Chapter 13
Effective Security and Access Control Framework for Multilevel Organizations

Ei Ei Moe and Mie Mie Su Thwin

13.1 Introduction

13.1.1 Introduction

The relevant data is a valuable and vital asset for most commercial organizations. Today, the business competitions among business organizations are highly raised so data assets must to be prevented from unauthenticated access and malicious operations. Access control is a principal concept in understanding computer and network security and access privacy to protect data, intellectual property, physical equipment, and systems from accident or intentional damage. One of the technologies that organizations have used to achieve this is access control. By making information resources accessible to only authorized users, the mechanism ensures that only information is always available to those permitted to access it. In large and complex multilevel organizations, it allow users with many clearance, authorization, and need to know ability to ensure that accessing given resources or information in system without risk of compromise. In MAC mechanisms, given resources are categorized with a specific classification level, and each user is specified a certain authorization level.

E. E. Moe (✉)
University of Computer Studies, Yangon, Myanmar
e-mail: eieimoe@ucsy.edu.mm

M. M. S. Thwin
Cyber Security Research Lab, University of Computer Studies, Yangon, Myanmar
e-mail: drmiemiesuthwin@ucsy.edu.mm

G.R. Sinha (ed.), *Advances in Biometrics*,
https://doi.org/10.1007/978-3-030-30436-2_13

13.1.2 Objectives of the Proposed System

Objectives of the proposed framework are as follows:

- To observe the security control policies for information management systems.
- To apply the security mechanisms for internal and external threats in a complex multilevel organizations.
- To use accurate access control mechanisms and policies depending on the nature of organizations.
- To propose an effective security framework for multilevel organizations.
- To implement secure and trusted information system by concentrating on aspects of computer security attacks and vulnerability.

13.2 Related Work

Database security means system, processes, and procedures which prevent the organization's database from unintended and unknown actions [1]. The authorized individuals or processes can make authenticated misuse, malicious attacks, or inadvertent mistakes. Fundamentally, there are two types of database security, DAC and MAC also called multilevel security (MLS). In this paper we will describe how to control banking database system by using MLS techniques. In the case of MAC, each subject is given a certain clearance level, and each object is labeled with a certain classification. The specific object can be accessed only by authorized users with right clearance level. Our system is intended to provide right access control based on user's roles that are assigned according to the enterprise's policy decision. Users who own right access account can manage data from database server.

The system is intended to provide right access control based on user's roles that are assigned according to the enterprise's policy decision. In the system, the administrator can access all data and can make all transactions of the whole system and the data occupation of the respective level. The system users have project manager (level 4), assistant manager (level 3), team leader (level 2), and developer (level 1).These levels are defined by the system administrator. User who owns right access account can manage data from database server [2].

Database security and integrity are vital aspects of an organization's security posture [3]. Database security is the system, processes, and procedures that protect a database from unintentional actions. It is important to develop a security model and policies for every system that use database to store data. The various different security models can solve many security problems. All security models' aim is to outline a system authorized and unauthorized conditions and to constrain the system to move into an unauthorized and unsafe state. Security models of the implemented system can rely on either mandatory or discretionary access control mechanisms. In this paper, the main intention is to implement Biba's Ring Policy that is used to maintain integrity of resources and to provide right access control based on user's roles and attributes that are assigned according to UCSY's attendance policy decision in online attendance marking system – a system that will replace paper-based attendance into digital attendance system.

13.3 Background Theory

Computer security is concerned with five aspects:

Confidentiality: It means that sensitive data or information belonging to an organization or government should not be accessed by or disclosed to unauthorized people. Such data include employees' details, classified military information, business financial records, etc.

Integrity: This means that data should not be modified without owner's authority. Data integrity is violated when a person accidentally, or with malicious intent, erases or modifies important files such as payroll or a customer's bank account file.

Availability: The information must be available on demand. This means that any information system and communication link used to access it must be efficient and functional. An information system may be unavailable due to power outages, hardware failures, and unplanned upgrades or repairs.

Authenticity: It is the confirmation of the identity of the user. It is accomplished through something only the user knows, i.e., password; using what the user has, i.e., badge and smartcard; and something that the user is, e.g., biometric analysis, i.e., finger prints, voice recognition, retina, face recognition, etc.

Non-repudiation: It is the assurance that someone cannot deny the validity of something. It offers the ability to decide whether a specified individual took a certain accomplishment such as message sending, information generating, or approving and message receiving.

13.3.1 What Are External and Internal Threats?

Everything or everyone that can cause risks to computer system of organization, computing resources, users, or data owned by business is called threats.

External threats are initiated from an outsider of an organization, mainly from the environments in which the organization makes their operations. The attackers perform various attacks by stealing credentials of a legitimate. Examples of external threats are hacking, code injection attacks, malware, phishing, corporate espionage/competitors, and business partners/contractors.

The second threats initiate from inside the organization. The employees or providers to whom work is outsourced are the key contributors for causing internal threats. Frauds, exploitation of information, damage of information, and sensitive data leakage within organization are the main threats for that organization. Mostly, the employee in every organization can be biggest threats rather than hackers outside the organization.

13.3.2 Security Control Model

An organization should define its security strategies and plans. An organization can use a security model to support the workplace policies or IT security guidelines to be applied in an organization's computer system.

Security Policy
A security policy is a specialized paper which outlines how to protect the organization from threats, including types of computer security threats, and how to handle situations when they do occur. It manages a set of security procedures and purposes desired by an organization. The security policy must identify all of a company's assets and resources as well as all the potential threats to those assets.

Security Model
A security model is a framework in which the security policy is developed for the security needs of organizations. The security control models are used to outline how security patterns will be implemented, what users can access the system, and which information they will have read or write. Essentially, they are a way of defining security policies between users and organization. Security models are generally implemented with integrity, confidentiality, and other essential security controls.

13.3.3 Bell-LaPadula Model

The security model was created for preventing access to objects (data) in a system. It is the first mathematical model that applied a multilevel security policy that is used to express a secure state machine concept.

The properties of this model are as following:

- Simple security property mentions that a given subject at a security level cannot read objects that exist in at a higher security level.
- Star property mentions that a given subject in a security level cannot write objects to a lower security levels.
- Strong star ($_*$) property mentions that a subject cannot read or write to objects at higher and lower levels.

A problem of this model is it does not perform the integrity of data, although all mandatory access control systems are based on the Bell-LaPadula model.

13.3.4 Integrity

The integrity denotes that the trust worthiness of data or business assets. It plays an important role in IT security and defined the processes of preventing improper and unauthorized changes to the data. Although governmental entities are usually concerned with confidentiality, other business and education organizations might be more focused on the integrity of information.

Generally, four main goals of the integrity are:

1. Prevention of making modifications to data or programs by unauthorized parties.
2. Prevention of making improper or unauthorized modifications by authorized parties.
3. Maintaining external and internal consistency of programs and data.
4. Reflecting the real world by ensuring transition to use data accurately.

13.3.5 Levels of Integrity

Levels of integrity are labels which consist of two parts:

1. Level of Classification

   The form of classification is a hierarchical set.

   Crucial, important, and insignificant can be divided as the example of classification. The highest level is crucial and insignificant as the lowest level. For this case: crucial > important > insignificant.
2. Set of Categories

   This is a compartment which contains label that can be a subset of system's all the sets. The nonhierarchical form is the form of a set of categories.

All subjects and objects in the system give integrity levels. The integrity levels become a dominance relationship between subjects and objects in system. The integrity label corrects the confidence level that may be retained in the data.

13.3.6 Strict Integrity Policy

This policy is an integrity policy and involves among the types of mandatory access control. It is also the dual of Bell-LaPadula model and basically has the following three defining properties.

The *simple integrity property* means the subject can only read objects at its integrity level or above level. The subjects can read objects only if i (o) is greater or equal to i (s).

The *integrity* property* means the subject can only write objects at its integrity level or below level. The subjects can write to objects only if i (o) is less than i (s).

A subject with low integrity level is prohibited from invoking or calling up a subject with a higher level of integrity is called *invocation* property.

13.3.7 Strict Integrity Access Control Model

In the meantime it is an access control policy, it can be represented as the access control matrix. Assume that H (high level) > L (low level) > VL (very low level) are hierarchical integrity levels (Fig. 13.1).

13.3.8 Conditions of Integrity

- Simple integrity condition is also known as "no read down" axiom (Fig. 13.2).
- Integrity star property is also known as "no write up" axiom (Fig. 13.3).

13.3.9 Levels of Entity to Control Security

A reliable computer system ensures that preventing access to objects based on the sensitivity (label) of the information contained in that objects and the proper authorization (clearance) of subjects to get given access to specific objects in the system. A subject is an active entity that makes request to objects and an object is a passive entity that consists of information. Security labels denote the security sensitivity level of:

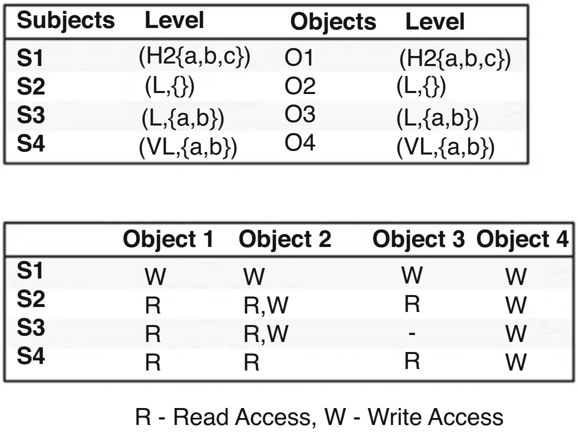


Fig. 13.1 Access control matrix between subject and object

Subjects	Level	Objects	Level
S1	(H2{a,b,c})	O1	(H2{a,b,c})
S2	(L,{})	O2	(L,{})
S3	(L,{a,b})	O3	(L,{a,b})
S4	(VL,{a,b})	O4	(VL,{a,b})

	Object 1	Object 2	Object 3	Object 4
S1	W	W	W	W
S2	R	R,W	R	W
S3	R	R,W	-	W
S4	R	R	R	W

R - Read Access, W - Write Access

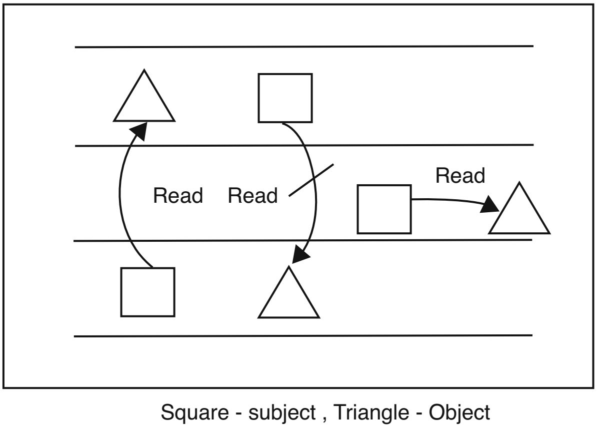
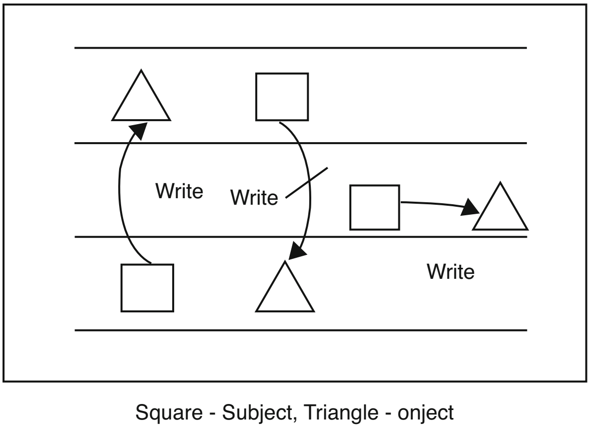


Fig. 13.2 Simple Integrity Condition

Fig. 13.3 Integrity star property



- Subjects that are given clearances labels.
- Objects that are given classifications labels.

Clearance label is considered as security level that an individual user can access the data. This is usually related to a "need to know" necessity. When the clearance and classification labels work together, a user's clearance is a restriction to the access of resources based on their classification.

Each desired security control level is supposed to govern itself and all others below it in this hierarchy structure.

13.4 Access Control

It governs who can access, place, or use what resources in a computing atmosphere and is also an essential component in security. It minimizes the risks of unauthorized access for businesses or organizations. Access control ensures that an acting authenticated user can access only what they are authorized to and nothing more. Generally, access control involves user identification, authorization, authentication, accountability, and audition concepts.

13.4.1 Identification

Identification defines a method to ensure that a subject (e.g., user, program, or process) is the entity it claims to be. It can provide using valid identity such as username or account number and password.

13.4.2 Account Authentication

The authentication is the most elementary requirement for handling of user access in the system. The user authentication comprises the user is who he claims to be actually. In the user authentication process, the subject is always required to enter a second part to the credential set such as password, personal identification number (PIN), or cryptographic key.

13.4.3 Authorization

The subject is actually authenticated when the credentials of identification and authentication match the stored information in database of the system. The system tries to control the access to resources for subject after the subject is authorized.

13.4.4 Accountability

Accountability mechanism keeps track of subject actions in the system. It keeps track of who, when, and how the subjects access the system. It helps in identifying authorized and unauthorized activities between the subject and object.

13.4.5 Types of Access Control

The organizations can apply diverse access control models that depend on their business policies or compliance need and the security levels of organization they want to guard. The core access control types are:

Mandatory access control (MAC) sets access rights by a system administrator (central authority) based on multiple levels of security. This mechanism assigns all resource objects with security labels in the system. These security labels are divided into two information parts: a classification (secret, confidential, unclassified, etc.) and a set of category (the management level, department, or project).

In *discretionary access control (DAC)*, administrators of the protected system set data or resources with the specified policies in which who or what gives authorization to access them. It allows individual user to control access to their own operations and data.

Role-based access control (RBAC) is also known as non-discretionary mechanisms. This mechanism limits access to resources based on individuals or groups with specific functions rather than the identities of individual users. It gives permissions to particular roles that have assigned by the users in an organization.

Rule-based access control model in which the system administrator defines a set of security rules allows or denies access to specific objects by subjects. These often depend on circumstances such as time of day or location.

Attribute-based access control (ABAC) is known as a policy-based access control that evaluates a set of policies, rules, and relationships by using the attributes of users, systems, and environmental situations to manage access rights for users. A key difference among these mechanisms is the concept of policies precise a complex Boolean rule set that can evaluate many different attributes.

13.5 Biba Security Model

Although many governments are principally concerned with confidentiality, most businesses wish to ensure that the integrity of the information is protected at the highest level. When the protection of integrity is vital, Biba is the model of choice by most organization. Bell-LaPadula model cannot grantee data integrity but can offer confidentiality of data. So, this integrity model addresses the requirement of enforcing integrity for such computational environment.

13.5.1 Access Modes of Biba Model

The Biba Model involves the type of access modes. Although these modes of access use different definitions to express them, they are similar to those used in other models. The access modes that can support Biba Model are:

1. Modifying mode permits writing to an object by a subject and is similar to the write mode of another models.
2. Observing mode permits reading to an object by a subject and is a synonym with the read command of other models.
3. Invoking mode permits a subject to interconnect with another subject.
4. Executing mode permits executing an object by a subject. The command essentially allows executing a program which is the object by a subject [4].

13.5.2 Policies of Biba Model

The Biba Model can be separated into mandatory and discretionary policies as two types of policies according to the need of the system.

Mandatory policies in Biba Model are:

1. Strict Integrity Policy.
2. Low-Water-Mark Policy for Subjects.
3. Low-Water-Mark Policy for Objects.
4. Low-Water-Mark Integrity Audit Policy.
5. Ring Policy.

Discretionary policies in Biba Model are:

1. Access Control Lists.
2. Object Hierarchy.
3. Ring Policy.

Biba Model also uses labels to define security. The labeling technique of Biba Model is used to provide integrity levels for the subjects and objects in the system. The labeled objects with a high level of integrity will be more sensitive and accurate than the labeled objects with a low level. The integrity levels are used to restrict the unsuitable modification of data and allow the right operations on that data.

13.5.3 Advantages and Disadvantages of Biba Model

There are many pros in using Biba Model in organizations' security. The Biba Model is simple and can be implemented easily. This model also can provide many different policies based on the different organizations' nature and necessities.

The Biba Model also has some disadvantages. The first issue is that the programmers need to use the right policy and rules according to the implementation of different organizations' security. The second disadvantage is that the Biba Model does not perform about confidentiality, while the Bell-LaPadula can enforce.

Moreover, the Biba Model does not support the granting and revocation of authorization. So access control mechanisms can achieve this failing mechanism. The last disadvantage is that to use this model, all computers in multilevel organizations must provide labeling of integrity for both subjects and objects. There are problems in using Biba Model in the network environment because the labeling techniques cannot be supported by network protocol.

13.6 Security Controls

The security safeguards and security controls in such information security system are capable of several criteria such as preventing security incidents, minimizing risks, detecting attackers, and recovering damage to normal state. For multilevel organizations, it must consider the effective security control mechanisms to become more secure and safe. A number of different types of user such as unknown guest users, administrative users, and regular authenticated users may be consisted in multilevel organization's environment. The different set of data and resources are permitted to access by many users. It will discuss the following necessary security controls for information security management system of that organization.

13.6.1 Account Authentication Control

This is the handling of user request to the system and is also the most basic dependency. The user authentication involves proving that a user is in fact who he or she claims to be. If there is no such facility, the system will assume all users as unknown which is the lowest possible level of trust. Most systems use the simple authentication method in that the user submits username and password for checking account validity [5]. But this proposed system uses two-factor authentication mechanism to avoid SQL infection attack.

13.6.2 Handling User Access Control

It is making to impose correct decisions about whether each individual user request should be allowed or denied in the process of handling user access. If this is functioning correctly, the system detects the identity of the user from whom each request is received [5]. Access control mechanisms can support the need to know restriction. The need to know ability ensures that only authorized users gain access to information or systems necessary to accept their responsibilities. To approve these control mechanisms, access control is used as basic theory.

13.6.3 Using User Input Control

The users in most organizations often have not been potentially aware of the risky faults they're making. The documents are put onto unsecure cloud apps, to working from home on their personal devices, untrusted user input into application and even sharing passwords. It can then somehow be made vulnerable to information theft and data leakage within organizations. So, user input handling controls basically prevent the effects of mistakes made by nontechnical users through a secure work culture. As a result of this control in desired proposed system, input sanitization method can be used.

13.6.4 Handling Communication and Data Transfer Controls

The employees within an organization can communicate safely to each other according to access control security features. These features control how users and system communicate and interact with other systems and resources.

13.6.5 How to Handle Employees' Daily Operations Controls?

The employees in organization have specific individual role and responsibilities to perform business operations and duties. Before using the proposed security framework, unique passwords for different logins are identified by system administrator. To check improper activity, employee's usage record will traced by auditing method. When transferring sensitive data of organizations, the need to know the level of employees will determine the access of these types of data. While an employee requests the data, process, or device of organization, respective security controls examine whether to accept or not deny each request.

13.7 What Is Multilevel Organization?

The classification of organizations is defined according to a hierarchy of authority and different responsibilities of individual employee. The three management levels most organizations have are first-level, middle-level, and top-level employees. The management style is influenced by the goals and purpose of the organization.

The term multilevel stands from the security classification of the defense community with confidential, secret, and top secret clearance levels. Individual users must be approved with accurate clearance levels before they can access the set of classified information. The confidential clearance users are only authorized to view confidential documents; they are not reliable to look at secret or top secret information. The multilevel organizations include many user classification levels and set of categories of business's digital resources [6]. A multilevel system is a single computer system that handles various classification levels between subjects and objects. In this system, access rights are associated with user, and roles are granted to appropriate user.

13.8 Secure Framework for Multilevel Organizations

13.8.1 Secure Framework for Multilevel Organizations (SFMO)

Secure framework for multilevel organizations (SFMO) is a security framework that involves the integration of security mechanisms such as user identification, account authentication, user authorization, access permission, user classification and access privacy, data classification in organization, and protection of most sensitive data. The goal of SFMO is to defend the vulnerability of insider and external threats, to protect from stealing company's business legal resources, and to secure any different structure of user levels and system resources in an organization. The following figure is the pattern of SFMO which makes a secure and safe environment for multilevel organization (Fig. 13.4).

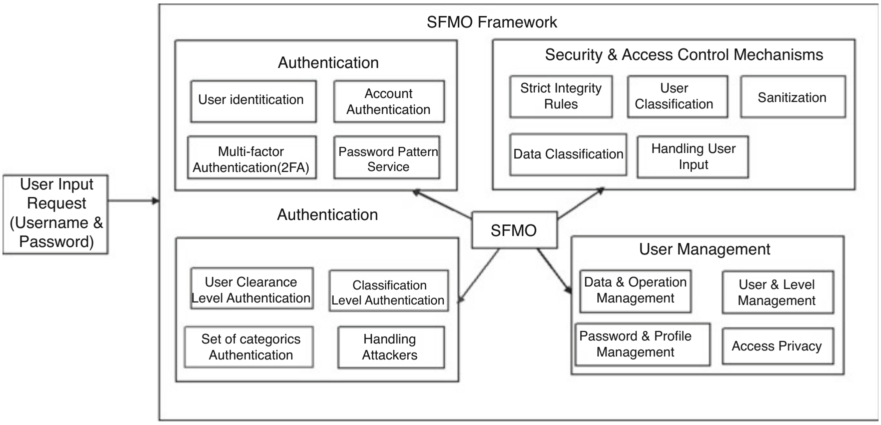


Fig. 13.4 Components of secure framework for multilevel organization

13.8.2 Features of Secure Framework for Multilevel Organizations (FSFMO)

Organizations with many staff management levels are generally called multilevel organizations which include groups of employees with different authority levels, many operations or functions, and relevant companies' data. These complex natured organizations must have an effective security countermeasure to keep their business safe from cyber threats. So, a secure framework will develop with the deployment of a set of security controls which obey the computer security aspects. The proposed secure framework for multilevel organizations will support the following features:

User Identification
It ensures a valid identity for an individual in the organizations with username and user level, for example, the system administrator login with username "admin" and user-level "administrator."

The rules of the authorized user and anonymous user are as follows:

```
IF username_identity is exist AND userlevel_ identity is exist
      THEN GRANT
      "User Identification" request is valid.
ELSE IF username_identity does not exist AND userlevel_identity
is unknow level
        THEN GRANT
      "User Identification" request is invalid and return invalid
      message.
END IF
END IF
```

Account Authentication with Two-Factor Authentication
This component of feature checks the identity of an individual user with password or PIN after user identification process is valid. The rules of the account authentication are as follows:

```
IF username is valid AND userlevel is exist AND password is
correct
      THEN
      "Authentication" is successful and the user is authenticated.
 END IF
ELSE
      THEN
      "Authentication" fail.
END IF
END IF
```

The single-step logins will compromise an attacker to get the usernames of other users, password prediction, and exploiting defects by bypassing the login functions. Therefore, the proposed framework uses two-factor authentication (2FA) to secure the system. The 2FA, two-step verification, is an extra security control that is also known as "multifactor authentication" (MFA). This control can be used as a combination of something the users have and something the users know.

User Authorization

This feature controls the access to system resources for authorized and unauthorized users. The user is authenticated and gets fully access right according to the user level in system. For example, the guest can view the profile of the university, while the authorized student user can view and search the respective information of that university.

The rules of the authorization are as follows:

```
IF userlevel is Level 1 AND classification level is Top secret
      THEN GRANT
     Give "Level 1 User" access right and can request to access
     "Top Secret object".
END IF
```

Integrity and Access Control

This type of feature applied Biba Model's Strict Integrity Policy. The policy provides subjects and objects with the integrity levels. L = (C, S) will represent as integrity level. In this equation, integrity level is defined as capital letter (L), the classification label is defined as capital letter (C), and set of categories label is defined as the capita letter (S). No write up and no read down are the main function of Strict Integrity Policy.

```
Algorithm 8.1
Integrity and Access Control Algorithm
INPUT: subject $L_n$= ($C_n$, $S_n$), object $L_{n+1}$= ($C_{n+1}$, $S_{n+1}$),
OUTPUT: if ($S_{n+1} \not\subset S_n$) REJECT, otherwise
METHOD:
      1. Initialize $C_n$,$C_{n+1}$
      2. $C_n$ and $C_{n+1}$ are assigned with values.
      3. If $S_n \supseteq S_{n+1}$:
             If $C_n$ = =$C_{n+1}$: Ln WRITE Access to $L_{n+1}$
               End if
               Else If $C_n > C_{n+1}$: Ln WRITE Access to $L_{n+1}$
               End if
              Else If $C_n < C_{n+1}$: REJECT WRITE Access to $L_{n+1}$
               End if
             Else If $C_n > C_{n+1}$: Ln REJECT READ Access to $L_{n+1}$
               End if
         End if
      4. return access request type
```

The subject L_1's integrity level = (C_1, S_1), and the object L_2's integrity level = (C_2, S_2). If the classification level C_1 (top secret), C_2 (secret), and S_2 is a subset of S_1, the subject level dominates the object level. According to the Biba's Strict Integrity. Policy, subject writes the object because L_1's integrity level is higher than integrity level of L2.

User Classification and Access Privacy

This feature can define the access rights and responsibilities for each user level and individual user. Access control rule defines the clearance (need to know) level for the user in the system. It provides the user profile management, privacy control for personal information confidentiality, password management, self-service, etc.

The rules of the user privacy and access right are as follows:

```
IF userlevel is Level 1 AND classification level is Top secret
AND set of categories "Group 1"
       THEN GRANT
      Give "Level 1 User" access right.
      Can request to write "Secret object".
      Can connect to everyone in "Group 1"
END IF
```

Data Classification
It classifies all data and resources of the organizations with integrity access control policy. It can provide labeling with classification level and set of categories for system data and resources.

The rules of the data classification are as follows:

```
IF object level is obj 1 AND classification level is Top secret
       THEN GRANT
      Can access to writ with same level subject (user)
END IF
```

Sensitive Data Protection
The feature contains the logic to protect data leakage of very sensitive data and digital asset from company' internal to the outside of organization by data encryption method.

13.8.3 Design of Proposed System

The proposed system aims to ensure that a secure framework of multilevel organizations. There are many levels of user (subjects) and different categories of objects (data) in the system. As the aspect of authenticity, this system identified the users by the predefined username and password before they enter the system. Users must enter username and password to check the validity of member in the system. So, the data availability is depending on the authentication checking. The system authorized users if their login name, password, and user level is correct. The user performs the operations of system resources according to their clearance level that had given by system administrator. Moreover, the system administrator classifies the organization's business data and resources with types of category and important level of business.

At the processing of the objects:

Integrity aspect:

- Higher-level subject can write to the lower level object.
- Same level subject can write to the same level object.
- Subject at lower level can't write to the object at higher level.
- Higher-level subject can't read to the lower level object.

As the system permits the access of each right user, the whole system can also retain the confidentiality on each object. And it can also comprise the protection of sensitive information of the organization in this framework (Fig. 13.5).

13.8.4 System Flow of Proposed System

The flow of this system is designed with only four user classification level as an example (Fig. 13.6).

13.8.5 Case Study for Multilevel Organizations

The following are three case studies for multilevel organizations and their user-level classifications.

1. *MCC Training Institute*

The first case study of multilevel organization is an education training center. There are three departments in that organization such as education services, finance department, and human resource department. In education services, it is divided into two teams: management and teaching.

The management includes CEO, COO, GM, dean manager, and AGM. At the teaching team, there are professors, lecturer, assistant lecturer, and class tutor, respectively.

So the following can show the user classification level of teaching team in MCC Training Institute. The highest user level is professor, and the lowest user level is class tutor. Each user level can have individual user right and responsibility. And the data and resources (object categories) had assigned to them by system administrator (Fig. 13.7).

2. *Mahar Myaing Trading Co. Ltd*

The second case study is a trading company organization. This organization generally includes CEO, manager, assistant manager, accountant, and office staff. CEO is the highest user level in that organization. So he or she can fully access almost system resources and files. The lowest user level, office staff, can request to access with the same or lower level of objects in the organization (Fig. 13.8).

3. *Galaxy Software Company*

The third one is a case study of a software company. In software company, it may have different departments such as development, testing, maintenance, customer service, and sales and marketing if this company is a big software company. However, there are few numbers of the company with many departments. Especially, only one team performs different duties at the same time in small office. So the

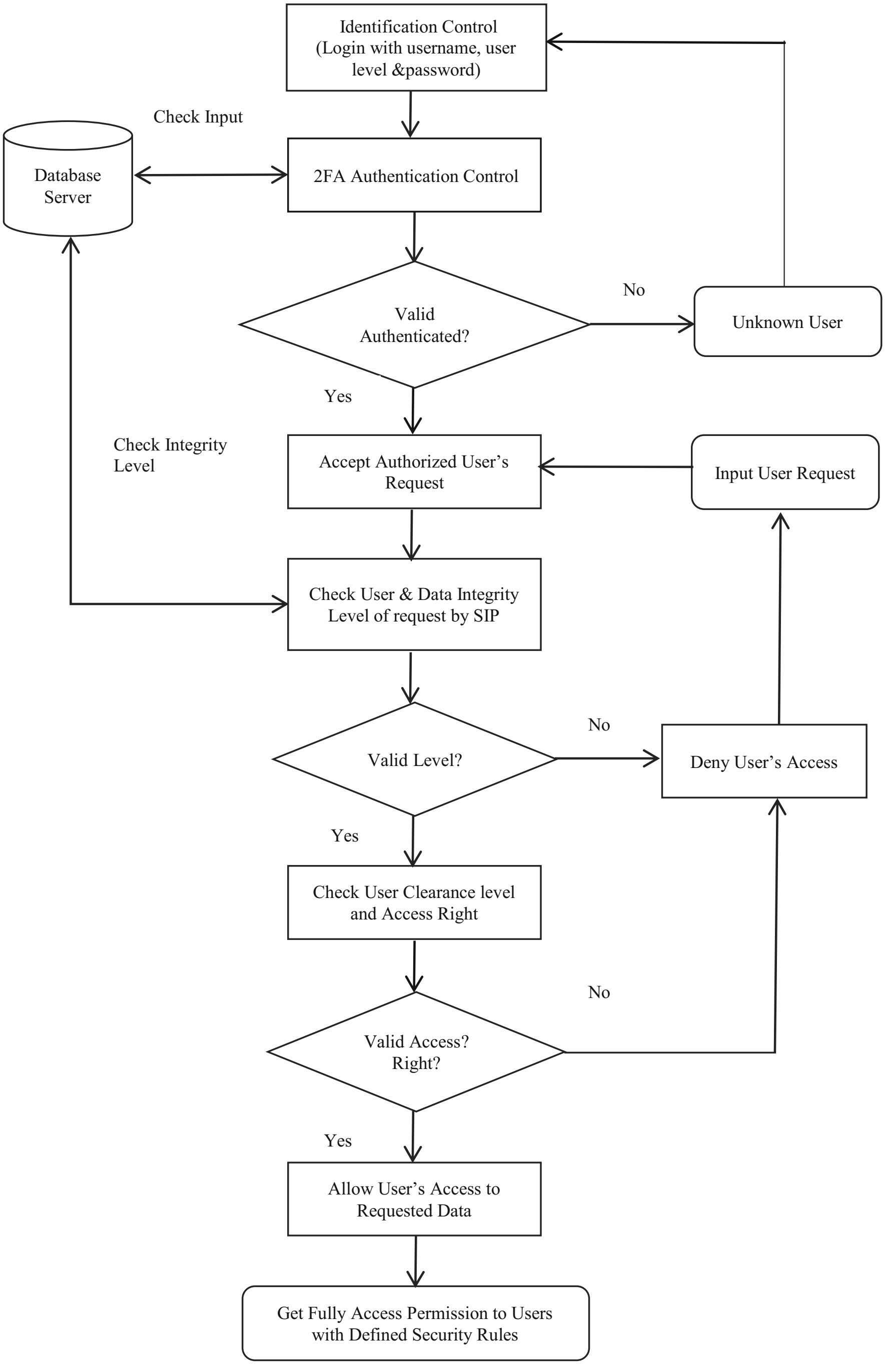

Identification Control (Login with username, user level &password)
Check Input
Database Server
2FA Authentication Control
Valid Authenticated?
No
Unknown User
Yes
Check Integrity Level
Accept Authorized User's Request
Input User Request
Check User & Data Integrity Level of request by SIP
Valid Level?
No
Deny User's Access
Yes
Check User Clearance level and Access Right
No
Valid Access? Right?
Yes
Allow User's Access to Requested Data
Get Fully Access Permission to Users with Defined Security Rules

Fig. 13.5 Design of the proposed system when user requests access to data

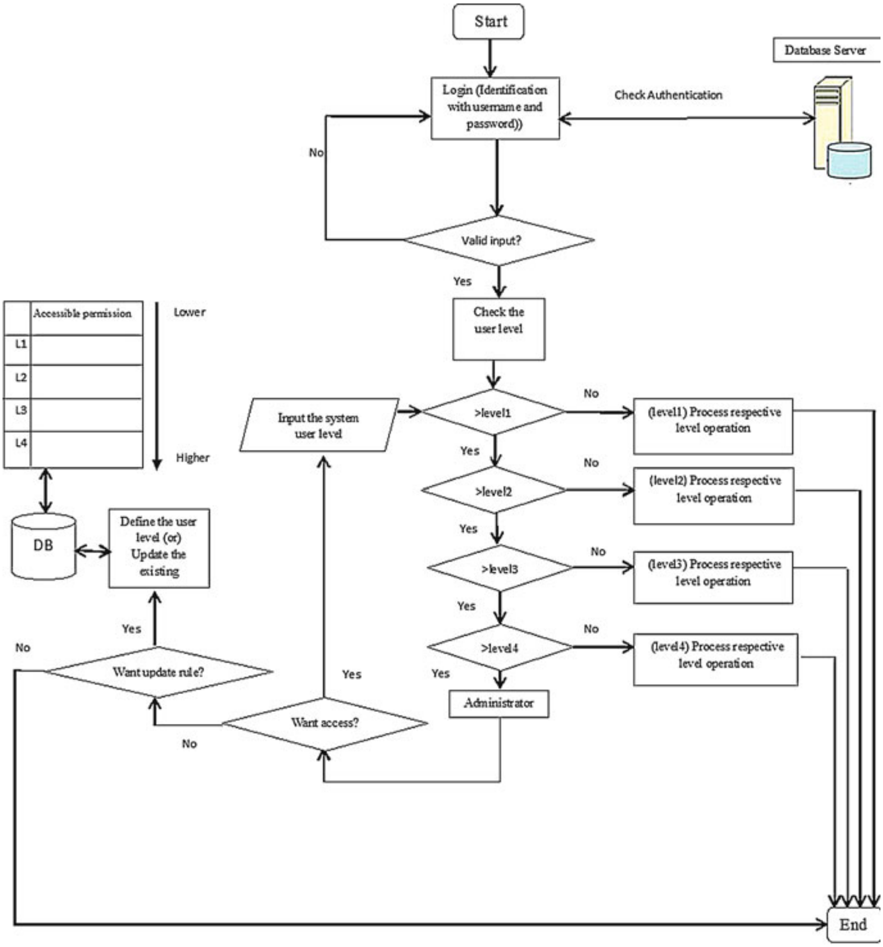

Start
Database Server
Login (Identification with username and password))
Check Authentication
No
Valid input?
Yes
Check the user level
Accessible permission
L1
L2
L3
L4
Lower
Higher
Input the system user level
>level1
No
(level1) Process respective level operation
Yes
>level2
No
(level2) Process respective level operation
Yes
>level3
No
(level3) Process respective level operation
Yes
>level4
No
(level4) Process respective level operation
Yes
Administrator
DB
Define the user level (or) Update the existing
Yes
No
Want update rule?
Yes
Want access?
No
End

Fig. 13.6 System flow of the proposed system with four user level

company is generally divided into five user level with project manager, programmer, developer, system analyst, software designer, and tester (Fig. 13.9).

The labels of classification and set of categories for subject (user) and object (resource, information, and file) are specified by system administrator (SA). One or more system administrator will control the system. The needs and nature of the organization change user-level classification and data categories.

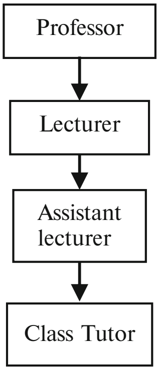


Fig. 13.7 User classification level of MCC case study

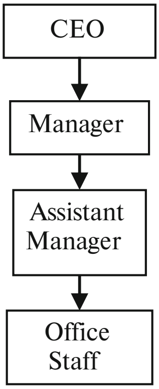


Fig. 13.8 User classification level of trading company case study

13.9 Privacy Policies at Workplace

The proposed secure framework imposes the multilevel organizations to be more secure and trusted. The data in the organizations categorize into the sets by defining labels, and the users define classification level. The system administrator can manage internal operations for individual users and data. The highest-level user in the system knows everything and can access any resources. But every user needs to protect user privacy that they wish to keep and their personality information that may be confidential. So the organization must identify basic rules for privacy policies for users.

The following are basic rules for privacy policies to define in organization by system administrator:

1. It intimates users about what you collect and why and what you will do with it.
2. It should limit the collection of information and collect it by fair and lawful means.
3. Inform users about the potential collection, use, and disclosure of personal information.

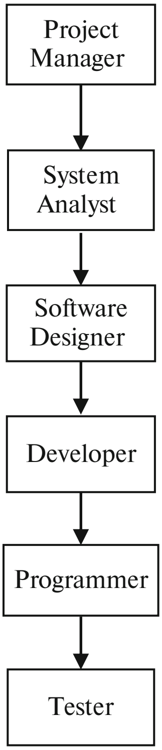


Fig. 13.9 User classification level of software company case study

4. Keep user's personal information accurate, complete, and up-to-date.
5. Provide users access to their personal information.
6. It must keep user's personal information secure [7].

13.10 Conclusion

The intellectual property and assets of an organization or a company are mostly stored as digital format in database. Database security is an essential part in the information security management of nowadays digital system. The employees in every organizations can become the biggest threat because they often are not mindful on the possible risky mistakes whether they are doing or not in the database of that organization. In this case, the most effective cybercrime are facilitated by employees' accidental or careless actions. So, the organizations need to address the problems and solutions of this risk. The protection of database is to restrict unauthorized employee to access a company's confidential data and digital property.

The proposed secure framework implements the collaboration of access control, integrity, and possible security control mechanisms to ensure that defend malicious threads, end user's faults and intentional attacks of information stealers. This proposed framework ensures that the organizations get a security-driven work culture and acts like a defensive wall of the organization's information security system.

References

1. Z. Aung, Database server security for banking information system. M.C.SC Dissertation. University of Computer Studies, Yangon, 2010
2. M.K. Moe, Implementation of mandatory access control using staff levels. M.C.Sc Dissertation. University of Computer Studies, Yangon, 2016
3. S. Zune, Mandatory access control by Biba model. M.C.Sc Dissertation. University of Computer Studies, Yangon, 2018
4. N. Balon, I. Thabet, Biba Security Model. CIS 576. (2004, March 17)
5. D. Stuttard, M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd edn
6. Red Hat®, Multi-level Security (MIS), https://www.centos.org/docs/5/html/Deployment_Guide-en-US.html. Accessed 1 May 2019
7. Council, EC, *Certified Ethical Hacker Note*