the security of bank customer records with the help of access control and heuristics-based intrusion detection techniques. Through the implementation of such system, the researchers seek to overcome the limitations associated with previous research. Namely, it is necessary to fill the gap

of practical application of access control and intrusion detection systems for banks and insufficient measures of ensuring access restriction in real-time context.

2.1 Adopted Existing System

The adopted existing system by Happiness et al. (2024) integrated Network Security Model with Role-Based access control for Mobile applications to enhance data privacy and security.

The user in this context is the mobile user devices running on the Android operating system which interact with the network application in which they are authenticated and authorized. The key aspects/components of the authentication policy utilized are; Email, password and Multi-Factor Authentication (MFA). OAuth 2.0 is one of the authentication and authorization protocols commonly used in authentication policy which allows a node to register into the network and also supports identity providers such as Google, Facebook among others. Once the user is authenticated, a unique identifier (UID) is created for each authenticated user, when the user accesses the application through the mobile device, for accessing resources, a second authentication factor such as OTP (One Time Password) is sent to the user's registered phone number. Access control policy manages and regulates user access to resources in order to ensure the confidentiality, integrity and availability of the resources. Access Trust Manager defined whether a user is allowed to access or deny for each action of CRUD (Create, Read, Update, Delete) on a particular subject. RBAC is the access control policy mechanism which uses administrative and regular roles adhering to the principle of least privilege which minimizes the risk of unauthorized access and potential security breaches. Session timeout security ensures that the user session on the network or application is terminated once the user is inactive, the user can be re-verified using pin, biometric and OTP. Auditing/incidence Analytic ensures the logging of events and activities in the network or within the application. It logs the successful or failed login attempts, changes in authentication settings, requests and responses to and from the server and events that can cause serious bugs in the application.

Consequently, the proposed system seeks to enhance these capabilities through access control and heuristic intrusion detection, this hybrid approach ensures that protecting of customer records is guided by roles, attributes and real time conditions for enhanced data protection in banking environments.

Table 1: Summary of Related Literature

Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Punia et al., 2024	A systematic review on blockchain-based access control systems in cloud environment.	Review	To review blockchain based access control	D	RuBAC	ABAC	RBAC	MAC	DAC	The author never adopted any of the access control understudied. It was a review work based on blockchain access control
				✗	✗	✗	✗	✗	✗	
Author	Title	Method	Aim	Parameters						Limitation
Kumar et al., 2022	Rule-based credit card fraud detection using user's keystroke behavior. In *Soft Computing: Theories and Applications*	Users Keystroke	To detect fraud in credit card	D	RuBAC	ABAC	RBAC	MAC	DAC	The authors used RuBAC but never used complete parameters to strengthen the model. The model needs more parameters to ensure robustness.
				✗	✓	✗	✗	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Ullah et al., 2020	SS7 vulnerabilities — a survey and implementation of machine learning vs rule-based filtering for detection of SS7 network attacks	Machine Learning	To check vulnerability of SS7 network attacks	D	RuBAC	ABAC	RBAC	MAC	DAC	Used RuBAC but not applied in banking application for customer records security
				✗	✓	✗	✗	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Fareed ete al., 2022	Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system	Authentication scheme	To protect e-health system	D	RuBAC	ABAC	RBAC	MAC	DAC	Does not use RuBAC Parameters in the model not enough to ensure robustness
				✗	✗	✗	✓	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Saxena et al., 2023	Role-based access using partial homomorphic encryption for securing cloud data.	Partial Homomorphic encryption	To secure cloud data	D	RuBAC	ABAC	RBAC	MAC	DAC	Did not use RuBAC, and other methods are better than RBAC which the authors adopted
				✗	✗	✗	✓	✗	✗	

Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Jayasankar et al., 2021	Securing Medical Data using Extended Role Based Access Control Model and Two fish Algorithms on Cloud Platform	Two Fish Algorithms	To secure medical data	D	RuBAC	ABAC	RBAC	MAC	DAC	The work used RBAC, no dynamism added to the model Two fish algorithm is a weak encryption algorithm and cannot protect bank records
				✗	✗	✗	✓	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Ghazal et al., 2024	Automated Semantic Role Mining Using Intelligent Role Based Access Control in Globally Distributed Banking Environment	Distributed Banking	To mine role activities for access control	D	RuBAC	ABAC	RBAC	MAC	DAC	The work used RBAC, with no dynamism added to it. A strong banking access control system must have element of dynamism to ensure interactivity
				✗	✗	✗	✓	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Liao et al., 2022	Blockchain-based identity management and access control framework for open banking ecosystem.	Identity management	To develop access control system for open banking system	D	RuBAC	ABAC	RBAC	MAC	DAC	The work ensured storage security with blockchain, but lacked access control mechanism. This work need improvement
				✗	✗	✗	✗	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Subia et al., 2020	Archiving and digitizing of customer records of golden rural bank of the Philippines	Review	To digitalize customer records in Bank	D	RuBAC	ABAC	RBAC	MAC	DAC	No Access control mechanism was used in the bank customer records
				✗	✗	✗	✗	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Alzoubi et al., 2022	Cyber security threats on digital banking	Gitial banking	To examine cybersecurity threats on digital banking	D	RuBAC	ABAC	RBAC	MAC	DAC	No access control mechanism was used to secure bank information. Only cybersecurity threats were combated in the work
				✗	✗	✗	✗	✗	✗	
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Han et al., 2020	Information Security Risk Management in Electronic Banking System	Risk Analysis	To assess risk in electronic banking systems	D	RuBAC	ABAC	RBAC	MAC	DAC	ABAC was used in combination with MAC
				✗	✗	✓	✗	✓	✗	

										No RuBAC was used and there was no dynamism in the system
Author	Title	Method	Aim	Parameters/Security Approaches						Limitation
Chattopadhyayet al., 2024	AI-Driven Adaptive Encryption: Transforming Financial Data Security in the Age of Digital Banking	Encryption Scheme	To secure bank data using adaptive encryption scheme	D	RuBAC	ABAC	RBAC	MAC	DAC	No RuBAC was used System lacked dynamism No access security framework was adopted. Only encryption mechanism was used The system needs improvement to make it robust
				✗	✗	✗	✗	✗	✗	
Sarfaraz et al., 2023	AccessChain: An access control framework to protect data access in blockchain enabled supply chain	Access Control Scheme	To protect Data using access control method	✗	✗	✓	✗	✗	✗	No heuristic approach was used. No dynamic system control
Happiness et al. 2024	Enhanced Network Security model with Role-based access control for mobile applications	Network Access Control (NAC)	Role-Based and OAuth 2.0 protocols	✗	✗	✗	✓	✗	✗	No heuristic approach, only RBAC was used and not tailored to Banking
Total Number of Access Control Mechanism studied Is 6				Definition of Parameters/Security Approaches Dynamic Access Control RuBAC - Rule-based Access Control ABAC - Attribute Based Access Control RBAC - Role Based Access Control MAC - Mandatory Access Control DAC - Decretory Access Control						

Table 2: Key Comparisons of the Existing and Proposed work

Feature	Existing System (Happiness et al., 2024)	Proposed System (Heuristic Access Control Mechanism)
Access Control Model	Role-Based Access Control (RBAC)	Role-Based and Attribute-Based Access Control
Decision Criteria	Based on roles of users, resources, and environment	Based on roles combining context, time, role, and device factors
Flexibility	Limited – relies on predefined attribute policies	Highly flexible – dynamically adjusts access rules based on real-time conditions
Context Awareness	Minimal contextual awareness	Strong context sensitivity (e.g., location, time, and device verification)
Insider Threat Mitigation	Basic policy enforcement only	Advanced detection via behavioral and contextual rule analysis
Session and Time Control	Absent	Integrated timer-based access expiry and session control
Implementation Environment	Mobile Application	Secure banking system for customer record protection

The Architecture of the existing system is centered around Network access control which allows network resources available to endpoint devices which aligns user with predetermined security protocol within a mobile application.

Other mobile application can be allowed entry but restricted to confined zone.

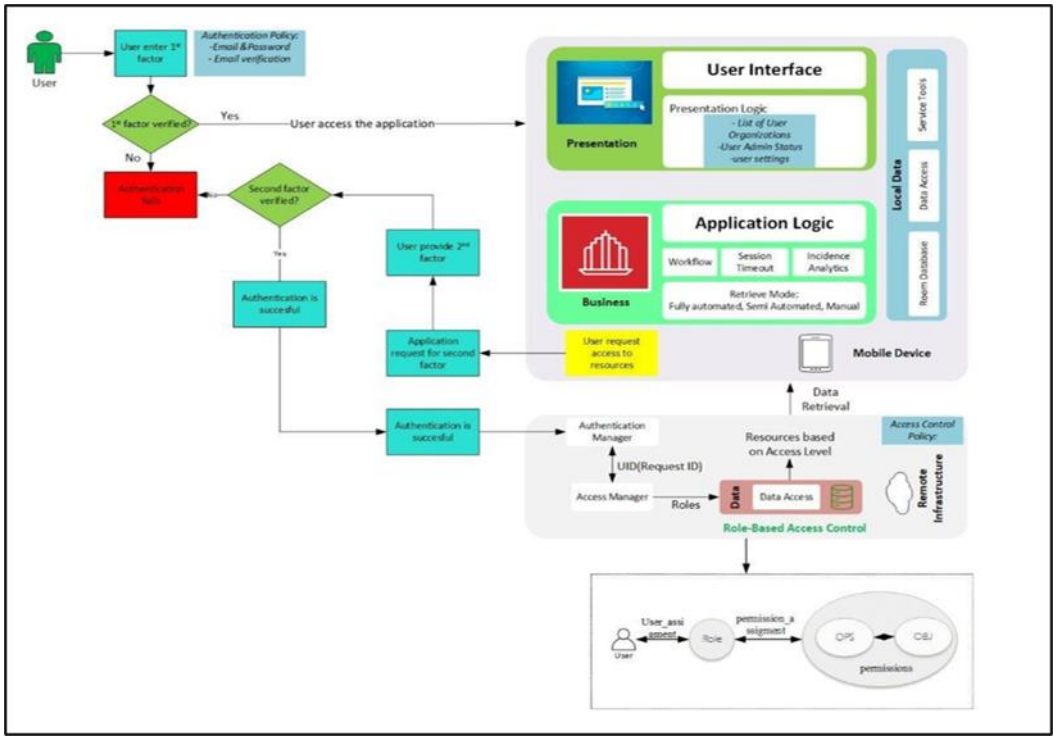


Figure 1: Architecture of the Existing system (Happiness et al.2024).

3 METHODOLOGY

Even though considerable progress has been made in terms of digital security, numerous cases of information leakage and breach of sensitive data in banks persist because of the deficiencies of the current access control systems. Role-Based Access Control is an example of an old-fashioned approach to access that provides universal access permissions regardless of the context, such as time, geographical position, integrity of the device, or transaction type. This approach makes the system vulnerable to potential insider risks and attacks. With increasing digitization of financial processes, the flaws of the traditional framework are becoming evident.

The problems identified above necessitate the development of a much more advanced and flexible access control model which would be able to consider access requests based on certain parameters in a dynamic way. To overcome the mentioned challenges, the proposed solution involves development of Heuristic Intrusion Detection and Access Control Mechanism which would involve the use of the advantages of rule-based systems combined with heuristic reasoning. Unlike traditional systems, use of security policies together with the application of heuristic reasoning for analysis of certain aspects related to access request such as time, user's behavior, device and others will help to improve decision-making process on whether to grant or deny access. For example, access to loan records can be granted only during working hours and through office devices, whereas customer service representatives will be allowed to view only general information about customers. Access to risky accounts should be provided together with secondary authentication and in some cases – manager's permission. Temporary access to certain documents should be granted for specific period of time (for example, until completion of certain tasks or until specific time passes).

Based on the identified gaps and intended solutions, the aim of this study is to design and implement a robust access control with heuristic intrusion detection for the protection of bank customer records. To achieve this, the following specific objectives are established: (i) to conduct a comprehensive review of existing literature to identify limitations in current access control systems and explore areas for improvement; (ii) to design a system that ensures the security and integrity of customer records in banking environments; (iii) to implement the system using an hybrid approach that support dynamic and context-aware access decisions; and (iv) to develop the system using PHP, HTML, CSS, and JavaScript to enable a secure, responsive, and user-friendly interface.

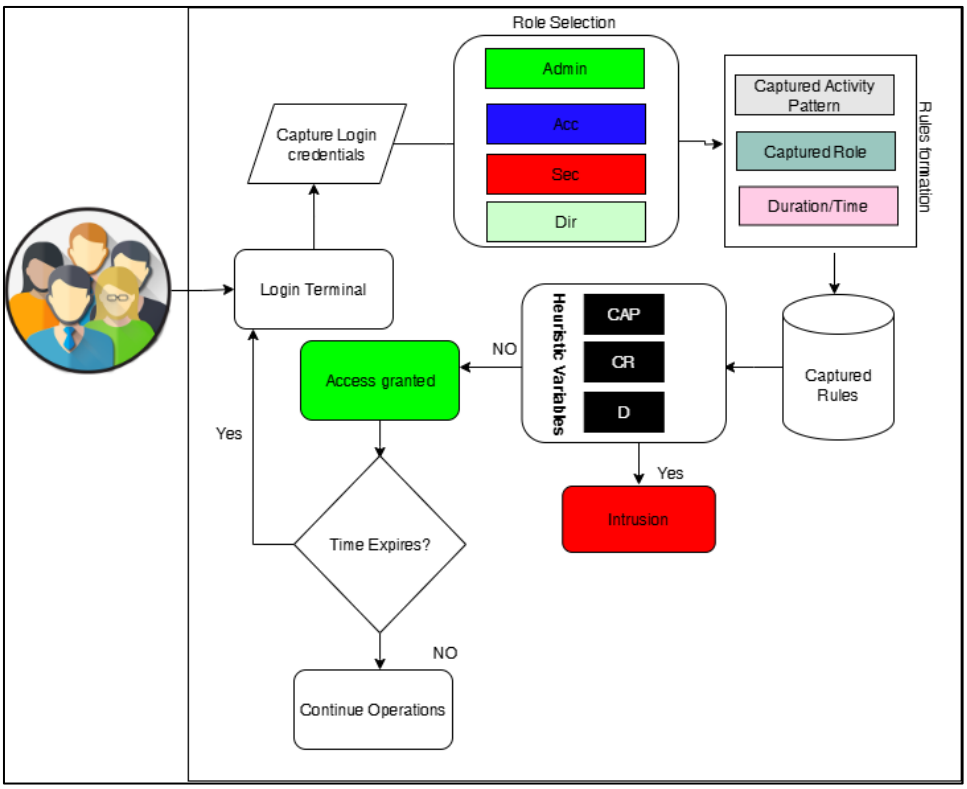


Figure 2: Proposed System Architecture

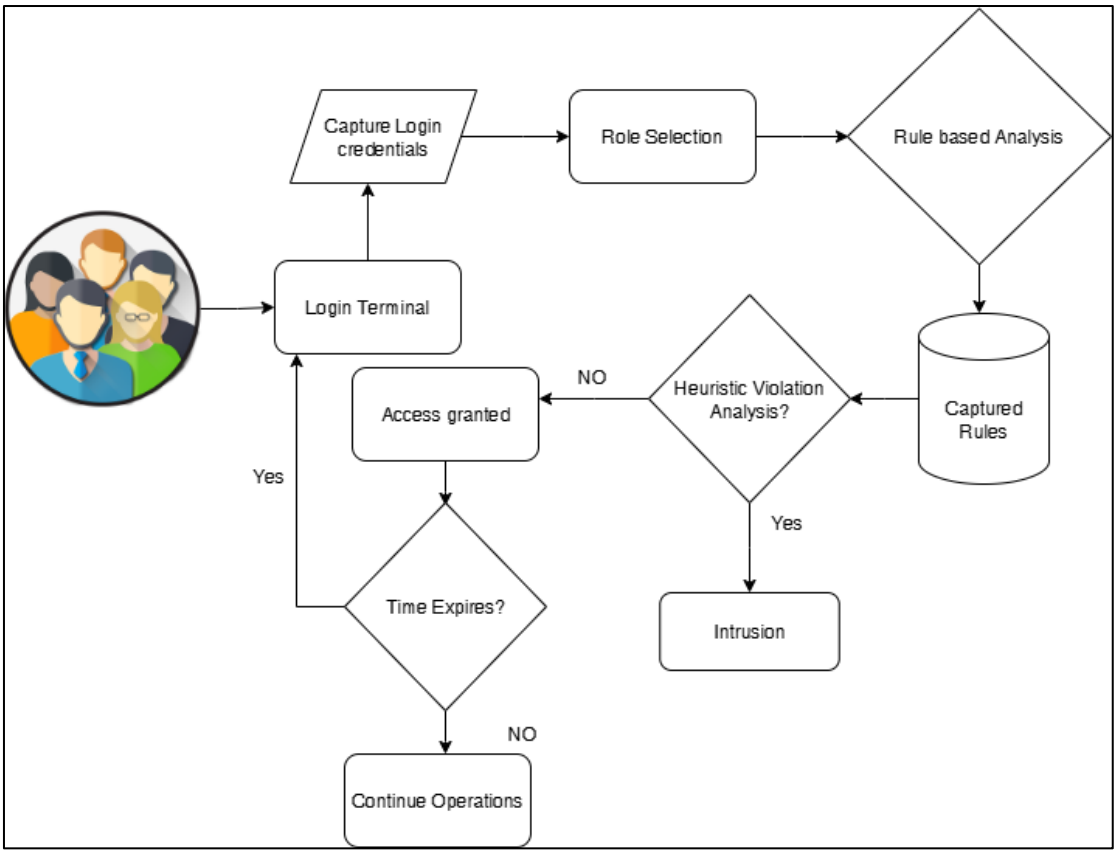


Figure 3: Proposed System Flow Diagram

The methodology adopted in this study focuses on the design and implementation of a secure, intelligent, and rule-driven access control mechanism to protect sensitive bank customer records. The approach ensures that access to critical data is governed by dynamic, context-aware rules that address the weaknesses of traditional systems and prevent unauthorized usage—especially during periods of heightened risk such as after work hours. The system development follows four major phases: system analysis, system design, system implementation, and system testing. The methodological steps followed in this work are as seen below;

3.1 System Logic Engineering

The initial phase involved identifying the shortcomings of conventional access control systems used in the banking sector. A major issue observed is the absence of time-sensitive and role-specific restrictions, leading to increased risk of insider threats and accidental data leaks. This analysis informed the decision to build a rule-based access control system where user roles, access times, and device contexts are taken into account before granting access to records. The system is designed around a centralized rule engine that evaluates each user request based on a set of predefined access rules. Users are assigned roles such as loan officers, customer service agents, auditors, or IT staff, each with specific access privileges. When a user logs in, the system verifies their role and dynamically allocates only the resources necessary for that role. The design also includes a timer-based control mechanism that limits access to sensitive resources during specific time windows—primarily during official and unofficial business hours. For example, access to customer loan documents is permitted only between 9 AM and 5 PM from authorized office locations. Outside these hours, the system automatically logs users out or blocks further access attempts, significantly minimizing the risk of insider attacks.

3.2 Web based Technologies Adopted

The system was implemented as a web-based platform using PHP for backend logic, HTML and CSS for user interface design, and JavaScript to manage interactive behavior and timer functionality. The rule engine is programmed to read from a set of rules that specify which user roles can access which resources, under what conditions (time, location, or device). When a user attempts to access a resource, the system evaluates the current context against the stored rules. Only if all conditions are met is access granted. Temporary access privileges, such as those assigned to auditors, are configured with automatic expiration to prevent prolonged unauthorized access.

3.3 System Testing and Evaluation

The system underwent rigorous testing to validate the rule enforcement mechanism and ensure secure access control. Specific scenarios were created to test different user roles, working hours, and resource types. For example, tests were conducted to ensure a loan officer could not access customer records after business hours or from an unrecognized device. Similarly, customer service staff were tested to verify they could only view general customer information, not detailed financial records. The system was also evaluated for its responsiveness, error-handling capability, and ability to enforce logout actions automatically based on time-based restrictions. By incorporating a rule-driven framework, time-sensitive access control, and strict resource assignment based on user roles, the proposed system offers a robust solution for mitigating unauthorized access and enhancing data protection in the banking environment.

3.4 Heuristic Access Control Algorithm for Bank Customer Records

i. User Login Initiation
The user enters login credentials (username and password)
The system verifies credentials against stored authentication data.
If credentials are valid, the session begins; if not, the attempt is logged as a failed access event.

ii. Role Identification with Heuristic Adjustment
Upon successful authentication, the system identifies the user's role (e.g., Loan Officer, Customer Service Staff, Auditor, T Staff).
The role is matched against a baseline role-permission matrix.
Heuristic logic refines this mapping by considering prior access history and typical behavior for the role, adjusting expected access boundaries where necessary.

iii. Contextual Heuristic Evaluation
The heuristic engine evaluates contextual factors beyond static rules:

- Time of access: Is the request during normal working hours, or is it unusual compared to the user's past activity?
- Device and location check: Is the request from a registered device and typical access location, or is it anomalous?
- Resource type requested: Is the resource aligned with past requests for this role, or does it deviate from normal.

Suspicious deviations trigger additional verification (e.g., supervisor approval or secondary authentication).
v.Dynamic Resource Assignment Heuristic Access Decision Logic
Access is granted if conditions match expected patterns and heuristic thresholds are satisfied.
If deviations exist but fall within acceptable tolerances, access may be provisionally granted with restrictions (e.g., read-only access).

If anomalies exceed thresholds (e.g., high-risk requests at odd hours), access is denied, flagged, and logged for review.

The system assigns resources adaptively, based on both the role and heuristic evaluation:

- Loan Officers access loan files only during work hours and on registered devices
- Customer Service Staff view general profiles but cannot access transactions.
- Auditors/IT Staff receive temporary access with auto-expiry, dynamically shortened if anomalous behavior is detected.

vi. Timer and Behavior-Based Control
Session timers are activated to enforce:

- Automatic logout after the permitted session duration.
- Inactivity-based termination.
- Scheduled logouts at the end of business hours.

Heuristic checks monitor activity within the session; unusual behavior (e.g., rapid repeated queries) triggers early termination.

vii. Temporary Access ExpiryTemporary privileges (e.g., auditors, IT staff) automatically expire when:

- The task is marked complete.
- The allowed duration ends.
- Heuristic monitoring detects abnormal use inconsistent with the task scope.

- viii. Heuristic-Aided Audit Logging
  Every access attempt—granted, restricted, or denied—is logged with:
- Timestamp
- User ID and role
- Device and location
- Resource requested
- Rule and heuristic evaluation outcome
  Logs are analyzed to refine heuristic thresholds, improve anomaly detection, and support regulatory compliance.

4 RESULTS AND DISCUSSION

The access control model can be represented using an RBAC matrix.

Table 2: Data Features Description

BANK ROLES	ROLE DESCRIPTION
Teller	Performs deposits, withdrawals and transfers.
Account Manager	Manages customer accounts
Customer Service Officer (CSO)	Handles customer complaints and inquiries
Auditor	Reviews records for compliance
Security Administrator (IT)	Manages user privileges and network issues
Loan Officer	Handles loan records
Database Administrator	Maintains database infrastructure

Table 3: Customer Record Resources

Resource	Resource Code
Customer Personal Records	CR
Bank Account Information	BA
Transaction Records	TR
Loan Records	LR
Audit Records	AR
User Role Records	UR

Access Rights: i R = Read; ii W = Write; iii U = Update; iv D = Delete; v A = Approve

Table 4: RBAC Matrix

ROLE	CR	BA	TR	LR	AR	UR
Teller	R	R, U	R, W	-	-	-
Account Manager						
Customer Service Officer (CSO)	R	R				
Auditor	R	R	R	R	R	
Security Administrator (IT)					R	R, W, U
Loan Officer	R	R	R	R	R, W, U	-
Database Administrator	R, W, U, D	R, W, U, D	R, W, U, D	R, W, U, D	R, W, U, D	-

System traces are audit logs recording user activities.

Example log format:

Time	User	Role	Resource	Action	Result
09:00	U101	Teller	BA	Read	Success
09:05	U101	Teller	LR	Read	Denied
09:07	U101	Teller	LR	Read	Denied
09:08	U101	Teller	LR	Read	Denied

These traces are continuously analyzed.

A user log in, the process checks for authentication of the user with the list in the database.

If the user's information is not captured, an error message pop up and access is denied, the user is re-verified for three times maximum.

If the user's role is matches with organization assigned role for the specific role. the role is then extracted for the current user. The user then access objects from the database and perform operations based on the assigned role.

The manager has full permission and is the administrator. He can add user as need arises.

The auditor has limited role that expires with time.

The account officer is granted limited permission to access customer loan file and view customer records

The teller is granted limited access to process transaction and view account.

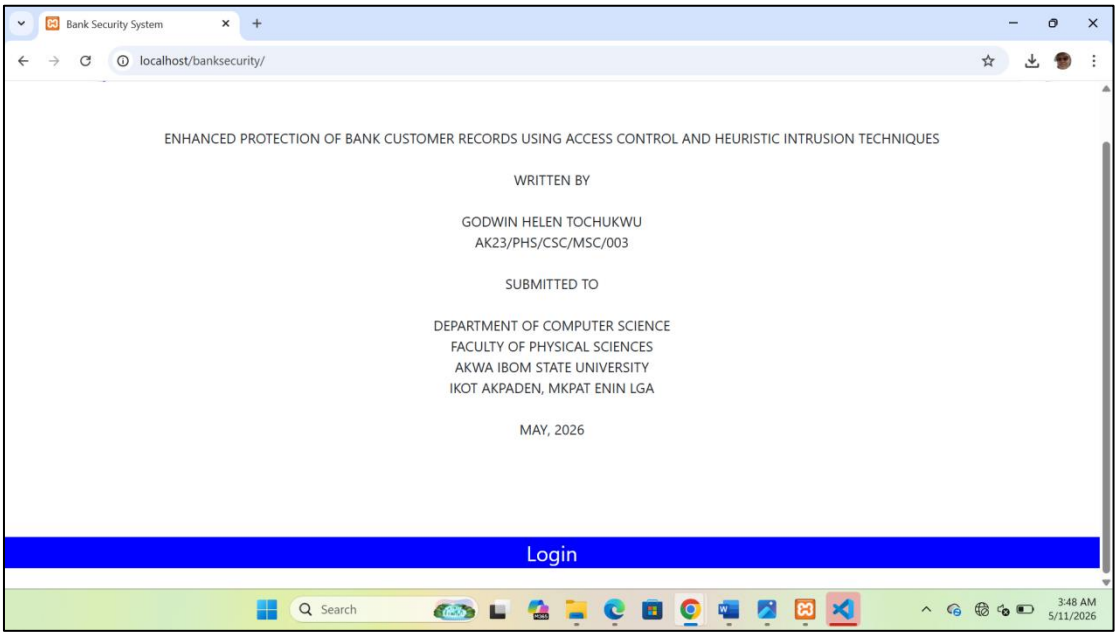


Figure 4: System Landing Page

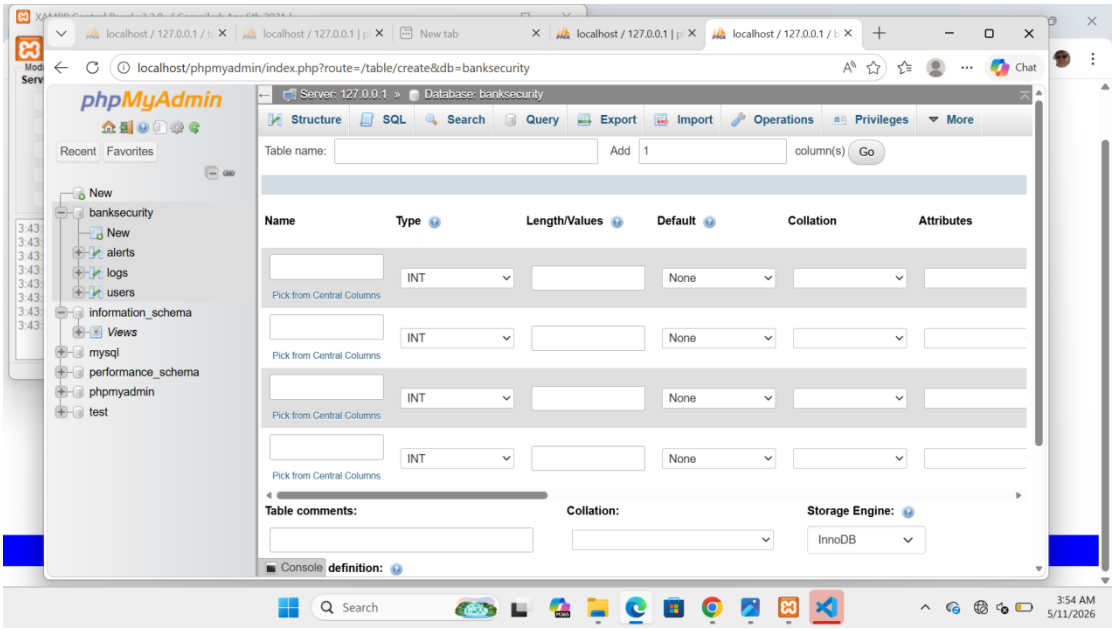


Figure 5: Database Construction Interface using Xampp

4.1.1 Roles and Permissions Table

The RBAC model uses roles to manage access permissions.

Role based support least privilege principle, enhances accountability, simplifies permission management, and reduce unauthorized access.

Table 5: Role Table

1	**Manager**	**Full permission**
2	Auditor	Limited permission
3	Account officer	Limited permission
4	Teller	Limited Permission

4.1.2 Automated Response Mechanisms (e.g., Session Suspension, Alerts)

The system automatically responds to detected threats.

4.1.3 Automated Responses

Table 6: Detection and Response

Threat detected	**Response**
Excessive login failures	Account suspension
Suspicious IP location	Location not allowed
Time of access	Outside allowed time
SQL injection attempt	Request blocked
Privilege Abuse	Alert Generation

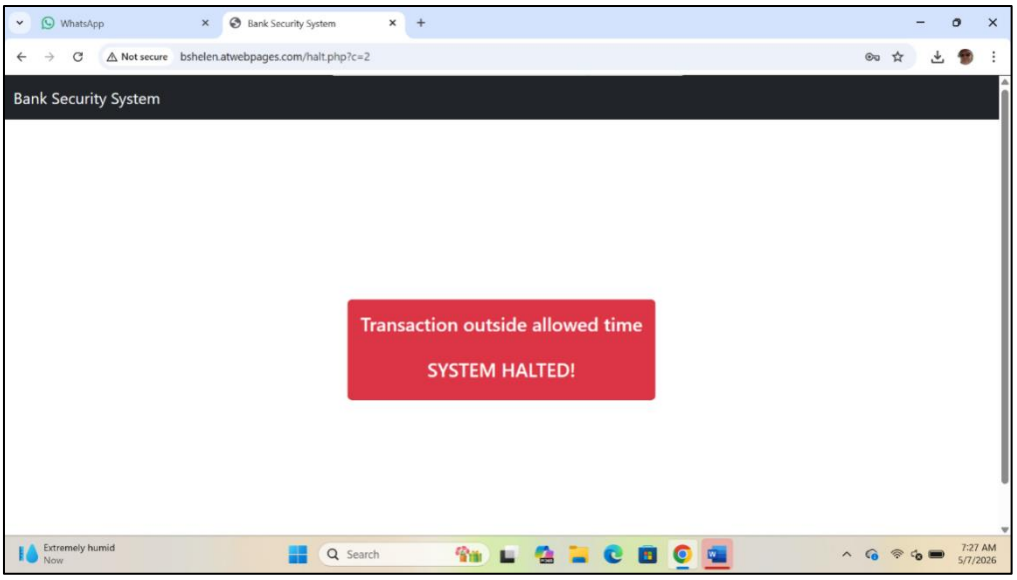


Figure 6: Restricted Transaction

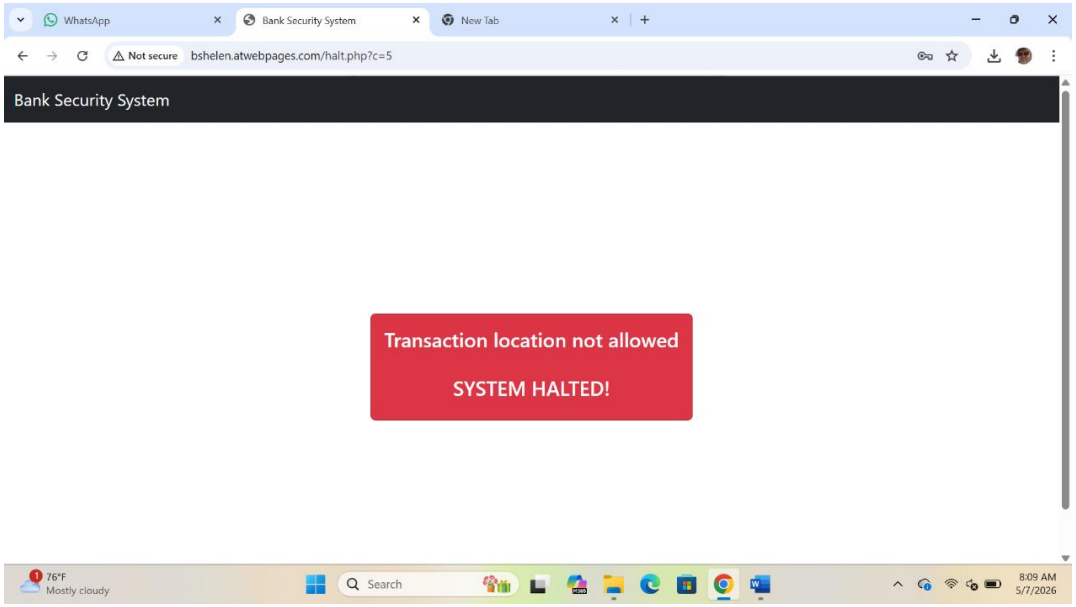


Figure 7: System Halted, Unrecognized Location

5 DISCUSSION

The study achieved the protection of bank customer records using Role-based access control model and heuristic intrusion detection, authentication, session management and role-based authorization.

The database has credentials that are used to verify user, password that are stored safely when a user successfully logs in, the system assigns roles to user and control access effectively.

The user is redirected based on their roles, the activities of user logged, audit trail records the time and details of interaction. The database system encrypts data and restrict or grants access by effective access management.

Furthermore, the system integrates heuristic intrusion techniques to detect suspicious behavior based on predefined rules. For example, the system restricts access based on the type of device used such as phones, tablet, laptop is not allowed access. Only desktop devices are permitted and any other device used will trigger system halted alert.

The system restrict access based on the location and permits desktops within the banking premises on the same internet protocol (IP) address.

The time of access is also considered, the time range spans between 8:00am to 5:00pm, the system flags halted before 8:00am and after 5:00pm, the event is logged while access is denied.

Heuristic rules are maintained for instance; maximum allowed attempt is 5times, multiple failed logins, unknown user name attempts, login outside working hours. The system logs all user activities for accountability and auditing.

The research addresses gaps in security enforcement and policies, this ensures that the system is monitored in real time and incident reported to the administrator. Thereby, reducing security vulnerabilities and enhance the protection of bank customer records.

6 CONCLUSION

The proposed system successfully combines access control mechanism with heuristic intrusion detection to improve confidentiality, integrity and availability of customer information. Access control ensures that only authorized user could access specific records based on their roles and permissions whilst intrusion detection identifies specific activities and potential threats in real time.

The implementation of the system using PHP, MySQL, HTML, CSS, Bootstrap and Apache Server environment demonstrate that modern web technologies can be used to build secure and reliable banking applications. The system improved security performance, reduce unauthorized access attempt and ensure monitoring capabilities.

In conclusion, the system provides a reliable approach for securing bank customer records against both internal and external threats. Therefore, Banks should adopt hybrid security mechanisms to protect customer records, thereby maintaining trust in digital banking systems.

The study achieved the protection of bank customer records using Role-based access control model and heuristic intrusion detection, authentication, session management and role-based authorization.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

[1] Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022, May). Cyber security threats on digital banking. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-4). IEEE.

[2] Bayram, U. (2020). *Semantic-Attribute Based Access Control* (Master's thesis).

[3] Chattopadhyay, R. (2024). AI-Driven Adaptive Encryption: Transforming Financial Data Security in the Age of Digital Banking. *Research Journal of Advanced Engineering and Science*, *9*(4), 281-290.

[4] Fareed, M., & Yassin, A. A. (2022). Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system. *Bulletin of Electrical Engineering and Informatics*, *11*(4), 2131-2141.

[5] Gangele, S. (2024). Data Security System for a Bank Based on Two Different Asymmetric Algorithms Cryptography. *International Journal for Multidisciplinary Research*, *6*(1).

[6] Ghazal, R., Qadeer, N., Raza, H., & Malik, A. K. (2024, April). Automated Semantic Role Mining Using Intelligent Role Based Access Control in Globally Distributed Banking Environment. In *International Conference on Information Technology-New Generations* (pp. 51-55). Cham: Springer Nature Switzerland.

[7] Han, U. S. S. (2020, February). Information Security Risk Management in Electronic Banking System. In *2020 IEEE Conference on Computer Applications (ICCA)* (pp. 1-6). IEEE.

[8] Haryaman, A., Amrita, N. D. A., & Redjeki, F. (2024). SECURE AND INCLUSIVE UTILIZATION OF SHARED DATA POTENTIAL WITH MULTI-KEY HOMOMORPHIC ENCRYPTION IN BANKING INDUSTRY. *Journal of Economics, Accounting, Business, Management, Engineering and Society*, *1*(9), 1-13.

[9] Irsyad, Z., & Indraningsih, N. H. (2024). The impact of end-to-end encryption on the security of digital banking transactions: an in-depth analysis. *Jurnal Mantik*, *8*(3).

[10] Jayasankar, T., Bhavadharini, R. M., Nagarajanz, N. R., Mani, G., & Ramesh, S. (2021). Securing Medical Data using Extended Role Based Access Control Model and Two fish Algorithms on Cloud Platform. *European Journal of Molecular and Clinical Medicine*, *8*(1), 1075-1090.

[11] Kumar, J., & Saxena, V. (2022). Rule-based credit card fraud detection using user's keystroke behavior. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2021* (pp. 469-480). Singapore: Springer Nature Singapore.

[12] Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, *135*, 450-466.

[13] Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*, *13*(1), 146.

[14] Saxena, U. R., & Alam, T. (2023). Role-based access using partial homomorphic encryption for securing cloud data. *International Journal of System Assurance Engineering and Management*, *14*(3), 950-966.

[15] Singh, M. P., Sural, S., Vaidya, J., & Atluri, V. (2024). A role-based administrative model for administration of heterogeneous access control policies and its security analysis. *Information Systems Frontiers*, *26*(6), 2255-2272.

[16] Subia, P. M. G., & Corpuz, R. R. (2020). Archiving and digitizing of customer records of golden rural bank of the Philippines, Inc. *International Journal of Scientific and Technology Research*, *9*(1), 1820-1823.

[17] Ullah, K., Rashid, I., Afzal, H., Iqbal, M. M. W., Bangash, Y. A., & Abbas, H. (2020). SS7 vulnerabilities—a survey and implementation of machine learning vs rule-based filtering for detection of SS7 network attacks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1337-1371.

[18] Razali, M. K. M., Ayob, M., Rahman, A. H. A., Jarmin, R., Liu, C. Y., Maaya, M., ... & Kendall, G. (2025). Unveiling Effective Heuristic Strategies: A Review of Cross-Domain Heuristic Search Challenge Algorithms. *Computer Modeling in Engineering & Sciences (CMES)*, *142*(2).

[19] Lin, D., Hu, S., Gao, Y., & Tang, W. (2019). Heuristic-learning-based network architecture for device-to-device user access control. *IEEE Communications Magazine*, *57*(11), 96-101.

[20] Agarwal, A., Arun, V., Ray, D., Martins, R., & Seshan, S. (2022, November). Automating network heuristic design and analysis. In *Proceedings of the 21st ACM Workshop on Hot Topics in Networks* (pp. 8-16).

[21] Zhu, R., Ayyappan, A., Varatharaj, J. R., & Jeya Sheela John, J. (2025). A standard network selection and resource allocation mechanism in 5G heterogeneous networks using hybrid heuristic algorithm with multi-objective constraints. *EURASIP Journal on Wireless Communications and Networking*, *2025*(1), 1-31.

[22] da Costa Reis, B. P., & Gharib, M. (2025). Towards an Approach for Designing Responsible Privacy Heuristics.

[23] Baihan, A., Ghith, E., Garg, H., Mirjalili, S., Izci, D., Rashdan, M., ... & Saleem, K. (2025). A Hybrid Meta-Heuristic Algorithm for Optimum Micro-robotic Position Control with PID Controller. *International Journal of Computational Intelligence Systems*, *18*(1), 86.

[24] Vijayan, R., Mareeswari, V., & Sridhar, K. (2025). Healthcare Data Security in Multi-Cloud Infrastructure Using Heuristic Algorithms. In *Role of Artificial Intelligence, Telehealth, and Telemedicine in Medical Virology* (pp. 253-267). Singapore: Springer Nature Singapore.

[25] Danach, K., Harb, H., Amine, S., & Belhor, M. (2025). NeuHH: A Neuromorphic-Inspired Hyper-Heuristic Framework for Solving the Capacitated Single-Allocation p-Hub Location Routing Problem. *Vehicles*, *7*(2), 61.

[26] Amirghafouri, F., Neghabi, A. A., Shakeri, H., & Sola, Y. E. (2025). Nature-Inspired Meta-Heuristic Algorithms for Resource Allocation in the Internet of Things. *International Journal of Communication Systems*, *38*(5), e6141.

[27] Matrouk, K. M., Rasappan, P., Bhutani, P., Mittal, S., Nisha, A. S. A., & Konduru, R. M. (2025). Development of Heuristic Strategy with Hybrid Encryption for Energy Efficient and Secure Data Storage Scheme in Blockchain-Based Mobile Edge Computing. *Transactions on Emerging Telecommunications Technologies*, *36*(2), e70057.

[28] Jarkas, A. M., & Doss, M. (2025). Optimized PI controller tuning for improved performance in BLDC motor speed control using heuristic adaptive lyrebird optimization algorithm. *Electrical Engineering*, 1-21.

[29] Chi, X., Chen, H., Ni, Z., Sun, H., Sun, P., & Yu, D. (2025). H-STEP: heuristic stable edge service entity placement for mobile virtual reality systems. *IEEE Transactions on Mobile Computing*.

[30] Huang, Z., Wu, W., Wu, K., Wang, J., & Lee, W. B. (2025). Calm: Co-evolution of algorithms and language model for automatic heuristic design. *arXiv preprint arXiv:2505.12285*.

[31] Amitu, D. M., Akol, R. N., & Serugunda, J. (2025). Hybrid access control mechanism for massive machine type communications. *Discover Internet of Things*, *5*(1), 1-17.

[32] Nurrizqi, A. Z., & Ramadhan, A. W. (2025, May). User Experience Evaluation of the BPK RI Portal: A Combined UEQ and Heuristic Approach. In *2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)* (pp. 1-6). IEEE.

[33] Liu, J., Tsang, E. W., & Shi, W. (2025). The superstitious heuristic in strategic decision making. *Journal of Management*, *51*(2), 843-874.

[34] Sarfaraz, A., Chakrabortty, R. K., & Essam, D. L. (2023). AccessChain: An access control framework to protect data access in blockchain enabled supply chain. *Future Generation Computer Systems*, *148*, 380-394.

[35] Mpamuga, Ezichi Happiness, (2024). *Enhanced network security model with Role-Based access control for mobile application.* (Master's thesis).

[36] Udoetor, N., Ansa, G., Ekong, A., & Edet, A. (2024). Intelligent system for detection of copyright-protected data for enhanced data security. Technology, 7(4), 58–80.

[37] Edet, A., Godwin, H., Chukwuemeke, O., & Hanson, Y. (2025). Economic and cost-benefit analysis of diabetes treatment: Correlating treatment cost with clinical outcomes using multi-regression approach. International Journal of General Scientific Research and Application, 1(1), 1–19.