http://dx.doi.org/10.21622/ACE.2025.05.2.1684

USING MULTILEVEL POLICY TO MITIGATE DATABASE THREATS FROM FORMER EMPLOYEES: A CASE OF PUBLIC SECTOR ORGANISATIONS IN ZANZIBAR

Rogers P. Bhalalusesa[1] and Ibrahim Salum Saleh[2]

[1-2] The Open University of Tanzania, Tanzania.

Emails: {rogers.balalusesa@out.ac.tz, ibraboras@gmail.com}

Received on, 21 September 2025 - Accepted on, 23 November 2025 - Published on, 30 November 2025

ABSTRACT

The purpose of this study was to develop a framework that employs multilevel access to enhance authentication mechanisms in public sector organisations and to restrict former employees whose prior elevated privileges could pose significant security risks if not effectively revoked. To achieve this purpose, the study identified multilevel policies used to control authentication in databases, examined the extent to which these policies can strengthen authentication in organisations, and developed an SQL procedure for multilevel security access authentication in database systems. Findings from the first objective revealed that most organisations have multilevel security access policies in place, which are primarily applied to database authentication based on the three security triads: confidentiality, integrity, and availability. Building on these policies, the second objective proposed a framework designed to enhance authentication and mitigate the risks posed by former employees. The framework defines three levels of authentication and recommends their Implementation in public sector organisations. For the third objective, the framework was evaluated by database administration experts using SQL procedures developed from the model, and results confirmed its effectiveness in addressing the problem of access control for former employees. The study recommends the adoption of the proposed three-level security architecture, in which protection begins at the portal (level 1), continues through the engine (level 2), and extends to the database (level 3).

Keywords: *Multilevel security policy; database threats; Security threats; Database Authentication.*

1. INTRODUCTION

In the digital era, information security has become a global concern, especially in organisations that manage sensitive data. Across the world, public and private institutions face persistent threats from unauthorized access, data breaches, and insider threats.[1]. It is believed that most of the security breaches are from hackers, but the reality of the problem is from insiders.[2]. Former employees who retain knowledge of or access to critical systems and sensitive information pose such threats. Traditional authentication mechanisms have struggled to keep pace with evolving cybersecurity threats, prompting the need for more robust, multilevel authentication frameworks that can provide layered protection for information systems.

In Africa, governments and public sector institutions are increasingly digitising services to improve efficiency, transparency, and service delivery. However, this shift has also introduced new vulnerabilities. Many African countries face challenges, including outdated IT infrastructure, limited cybersecurity expertise, and ineffective policy enforcement, which makes their systems more susceptible to unauthorized access and cyberattacks.[3]. The

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

risk is amplified when access privileges of former employees are not properly revoked, leading to potential data misuse or sabotage.[4].

In Tanzania, the digital transformation of the public sector has accelerated through various e-government initiatives aimed at improving public service delivery.[5]. As more government agencies adopt digital platforms and database systems, the need for secure access control has become critical. However, many public sector organisations in Tanzania still rely on basic or single-layer authentication systems, which are inadequate in managing modern threats. [6]. Former employees with prior elevated access pose a particular risk, as mechanisms for revoking or restricting access are often weak or inconsistently applied. This has highlighted the urgent need for a tailored, multilevel security framework suited to the Tanzanian context.

The main objective of this study is to develop a framework that uses multilevel access to enhance the authentication mechanism. The specific objectives of this research are first to identify the multilevel policies used to control authentication in databases, second to develop a framework using identity policy to control former employees, and last to evaluate the framework using SQL procedures.

The study aims to bridge the gap between database security authentication and the use of multilevel policy. The ICT expert expected to find the research findings important in the development of measures to address the problem of database security and thereby contribute knowledge to the community. By focusing on policies, technical procedures (SQL-based), and expert validation, the study responds to the growing cybersecurity needs of Tanzania and offers a scalable model that could also benefit other developing nations.

2. RELATED WORK

Previous studies have explored diverse approaches, ranging from network-based monitoring and behavioural analytics to multilevel access control and policy-driven database security. These works collectively aim to enhance system resilience by improving authentication processes, enforcing role-based access, and integrating automated decision mechanisms. However, the existing literature shows a gradual yet incomplete shift from reactive detection methods toward proactive, policy-oriented frameworks that can address outsider threats, including those posed by former employees with prior insider experience.

Several previous studies have addressed insider threats through network-based detection and prevention mechanisms, particularly targeting data-leak attacks in complex environments. For example, Sarhan and Altwaijry [7]. More recently, Tian et al [8]. These studies employ advanced monitoring of user activities, extracting attributes such as user behaviour sequences and network events, and matching them against dynamic detection models to detect and block malicious activity. However, they still primarily focus on detecting malicious actions after access has been granted, without enforcing stricter access restrictions at the entry point.

A study by Baracaldo et al [9]. The proposed framework considered current and historical geo-social information of insiders who are associated with access control decisions[9]. Such information included social networks, which are represented as social graphs, and the user mobility was represented as locations on maps.

Alsowai and Al-Shehari [10]. The framework encompasses virtual, non-virtual, and contextual factors, covering the entire insider lifecycle from pre-joining to post-departure, thereby offering a holistic understanding of insider threat problems. [11]. While the study highlights the critical issue of former users, it does not explicitly propose mechanisms for their detection.

Mostafa et al.[12] proposed the design and Implementation of multi-layer policies for database security, emphasizing their Role in monitoring intrusive behaviour and strengthening protection mechanisms beyond the control of database administrators or individual users. Each policy introduced a distinct security dimension, collectively enhancing database resilience through mechanisms such as Admin Initiation Policy, User Profile Policy, Secret Role-Based Access Control (RBAC), Separation of Duty (SoD), Intrusion Detection Policy, Authentication Factor

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

Policy, Cryptography Policy, and Authorization Policy.[12]. By integrating these policies, the framework defined the expected functions of a security system in a multilevel environment, highlighting the importance of adapting to operating system considerations and emerging modern technologies to ensure comprehensive database protection.

Ragavan and company proposed an approach to prevent unauthorized modifications by assigning a variable threshold to each data item in the database, such that any update exceeding the threshold would be blocked[13]. While effective to some extent, the approach addresses threats only after access has already been granted, leaving a significant vulnerability at the initial point of database entry.

A recent study by Abdulla and Aladdin developed a multilevel secure DBMS (MLS/DBMS) model that integrates authentication prototypes and cryptographic algorithms (RSA, AES) to enforce user-level access restrictions across different security classifications[14]. The system ensures that users can only access data they are authorized to view, effectively operationalizing multilevel security in modern relational database contexts. While this model demonstrates the feasibility of enforcing multilevel controls at the database level, it still highlights gaps in policy and integration at higher system layers (e.g., operating system or network layer), underscoring the need for comprehensive, cross-layer multilevel access control.

These related works demonstrate notable advancements in insider threat detection and database security, particularly through the use of behavioural analytics, access control frameworks, and multi-layered policy enforcement. While models such as those by Baracaldo et al.[9] Alsowai and Al-Shehari [10] and Abdulla and Aladdin [15] have contributed to a more comprehensive understanding of insider risk management; however, critical gaps remain for outside actors with the inside knowledge. These limitations underscore the need for a unified framework that combines proactive authentication, dynamic policy enforcement, and multilevel security mechanisms to effectively mitigate threats from the external actors who were once the internal actors when they were former employees. The framework proposed here addresses these limitations by leveraging the HR database to identify former employees, ensuring that the authentication procedure incorporates an access layer linked to HR records for stronger multilevel security.

3. METHODOLOGY

The research approach used was mixed research, which includes both qualitative and quantitative techniques. The use of a mixed approach was justified by the need to not only quantify the situational analysis data but also to capture expert opinions, user experiences, and organizational contexts that quantitative data alone could not adequately explain. Both qualitative and quantitative methods were used for objectives 1 and 2 to gather inputs for the proposed framework, and qualitative methods were used to evaluate the framework after development of an SQL procedure based on the framework.

The study was carried out in four (4) Government Institutions in Zanzibar that implement Relational Database Management System (RDBMS), such as the Business and Property Registration Agency in Zanzibar (BPRA), the Ministry of Finance and Planning, Zanzibar, the People Bank of Zanzibar, and ZCSRA (Zanzibar Civil Status Registration Agency)

To ensure equal representation from all organizations, both purposive and random sampling techniques were employed. Yamane's formula was used to determine the appropriate sample size. The initial population design was guided by the Central Limit Theorem (CLT), which supports the use of a minimum of 30 participants per group to approximate a normal distribution. [16]. The study assumed a minimum of 30 participants from each of the four organisations, resulting in a total population of 120 individuals. From this population, a sample size of 55 respondents was calculated using Yamane's formula with a 10% margin of error. [17]. However, due to incomplete responses in three questionnaires, the final analysis was conducted using 52 valid responses.

n = N/1+Ne2
Whereby:
n=required sample size
N= Population Size=120
e= margin error-10%
n=120/1+(120*0.1*0.1) =55

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

The study collected both primary and secondary types of data and used them to achieve the objectives of the research. Primary data was collected from an organization that used a database system, and persons operating the database were involved in the form of unstructured questionnaires because information could be collected systematically, and it was simple to code answers from respondents. Questionnaires involved both closed-ended and open-ended questions. Observation and documentation review were done. The collected data were analysed using SPSS computer software. Expert interviews were used to evaluate the SQL procedure and the framework.

4. SITUATIONAL ANALYSIS FINDINGS AND DISCUSSION

4.1. INTRODUCTION

Generally, the study was geared to develop and evaluate a framework that uses multilevel access policies to enhance the authentication mechanism. This section, therefore, shows how the analysis was performed, presented, and then discussed. The descriptive statistics were the major form of analysis, of which cross-tabulation is presented and interpreted to show how each variable contributed to the other. Also, the percentage distribution of the response was used to present the findings.

4.2. DEMOGRAPHIC CHARACTERISTICS

Though the demographic characteristics are not part of the main findings, it is important for the same to be presented to be familiar with the type of population the study dealt with. In this case, the age group, sex, and education level were studied. The cross tabulation is used to present the findings where the gender is taken as a dominant factor (the row) crossed against other factors, age, and education level. The results are presented in Tables 1 and 2.

Table 1: Gender vs Age and Education Level

Sex		level of Education			Total
		Diploma	Degree	Masters	
Female	Frequency	5	13	6	24
	Percent	45.45%	46.43%	46.15%	46.15%
Male	Frequency	6	15	7	28
	Percent	54.55%	53.57%	53.85%	53.85%
	Frequency	11	28	13	52
	Percent	21.15%	53.85%	25.00%	100.00%

Table 1 presents the distribution of respondents by gender and education level. Female participants constituted 45.1% of the total sample, of whom 9.8% held Diplomas, 23.5% held Bachelor's degrees, and 11.8% possessed Master's qualifications. Male respondents accounted for 54.9% of the sample, with 11.8% holding Diplomas, 29.4% Bachelor's degrees, and 13.7% Master's degrees. As shown in Table 2, respondents were distributed across various age categories. Among females, 34.1% were aged 20–29 years, 7.3% were aged 30–39 years, and 2.9% were aged 40–49 years. In contrast, 9.8% of male respondents were aged 20–29 years, 34.1% were aged 30–39 years, 9.8% were aged 40–49 years, and 2.4% were aged 50–59 years. Overall, these results indicate a fairly balanced representation across gender, Education, and age groups, suggesting that the dataset reflects diverse perspectives suitable for comprehensive analysis.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

Table 2: Gender vs Age

Sex		Age Group				Total
		20-29	30-39	40-49	50-59	
Female	Frequency	14	3	1	0	24
	Percent	77.78%	17.65%	20.00%	0.00%	46.15%
Male	Frequency	4	14	4	1	28
	Percent	22.22%	82.35%	80.00%	100.0%	53.85%
	Frequency	18	17	5	1	52
	Percent	34.62%	32.69%	9.62%	1.92%	100.0%

4.3. AVAILABILITY OF MULTILEVEL ACCESS POLICIES

The first objective of the study was to identify the multilevel policies used to control authentication in the database. A series of questions was asked to realize the objective. The results, as presented in Table 3, indicate the response rate to the question asked.

First, the respondents were required to indicate whether they have an ICT security policy, which is one of the multilevel access policies used to control authentication in an organization. The results, as indicated in Table 3, show that most organizations, i.e., 23.1%, have an ICT security policy that defines multilevel access policies as a requirement, which is used to control authentication. In contrast, 75.0% have no such policy, and 1.9% are unsure.

Table 3: Availability of Multilevel Policies

	Frequency	Percent	Valid Percent	Cumulative Percent
Missing	1	1.9	1.9	1.9
Yes	39	23.1	23.1	76.9
No	12	75.0	75.0	100.0
Total	52	100.0	100.0	

4.4. USE OF MULTILEVEL ACCESS TO CONTROL AUTHENTICATION

The survey examined how respondents access and are authenticated in their organizational databases, focusing specifically on those who indicated "YES" to having multilevel policies from section 4.3. Using a five-point Likert scale, the findings in Table 4 reveal strong agreement that most organizations implement authentication controls through defined security policies, with a mean score of 4.3 for the presence of password policies and guidelines. Similarly, database structures were reported to include security lists (mean = 4.2) and clearly defined user roles (mean = 4.1). The existence of database security policies and job segregation mechanisms both recorded mean scores around 4.0, while the ability to record user actions and control usage averaged 3.9, indicating moderate Implementation. Overall, the results confirm that organizations with established security policies maintain multilevel authentication controls that support the broader security principles of confidentiality, integrity, and availability.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

Table 4: Control Authentication in Database

Statement	1	2	3	4	5	Total	Mean
Does the organization's policy state the password policy and guidelines	1	2	2	21	26	52	4.3
Does the database structure consist of a security list	3	0	5	19	25	52	4.2
Does the database password verify the policy available	2	2	5	28	15	52	4.0
Does your database system define job segregation in your policy	3	0	10	19	20	52	4.0
Does the database record user action to control usage	2	2	13	18	17	52	3.9
Does the database system allow the owner to make changes as per the policy guidelines	3	7	12	16	14	52	3.6
Does your organization's policy define a user role for the database system	3	4	3	16	26	52	4.1

Key: 5=strongly agree, 4=agree, 3=neutral, 1=disagree, 1=strongly disagree

However, for those who indicated a "NO" response, they were required to give a reason to state why the organization has no multilevel policies, particularly the ICT security policy. It was identified that the common reason lies in financial, knowledge, or awareness of the importance of ICT policy, management support, and inadequate ICT specialized experts.

4.5. POLICIES USED TO CONTROL AUTHENTICATION IN AN ORGANIZATION

In this study, there was a room for the respondent to specify the policies that the user uses to make changes in the database systems. In this case, the responses were as few as indicated in Table 5. The results show that the ICT policy with defined multilevel access policies, which received a response of 32.7% states who is the one to make changes in the database system, while, in other organizations, the same is stated in the ICT security policy, which shows a response of 13.5% and the Acceptable ICT use Policy, with a response of 9.6%.

Table 5: Multilevel Access Policies

Policy	Frequency	Percent	Cumulative Percent
Acceptable ICT Use Policy	5	9.6	9.6
ICT security policy	7	13.5	23.1
None	12	23.1	46.2
ICT Policy	17	32.7	78.9
No idea	11	21.1	100.0

There are different types of policies; however, from the findings in Fig. 1, it is clear that users are not aware of which policy is used for what purpose. Thus, awareness is important.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

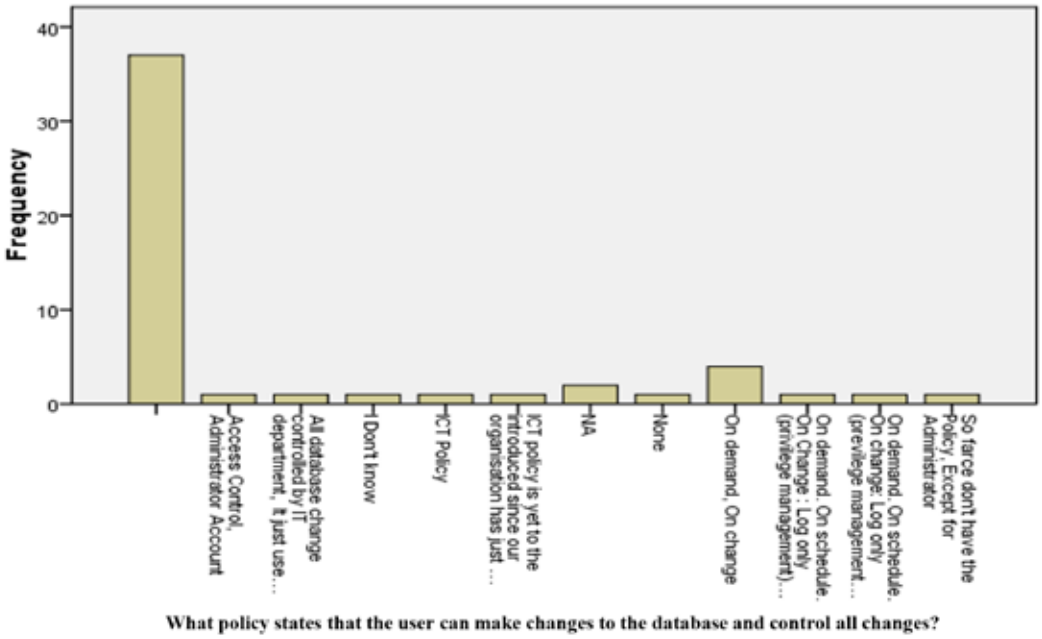

Figure 1: Access to Policy and Database Changes

For instance, according to the e-Government Authority, the ICT policy ensures that the Organisation's ICT-related investment, operations, and maintenance processes and usage are well directed[5]. On the other hand, the ICT security policy ensures that the information assets are protected from all types of threats, whether internal or external, deliberate or accidental. Apart from that, the Acceptable ICT Use Policy enables users to understand what is considered acceptable and unacceptable in the use of ICT resources of the Organisation.

5. PROPOSED FRAMEWORK

5.1. INTRODUCTION

The ultimate purpose of this study was to design and develop a Framework to Mitigate Authentication Threats in a Database Based on an Independent Multilevel Policy in public sector organisations. The rationale of the framework was also driven by the reason that access control is an important setting among security problems of resources in the database systems. The database system was considered because it is the data/information store through which access roles should be considered. The study adopted a Rule-Based Access Control model. The model allows the database or systems administrator to personalise the type of access to the users based on their roles within the Organisation. The framework allows multilevel access based on the access policies of the Organisation.

5.2. FRAMEWORK LEVELS

The proposed framework depicts three components, which are Access Level Policy, Role (User), and Implementation level (Management). The first component is the framework Access Level Policy. As shown in Fig. 2, the Access Level Policy defines the multilevel policy in ICT security policy, in which the level formulates the requirements of the policy and strategies to accomplish the policy. So, these influences define the action to be authenticated and execute the objective three to mitigate the threats to the database system.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

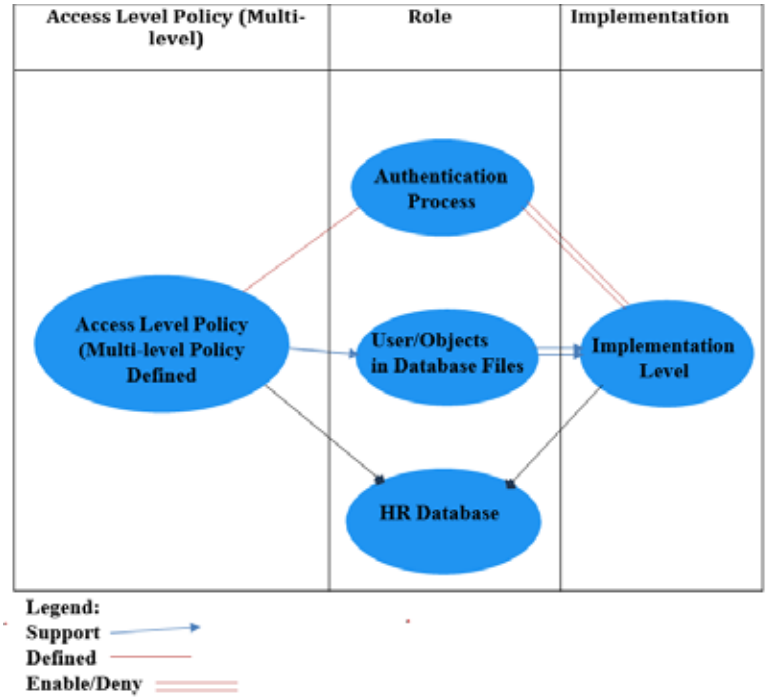

Figure . 2: Framework to mitigate the authentication threats process in the database using a multilevel policy

The second component of the framework is the Role. The framework developed a relationship between the policy and implementation strategy, in which the enforced policy utilizes the authentication process, users/objects, and the database itself to verify the existence of the policy defined in the database, thereby implementing the strategy that fulfills objective three of this study. An additional verification step that checks the human resource database to confirm whether a user still exists in the system is available to the role component. If verified, access to database objects is granted or denied based on the defined access-level policy requirements. In cases where the user is unauthorized, the multilevel policy enforces denial of access in accordance with established policy rules.

The third component of the framework is Implementation, which focuses on managing database security through effective authentication and user–object control as guided by existing policies. Access to the database is governed by a formulated policy that defines multilevel access controls within the database instance. Consequently, the enforcement of user roles plays a key role in mitigating potential threats and ensuring the overall security of the database system.

5.3. IMPLEMENTATION OF THE MULTILEVEL ACCESS POLICY IN THE FRAMEWORK

The proposed framework works by the principles highlighted by the Bell-LaPadula model[18]. Figure 3 below indicates how the framework implements multilevel access policies. Through the Bell-LaPadula model, a security level is assigned to transactions and data.[19]. A security level for a transaction represents its clearance level, and for data, the security level represents the classification level. Transactions are forbidden from reading data at a higher security level and from writing data to a lower security level. Thus, by delaying low-security-level transactions in a predetermined manner, high-security-level information can be indirectly transferred to the lower security level. In this case, a low security level transaction can be delayed or aborted by a high security level transaction due to shared data access.

The proposed policy facilitates access to data only after passing through multiple security levels. In this study, the use of multilevel access policies is applied for access control to different users depending upon the privileges given to them. The DBA is allowed to create database configuration-specific policies just for access control. These policies control and decide which changes are allowed and which ones are not. The framework gives the DBA the ability to institute a composite password where each part of the password is owned

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

by a different DBA team for added security. The purpose of using policies is to enforce DBA requirements and constraints on a database system. Policies are implemented into a database system for the purpose of making the database perform specific actions in response to attempts to alter its state or its configuration settings.

From the above developed model, the authentication factors defined include username, password, and IP address. The IP address is the last request after the user is successfully authenticated into the Database system by entering the username and password. In that case, the user's request, IP address, and digital credentials are forwarded to the preliminary access control system through passing the firewall, which filters the traffic based on the user's request. The preliminary access control is important to improve the system efficiency because the user's unauthenticated requests are terminated at an early stage. If the user's request is allowed by the preliminary access control, the user's request is forwarded to the security manager. The different request levels proposed are the user-level request and the confidential-level request, which are further divided into the secret-level request and the top-secret-level request. If the user is permitted access based on the user's access level, the query is limited to the user-level transaction; otherwise, the query is rolled back to confidential level security.

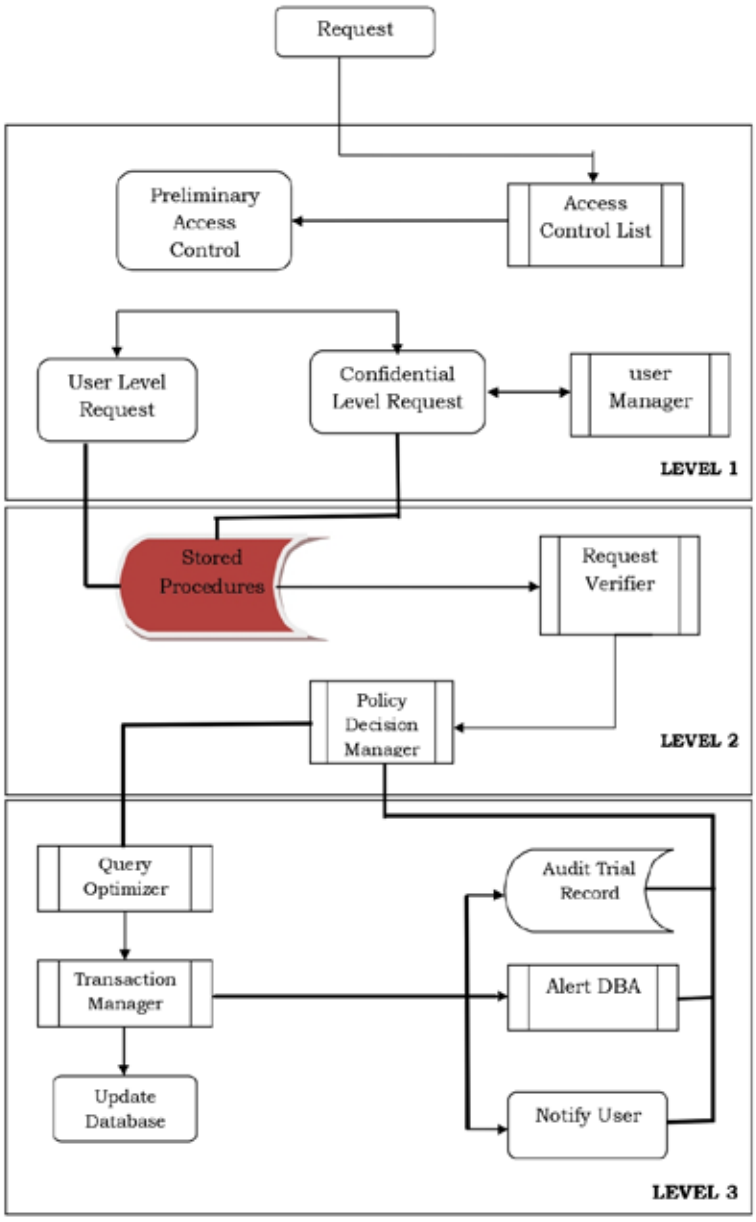

Figure 3: Mult-level Access Authentication in Database System

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

At the second access level, the user's request also goes through a process of verification before it can be processed. This step is carried out by database stored procedures that have built-in logic for checking the request against the policies. If the request complies with the set policies that govern its scope of applicability, the request is forwarded to the query optimizer. The query optimizer further divides the request into various levels for Database access and creates a new optimized query according to the data distribution. The transaction Manager pools the query in the transaction queue and allows the transaction to be executed. The lock signal is sent to all the Database sites. The transaction can update the data only when it passes all the clearance from all security levels; otherwise, it rolls back the transaction. When there is no objection from other sites, the audit trail, database system tables/views are updated to reflect the change, and an audit trail is recorded. Otherwise, the request is rejected, and the DBA is alerted, the user is notified, and an audit trail is recorded.

The main functions of the framework revolve around two things. First, the framework is able to control access to the database resources, and second, the framework covers the detection of unauthorised access.

5.4. PROCEDURE TO CONTROL ACCESS

The procedure diagram below is based on controlling access from unauthorised users. This follows granting access and specifying users, as explained in the SQL procedures. The access control refers to the idea of the framework through the system policy to define user roles and privileges. The system will first check based on the users' information previously saved in the database. Figure 4 shows how access control can be implemented in the database. It is in this articulatory function that the framework is facilitated by the information from the HR Database, as detailed in the section.

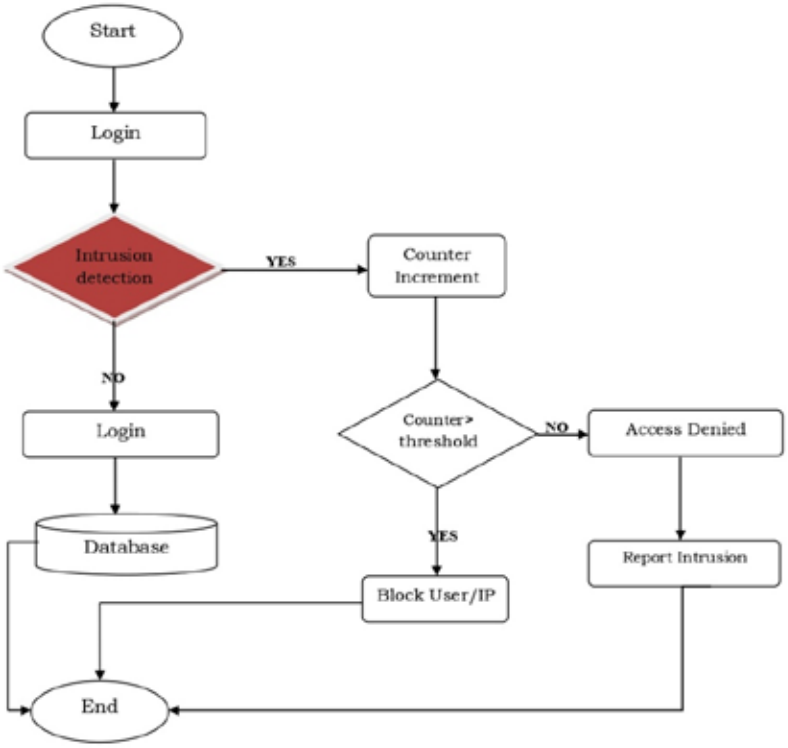

Figure 4: Flowchart of Access Control

Below is a pseudocode (Algorithm) based on controlling access from unauthorized users in terms of the actions to be executed and the order in which those actions are to be executed.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684


```
START
Log In
IF (Intrusion detection)
        counter increment
        if (counter > threshold)
                block user
        ELSE
                access denied
                report intrusion
ELSE
        Log In
        store login info
END
```

5.5. PROCEDURE TO DETECT THREATS

If an attack is not by the user in the organization, then it is by an outside attacker; then we proposed a high-level procedure for detection, which operates over the internet.

Figure 5 shows the procedure created to maintain a standardized and proper flow of the process of intrusion detection.

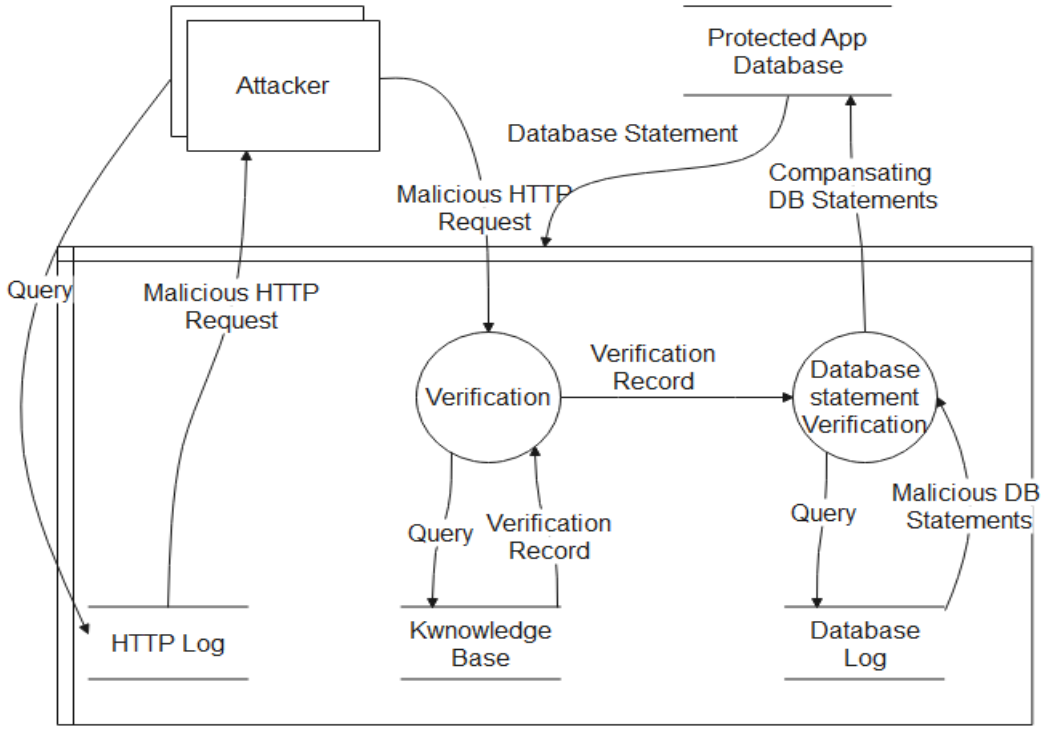

Figure 5: High-Level External Users Detection

The access control in Fig. 5 works the same as the former user's detection, except that in this case, the intrusion is from external (hackers). This applies only if the database can be accessed over the internet; thus, the attacker exploits the database through HTTP. Through http, the attacker accesses the database through the web address and send the SQL Query (SQL injection) to the Database system, the HTTP log database will store the request then the same is sent for verification, if the identity not match the records in the knowledge database or otherwise, it is returned to the verification process and record is sent to the database statement process for identity verification. If verified, the user is able to access the protected apps database, and if not, the user is not able to access the apps but returns a malicious database statement to DB statements verification, and the access is denied when accessing the secured database.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

5.6. PROCEDURE TO INTEGRATE HR DATABASE FOR FORMER EMPLOYEES

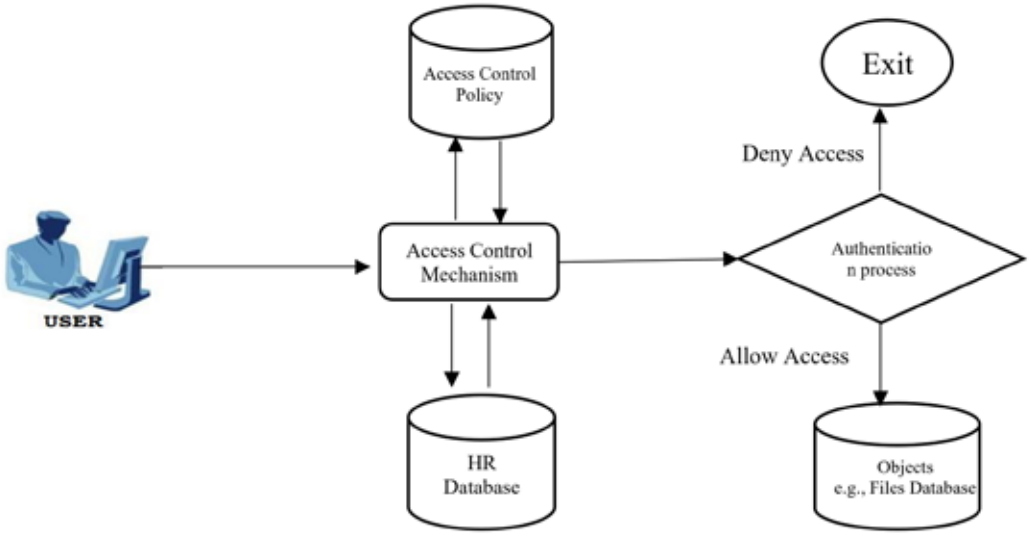

Figure 6: HR User Provide Role Level

The HR User provides a level of roles to the organization during registration and high-level authorization. The use of authentication flow and control access serves the purpose of limiting access to a single authentication at every level, as given by HR. Technical level extends the developed access control to the database multilevel in various central services (Denniss, 2019). The functionality of the developed control supports the requirements and contribution of HR to access control based on the query and technology at multiple levels in the Human Resource database.

The flow in Fig. 7 below describes a user authentication flow to match the developed framework in Fig. 2 above. The policy defined in the Role provides a relation for a user to implement the access granted. Whenever the framework is implemented, the authentication mechanism verifies the flow to match the Role developed.

The user and other entities are authenticated typically with other factors such as user ID, verifying user identity, user smart card, mobile device, or biometric data. The system or database matches the Role and implementation level, like an access list defined in the framework, assigns users to roles, and roles have specific permissions. This simplifies user management and reduces the need for individually managing permissions. These roles depend on the system, which can be either using a protocol or role-based access control (RBAC). So, the framework may differ according to the condition of the technology at the time.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

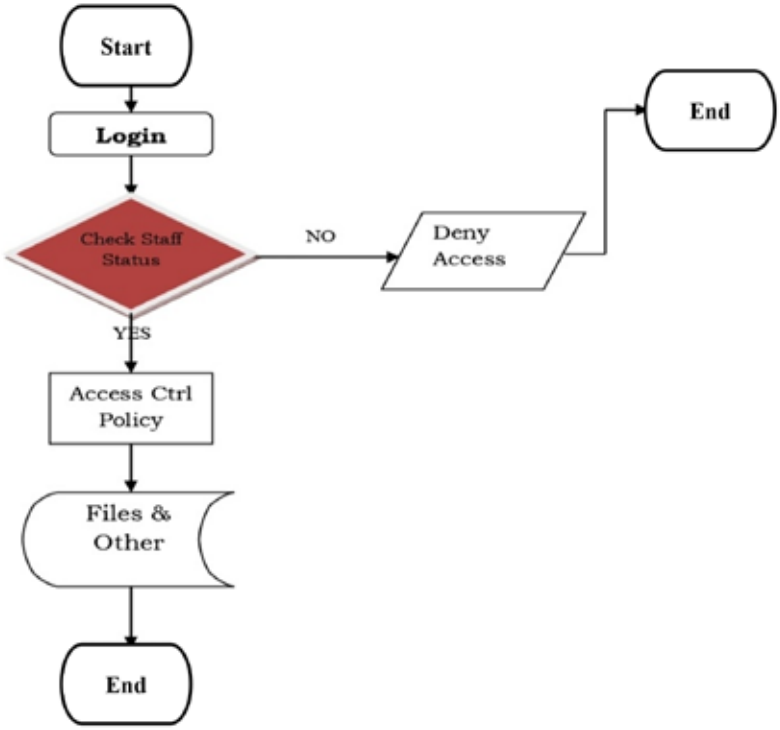

Figure 7: Authentication flow

Below is a procedure that checks and verifies user status (exists or does not exist) through the human resource database.

Require: username, passwd
Declare: count, username, passwd
Input data: Forms to fill in the data
IF username == passwd THEN
Redirect to access the database connection
ELSE
Check the wrong username or password matches 5 times

WHILE (count >= 5)
Access denied message,
END IF
END WHILE
END OF METHOD

6. FRAMEWORK EVALUATION USING SQL PROCEDURE

6.1. INTRODUCTION

In order to evaluate the multilevel access policy framework to see if it can truly control the access of former employees, SQL Procedures were developed. The SQL Procedures were then implemented in a testing environment, and Database Administrators (DBA) experts were interviewed to see the validity of the SQL procedures and to see if they conform to the framework and if the framework can control access of former employees. Section 4.2.6.1 gives the details of procedures, and Section 4.2.6.2 gives the report of the interview with DBA experts.

6.2. SQL PROCEDURE ON MULTILEVEL ACCESS AUTHENTICATION IN DATABASE

The third objective of the study was to develop an SQL procedure for multilevel security access authentication in a Database system. The procedure guides the access level of users in the Database system. The levels have been defined according to access roles to the respective users, of which the highest level is level 3 for system administrators,

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

level 2 for full access users, and level 1 for minimal access users. The system administrator goes beyond the access level of read and write access, but he can make changes such as deleting or disabling using, make changes to the database structure, and others. The full access users can access everything in the database system without restriction, different from the minimal access for the defined roles. The levels are also defined according to the advised security policy and the needs of the designed database.

1.1.1. Type 1; Top Security Level Policy

The purpose of this type is to verify and control the actions of privileged users; the database administrator in this case, and other power users, such as the head of the ICT unit in a public sector organization. The authentication process in this case is performed in response to the input of the user, as shown in the SQL code procedures. The database administrator is responsible for calling stored procedures. In this case, the DBA administrator restricts access to other users by defining the user roles in the system using a password. The procedure specifies a maximum lifetime for passwords. When the specified amount of time passes and the password expires, the user or DBA must change the password; otherwise, access to the account is denied until a new password is supplied.

The following statements create and assign a profile to user say Anna, and the PASSWORD_LIFE_TIME clause specifies that Anna can use the same password for 90 days before it expires. The permissible number of failed login attempts and the amount of time for which accounts remain locked are specified as 3 and 30 days, respectively. When a particular user exceeds a designated number of failed login attempts, the server automatically locks that user account. The account will unlock automatically after 3 days. After a user successfully logs into an account, the unsuccessful login attempt count for the user, if it exists, is reset to 0.

```
CREATE PROFILE prof LIMIT
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_LOCK_TIME 3
PASSWORD_LIFE_TIME 0;
ALTER USER john PROFILE prof;
```

The above SQL procedures are used to control access to unauthorized users who attempt to log in to the database without authorization.

1.1.2. Type 2: Grained Access Control Security Level

This access is based on dynamic, modified access. In this level, the DBA can change any option of a user's security domain by using the ALTER USER system privilege. This privilege is only designated to the DBA because it allows a modification of any user's security domain. The functions performed in this privilege include the ability to set table space quotas for a user on any table space in the database, even if the user performing the modification does not have a quota for a specified table space. When the security settings are changed, the next session of the user in the Database system will be affected; thus, the user will not be able to access data or information in the previous authorised access list. Therefore, by using the following SQL statements, the DBA will be able to change the access level or security settings of the user, say Anna.

```
ALTER USER Anna
IDENTIFIED EXTERNALLY
DEFAULT TABLESPACE data_te
TEMPORARY TABLESPACE temp_te
QUOTA 512M ON data_te
QUOTA 0 ON test_te
PROFILE read;
```

The ALTER USER statement here changes Anna's security settings as follows: Authentication is changed to use Anna's operating system account. Her default and temporary table spaces are explicitly set. She is given a 512 MB quota for the data_te table space. Her quota on the

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

test is revoked. She is assigned to the read profile.

1.1.3. Type 3: Controlled Access Security Level

This authorization is done to users only who can access data within the section, for instance, the examination section at university level, thus, the user does not expose examination results outside the examination section. The database connection in this case uses a dedicated one that one cannot connect to outside the connection. The SELECT command is used as shown below;

SELECT ENAME, Anna, John FROM emp, dept WHERE d.deptno = e.deptno AND d.dname="Exams";

In this case, it is important to note that the stored procedures do not allow the user to input values into variables. Instead, the procedures present the user with a set of values to select from. This is important because it removes any possibility of the users injecting variations into the expected input.

6.3. EXPERT INTERVIEW PROCEDURE AND FINDINGS

In order to confirm if the SQL procedures work well as part of the framework that controls the access of former employees, DB and HR experts used the SQL procedures, and they were interviewed afterwards. The outputs from the experts are described further in this section.

1.1.4. Expert Selection

Five experts in database administration and information security were purposively selected. Criteria for inclusion were:

1. At least five years of professional experience managing enterprise databases.
2. Direct involvement in identity and access management (IAM) or database security policies.
3. Demonstrated knowledge of SQL stored procedures and auditing mechanisms.

Experts were drawn from different organizations (two from financial institutions, one from higher Education, one from government, and one from a private ICT consultancy). This diversity provided a broad view of practical challenges in controlling former employees' access.

1.1.5. Data Collection Method

Semi-structured interviews were conducted over a period of two weeks. Each interview lasted approximately 45–60 minutes and was held either face-to-face or virtually (via Microsoft Teams).

A semi-structured guide was used to ensure consistency while allowing flexibility. The main themes included the following.

1. Framework constructs - Do the constructs (Identity Deactivation, Access Revocation, Audit & Logging, Policy Compliance, Residual Risk) reflect real-world needs?
2. Indicators - Are the chosen SQL-based indicators measurable and sufficient?
3. Implementation: Is the use of SQL stored procedures practical and secure in organizational settings?
4. Validity and reliability: How well does the framework align with existing best practices?
5. Limitations and improvements - What risks or blind spots remain unaddressed?

Interviews were audio-recorded and later transcribed for thematic analysis.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

1.1.6. Data Analysis

Thematic coding was applied to identify patterns across expert responses. Codes were grouped into three main categories.

- Validation of constructs (agreement, disagreement, modifications suggested)
- Practical challenges (e.g., data accuracy, timeliness, HR–IT integration)
- Recommendations (technical improvements, policy-level interventions)

1.1.7. Findings

1.1.7.1. Validation of Constructs

- All five experts agreed that the four constructs were necessary and sufficient to capture key aspects of identity control.
- Identity Deactivation and Access Revocation were emphasized as the highest priority.

1.1.7.2. Practical Challenges

- HR–IT synchronization: Delays in updating employment status can leave accounts active for days.
- Privileged accounts: Shared admin or service accounts pose risks because they do not map cleanly to individuals.
- Scalability: For large organizations, SQL procedures must be optimized to avoid performance bottlenecks.

1.1.7.3. Recommendations

- Automate triggers to disable accounts immediately upon status change rather than relying on batch jobs.
- Extend the framework to cover temporary staff and contractors.
- Integrate SQL-based outputs with SIEM (Security Information and Event Management) tools for continuous monitoring.
- Integrate AI in Threat detection and mitigation

1.1.7.4. Contribution to Validation

The expert interviews provided strong evidence of content validity (constructs reflect real-world needs) and practical feasibility (SQL procedures are implementable but need automation and monitoring). Experts also helped refine the framework by highlighting the following.

- The need to explicitly manage non-standard accounts.
- Importance of real-time enforcement.
- Need for integration with wider security ecosystems beyond SQL.

Thus, the expert feedback not only confirmed the reliability of the framework but also pointed to areas for future enhancement.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

7. CONCLUSION AND RECOMMENDATIONS

The study established that the proposed multilevel access control framework can play a significant role in enhancing database security within public sector organizations. A key contribution of this framework is its integration with human resource databases, which ensures that privileges are automatically revoked when an employee leaves the organization.

It is recommended that organizations adopt authentication systems that are directly synchronized with human resource records so that any changes in employment status, including resignations, transfers, or terminations, are immediately reflected in database access permissions.[4]. In addition, organizations should conduct periodic audits of database user accounts and access logs in order to identify and deactivate dormant accounts that may be exploited by malicious actors.[20]. Continuous monitoring tools should be deployed to detect unusual patterns of access, particularly attempts by former employees. Alongside technological interventions, there is a need to build capacity among IT administrators and HR personnel on access control procedures to ensure that the framework is implemented consistently and effectively. Finally, for sustainability, the multilevel access control framework should be embedded within official organizational policies and aligned with broader information security strategies, thereby institutionalizing secure practices across the organization.

While the framework demonstrates effectiveness in controlling access and restricting former employees, future studies could explore its integration with advanced technologies such as artificial intelligence and machine learning to enhance anomaly detection[21], [22]. Intelligent systems could identify suspicious access patterns in real time, thereby strengthening the proactive elements of access control. Moreover, as many organizations are transitioning to cloud-based infrastructures, there is a need to adapt and extend the framework to support distributed and hybrid environments where identity management becomes more complex.

In conclusion, the multilevel access control framework offers a practical and scalable approach to safeguarding organizational databases, with clear policy and operational implications. Its adoption, combined with technological, procedural, and organizational measures, can significantly reduce the risks posed by former employees and other insider threats, while laying the groundwork for more intelligent and adaptive security systems in the future.

REFERENCES

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," 2024. doi: 10.1016/j.csa.2023.100031.

[2] R. B, L. K, I. M, and P. S. H, "Distributed Scheme to Authenticate Data Storage Security in Cloud Computing," International Journal of Computer Science and Information Technology, vol. 9, no. 6, pp. 59–66, Dec. 2017, doi: 10.5121/ijcsit.2017.9606.

[3] M. R. Mphatheni and W. Maluleke, "Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions," International Journal of Research in Business and Social Science, vol. 11, no. 4, 2022.

[4] G. Silowash, T. J. Shimeall, D. Cappelli, A. Moore, L. Flynn, and R. Trzeciak, "Common Sense Guide to Mitigating Threats," 2012.

[5] M. Dewa and I. Zlotnikova, "Current Status of e-Government Services in Tanzania : A Security Perspective," Advances in Computer Science: an International Journal, vol. 3, no. 3, 2014.

[6] D. FELIX, "Investigating Human Factors Compromising the Security of Information Systems in the Public Sector in Tanzania," IAA, 2023.

[7] B. Bin Sarhan and N. Altwaijry, "Insider Threat Detection Using Machine Learning Approach," Applied Sciences (Switzerland), vol. 13, no. 1, 2023, doi: 10.3390/app13010259.

http://dx.doi.org/10.21622/ACE.2025.05.2.1684

[8] T. Tian, C. Zhang, B. Jiang, H. Feng, and Z. Lu, "Insider threat detection for specific threat scenarios," Cybersecurity, vol. 8, no. 1, p. 17, Mar. 2025, doi: 10.1186/s42400-024-00321-w.

[9] N. Baracaldo, B. Palanisamy, and J. Joshi, "G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework," IEEE Trans Dependable Secure Comput, vol. 16, no. 1, pp. 84–98, Jan. 2019, doi: 10.1109/TDSC.2017.2654438.

[10] R. A. Alsowail and T. Al-Shehari, "A Multi-Tiered Framework for Insider Threat Prevention," Electronics (Basel), vol. 10, no. 9, p. 1005, Apr. 2021, doi: 10.3390/electronics10091005.

[11] R. A. Alsowail and T. Al-Shehari, "A Multi-Tiered Framework for Insider Threat Prevention," Electronics (Basel), vol. 10, no. 9, p. 1005, Apr. 2021, doi: 10.3390/electronics10091005.

[12] A. M. Mostafa, M. H. Abdel-Aziz, and I. M. El-Henawy, "Design and implementation of multi-layer policies for database security," Information Sciences Letters, vol. 2, no. 3, pp. 147–153, Sep. 2013, doi: 10.12785/isl/020303.

[13] H. Ragavan and B. Panda, "Mitigating Malicious Updates: Prevention of Insider Threat to Databases," in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, Jul. 2013, pp. 781–788. doi: 10.1109/TrustCom.2013.95.

[14] H. S. Abdulla and A. M. Aladdin, "Enhancing Design and Authentication Performance Model: A Multilevel Secure Database Management System," Future Internet, vol. 17, pp. 1–22, 2025, [Online]. Available: https://ideas.repec.org/a/gam/jftint/v17y2025i2p74-d1586426.html

[15] H. S. Abdulla and A. M. Aladdin, "Enhancing Design and Authentication Performance Model: A Multilevel Secure Database Management System," Future Internet, vol. 17, no. 2, p. 74, Feb. 2025, doi: 10.3390/fi17020074.

[16] D. S. Moore, G. P. McCabe, and B. A. Craig, Introduction to the Practice of Statistic, vol. 4. WH Freeman New York, 2009.

[17] A. M. Umar and B. Wachiko, "Method for sample size calculation," Mathematical Association Of Nigeria (Man), vol. 46, no. 1, p. 188, 2021.

[18] M. Cristiá and G. Rossi, "Automated Proof of Bell–LaPadula Security Properties," J Autom Reason, vol. 65, no. 4, pp. 463–478, Apr. 2021, doi: 10.1007/s10817-020-09577-6.

[19] R. Zhang, G. Liu, H. Kang, Q. Wang, Y. Tian, and C. Wang, "Improved Bell–LaPadula Model With Break the Glass Mechanism," IEEE Trans Reliab, vol. 70, pp. 1232–1241, 2021, doi: 10.1109/tr.2020.3046768.

[20] J. E. Thy and L. Knutsen, "Leveraging Physical Access Data: Detecting Malicious Insider Activities During Employee Offboarding," Ntnu.no, 2025, doi: no.ntnu:inspera:300877113:360135215.

[21] A. Ali, M. Husain, and P. Hans, "Real-Time Detection of Insider Threats Using Behavioral Analytics and Deep Evidential Clustering," 2025. [Online]. Available: https://arxiv.org/abs/2505.15383v1

[22] C. Reddy, S. Prabhagaran, and A. Vaid, "Adaptive Anomaly Detection in Database Transactions: Bridging Security Gaps with Reinforcement Learning," European Journal of Artificial Intelligence and Machine Learning, vol. 4, no. 2, pp. 8–14, Apr. 2025, doi: 10.24018/ejai.2025.4.2.53.