SECURE EDUCATIONAL DATA MANAGEMENT USING LATTICE-BASED ACCESS CONTROL

Yie Yie Nwe

M.C.Sc. **September 2022**

SECURE EDUCATIONAL DATA MANAGEMENT USING LATTICE-BASED ACCESS CONTROL

By

Yie Yie Nwe

B.C.Sc.(Hons:)

A Dissertation Submitted in Partial Fulfilment of the Requirements for the Degree of

Master of Computer Science

(M.C.Sc.)

University of Computer Studies, Yangon

September 2022

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere thanks to those who helped me with various aspects of conducting research and writing this thesis. To complete this thesis, many things are needed like my hard work as well as the supporting of many people.

First and foremost, I would like to express my deepest gratitude and my thanks to **Dr. Mie Mie Khin**, Rector, University of Computer Studies, Yangon, for her kind permission to submit this thesis.

I would like to express my appreciation to **Dr. Si Si Mar Win**, **Professor, and Dr.Tin Zar Thaw, Professor,** Course Coordinators (M.C.Sc.(Thesis)/ M.I.Sc.(Thesis)), Faculty of Computer Science of the University of Computer Studies, Yangon, for their superior suggestion, administrative supports and encouragement during my academic study.

My thanks and regards go to my supervisor, **Dr. Nilar Aye, Professor,** Faculty of Information Science**,** University of Computer Studies, Yangon, for her support, guidance, supervision, patience and encouragement during the period of study towards completion of this thesis.

I also wish to express my deepest gratitude to **Daw Win Lai Lai Bo**, **Assistant Lecturer,** English Department, University of Computer Studies, Yangon, for her editing this thesis from the language point of view.

Moreover, I would like to extend my thanks to all my teachers who taught me throughout the master's degree course and my friends for their cooperation.

I especially thank to my parents, all of my colleagues, and friends for their encouragement and help during my thesis.

ABSTRACT

Database security is the system, processes, and procedures that protect a database from unintended activity. The protection of data storage is a challenging and formidable task and so the user data should be protected against security threats. In this system, the user's data are protected along with the association of lattice-based security technique. The proposed system is developed for secure data access control in Education Degree College (EDC). This system is intended to provide right access control based on user's roles that are assigned according to the enterprise's policy decision by using Lattice-Based Access Control Model on data and marks of EDC's students. In the proposed system, administrator can access all data and can make all transaction of the whole system and the data occupation of the respective level. The users of the proposed system are Admin User (level-1), Department Head (level-2), Senior Teacher (level-3), Teaching Staff (level-4) and Student Affair (level-5). These levels are defined by system administrator or board of the organization depend on the lattice-rules The assigned categories of the admin on the object access are (1) essential data submission, (2) Data Management (Limited By System Rules), and (3) user management .

This system is implemented using C# programming language with Microsoft SQL server database engine.

Key Word: EDC, Lattice-Based Access Control, database security

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

TABLE **PAGE**

CHAPTER 1

INTRODUCTION

Because of the fast improvement of Computer and Internet innovation, an ever-increasing number of resources of an organization or an association are put away in advanced design in data sets. Data sets are likewise generally utilized in each individual's regular routine of each and every association. These associations are danger to open the data sets frameworks, the procedures to be thought about while getting a data set, and how to get a data set in various trustworthiness levels of significant layers. The proposed framework will control the safe information access on understudies' instructive information of Education Degree College. This framework will be created as a safe information access control framework utilizing Lattice-Based Access Control in Education Degree College. Cross section-based admittance control gives authorization and forestalls approval assault. Cross section-based admittance control is additionally offering access control and used to safeguard unapproved revelation, change, guarantee accessibility. These kinds have been characterized by the information arrangement structure.

In this framework, in view of the jobs of the association, an entrance control strategy is ready in which various privileges are relegated to the clients of the association. The fundamental errand of this framework is making a limited admittance as far as access control strategy. Grid model is built and access control strategy has been characterized in light of the cross section to give limited admittance for the information.

This system is developed as a secure data access control system using Lattice-Based Access Control in Education Degree College (EDC). Lattice-Based access control gives approval and forestalls approval assault. Cross section-based admittance control is likewise offering access control and used to protect unapproved revelation, modification, guarantee accessibility. These sorts of exercises have been characterized by the information grouping system. In this framework, in view of the

jobs of the association, an entrance control strategy is ready in which various privileges are allotted to the clients of the association. The main task of Lattice-Based access control is creating a restricted access control policy to control the respective access grant on each user level.

1.1 Objectives of the Thesis

The main objectives of this thesis are:

- To provide right access control based on user's roles that are assigned according to the enterprise's policy decision
- To maintain the data availability by only authorized user that need-to-know
- To improve the two aspects of system management such as convenience and flexibility
- To study the method of security access controls

1.2 Motivations

When security is compromised at the opposite end that it turns into a test to guarantee secrecy and honesty of the user's information on EDC system. Consequently, to defeat the security issues, information should be done the authorization process prior to putting away it. In this framework, an adaptable and viable information security conspire is proposed to safeguard client information in view of access control strategy (Lattice Based).

1.3 Related Works

Teacher Steve Demurjian Fall Jin Ma portrayed Mandatory Access Control in Patient DB utilizing CORBA, Application predefines the security arrangement (T, S, C, U) for asset, administration and strategy. The security access control levels are arranged by ascending order (from lower to upper) with respect to their access granted. Security

refers to the protection of data against unauthorized disclosure, alteration, or destruction [12].

Steven A. Demurjian, University of Connecticut, Storrs, USA stated that: “Multi-Level Security in Healthcare Using a Lattice-Based Access Control Model”, International Journal of Privacy and Health Information Management in 2019. This article proposes the use of multi-level security defined by lattice-based sensitivity profiles to ensure compliance with data access restrictions between systems. This security approach accommodates the complexities needed for health data access and benefits from existing proven tools that are used for defense and national security applications [10].

“A Lattice-Based Approach for Updating Access Control Policies in Real-Time [1]”, Access control policies which are stored as policy objects control the person who can access the data objects. An environment where multiple types of transactions are carried out simultaneously. There may be transactions updating policy objects in some of these. While policy objects are being used by updating them that can cause security issues. Algorithms that not only guarantee serializable transaction execution but also prevent such security issues were presented. The levels of concurrency and types of policies that each algorithm can differ in update.

1.4 Organization of the Thesis

The thesis is organized in five chapters. They are as follows:

In Chapter 1, introduction of the system, objectives of the thesis, motivation, related works and thesis organization are described.

In Chapter 2 discusses the theoretical background.

In Chapter 3 presents the overview of the data security control method, typical problems between the executions of the difference user level, types of access.

In Chapter 4 expresses the design and implementation of the proposed system.

Finally, Chapter 5 presents the conclusions of this thesis and showing advantages in system restricts the write access by attributes. Thus, only the user who has full write access can insert new records. Moreover, each user is assigned to only one role. It does not allow multiple rows assignment for the user. For sensitive data, security is more important. The data can be made to secure by using various methodologies. This system

user has only data facilities to control security. This system is only implemented to control unauthorized access to data in the process to safeguard sensitive data, another facility – data encryption by using Cryptographic technique – is suggested as future work of this thesis. This system can also be extended hybrid structure of cryptography and access control techniques.

CHAPTER 2

BACKGROUND THEORY

Security alludes to exercises and measures to guarantee privately, respectability, and accessibility of a data framework and its primary resource information. In an organization of PC framework, security of framework assets is significant for performing data board. In some business framework, there are different staff levels as their jobs. Thus, there are different data levels as indicated by the staff levels. In the event such a business utilizes an electronic data framework, there is a need of safety control to deal with data level for multi-client levels. Macintosh is a mean of confining admittance to objects. A staggered framework handles different characterization levels among subjects and items. Staggered data set framework is endeavoring to foster data set framework that shields group data from unapproved clients in view of the order of the information and clearances of the clients.

2.1 Data Protection Systems

This entrance grid model presents an issue for secure frameworks: un-believed cycles can mess with the insurance framework. Utilizing insurance state activities, un-believed client cycles can alter the entrance network by adding new subjects, items, or tasks doled out to cells.

	File 1	File 2	File3	File 4	Process 2
Process 1	Read	Read, Write	Read, Write	Read	-
Process 2	-	Read	Read, Write	-	Read

Figure 2.1 Access Matrix

Suppose Process 1 has responsibility for 1. It can then concede some other interaction read or compose (or possibly even proprietorship) access over File 1. An insurance framework that grants un-confided in cycles to change the security state is known as a *discretionary access control* (DAC) system. This is on the grounds that the

assurance state is at the watchfulness of the clients and any un-confided in processes that they might execute.

The issue of guaranteeing that specific assurance state and all conceivable future insurance states that are logical won't give an unapproved access which is known as the wellbeing issue. It was observed that this issue is un-decidable for insurance frameworks with compound security state tasks, for example, for making record above which the two adds a document segment and adds the tasks to the proprietor's cell. Thus, it is preposterous as a general rule to confirm that an insurance state in such a framework will be secure (i.e., fulfill security objectives) later on. To a safe working framework fashioner, such an insurance framework cannot be utilized in light of the fact that it isn't carefully designed; an un-believed cycle can change the assurance state and consequently the security objectives implemented by the framework.

The assurance framework characterized expects to implement the necessity of security: one cycle is safeguarded from the tasks of another provided that the two cycles act kindly. On the off chance that no client cycle is malevolent with some level of unquestionably, the assurance state in any case will portray the genuine security objectives of the framework which even after a few tasks have changed the security state. Assume that a File 1 in Figure 2.1 stores a mystery esteem like a confidential key in a public key pair, and File 2 stores a high uprightness esteem like the relating public key. On the off chance that Process 1 is non-pernicious, it is far-fetched that it will release the confidential key to Process 2 through either File 1 or File 2 or by changing the Process 2's consents to File 1. However, assuming Process 1 is noxious almost certainly, the confidential key will be spilled. The mystery of File 1 is implemented to guarantee, all cycles that approach document should not have the option to release the record through the authorizations accessible to that interaction including by means of assurance state activities.

Likewise, the entrance grid insurance framework doesn't guarantee the trustworthiness of the public key document "Record 2" by the same token. By and large, an assailant should not have the option to adjust any client's public key since this could empower the aggressor to supplant this public key with one whose private key is known to the aggressor. Then, at that point, the aggressor could take on the appearance of the

client to other people. Hence, the uprightness split the difference of File 2 likewise security consequences. Obviously, the entrance network insurance framework cannot shield File 2 from a pernicious Process 1, as it has composed admittance to File 2. Further, a malignant Process 2 could improve this assault by empowering the aggressor to offer a specific benefit for the public key. Likewise, regardless of whether Process 1 isn't noxious, a malignant Process 2 might have the option to fool Process 1 into changing File 2 in a pernicious manner relying upon the connection point and potential weaknesses in Process 1. Support flood weaknesses are utilized thus a malevolent cycle (e.g., Process 2) to assume control over a weak cycle (e.g., Process 1) utilize its consents in an unapproved way.

Sadly, the assurance approach is fundamental the entrance lattice security state that is credulous in this day and age of malware and availability to pervasive organization assailants. The present registering frameworks depend on this security approach so they can't be guaranteed authorization of mystery and respectability prerequisites. Insurance frameworks that can implement mystery and respectability objectives should uphold the prerequisite of safety: a framework's security instruments can implement framework security objectives in any event when any of the product outside the believed processing base might be pernicious. In such a framework, the security state should be characterized in view of the exact recognizable proof of the mystery and uprightness of client information and cycles and no un-believed cycles might be permitted to perform assurance state tasks. Consequently, the reliance on possibly malignant programming is taken out and a substantial reason for the implementation of mystery and honesty prerequisites are conceivable. This rouses the meaning of an obligatory security framework underneath.

2.2 Mandatory Protection System

A *mandatory protection system* is a security framework that must be changed by confided in chairmen through confided in programming, comprising of the accompanying state portrayals:

- **A *mandatory protection state*** is a security state where subjects and items are addressed by marks where the state depicts the tasks that subject names might take upon object names.
- **A *labeling state*** arranges cycles and framework asset objects to marks.
- **A *transition state*** depicts the lawful ways that cycles and framework asset articles might be relabeled.

For secure working frameworks [4], the subjects and items in an entrance grid are addressed by framework characterized marks. A name is essentially a theoretical identifier — the task of consents to a mark characterizes its security semantics. Marks are carefully designed on the grounds that: (1) the arrangement of names is characterized by believed executives utilizing confided in programming and (2) the arrangement of marks is unchanging. Believed chairmen characterize the entrance framework's names and set the tasks that subjects of specific marks can perform on objects of specific names. Such insurance frameworks are obligatory access control (MAC) frameworks in light of the fact that the security framework is permanent to un-confided in processes 2. Since the arrangement of marks cannot be changed by the execution of client processes, we can demonstrate the security objectives upheld by the entrance grid and depend on these objectives being implemented all through the framework's execution.

Obviously, on the grounds that the arrangement of names is fixed doesn't imply that the arrangement of cycles and records are fixed. Secure working frameworks should have the option to join names to powerfully made subjects and articles and, surprisingly, empower mark advances.

A naming state doles out marks to new subjects and items. Figure 2.2 shows that cycles and documents are related with marks in a proper security state. At the point when new record is made, it should be doled out one of the article names in the security state. In Figure 2.2, it is allotted the mystery mark. Similarly, the cycle new interaction is likewise marked as unclassified. Since the entrance network doesn't allow unclassified subjects with admittance to secret items, new interaction cannot get to new record. Concerning the security state in a protected working framework, the marking state should be characterized by confided in chairmen and changeless during framework execution.

A progress state empowers a protected working framework to change the name of an interaction or a framework asset. For an interaction, a mark progress changes the consents accessible to the cycle (i.e., its insurance space), so such advances are called security space changes for processes. As an illustration where a security space change might be essential, look at when as a cycle executes an alternate program. At the point when an interaction plays out a framework call the cycle picture (i.e., code and information) of the program is supplanted with that of the document being executed. Since an alternate program is run because of the framework call, the name related with that cycle might should be changed too to show the essential consents or confidence in the new picture.

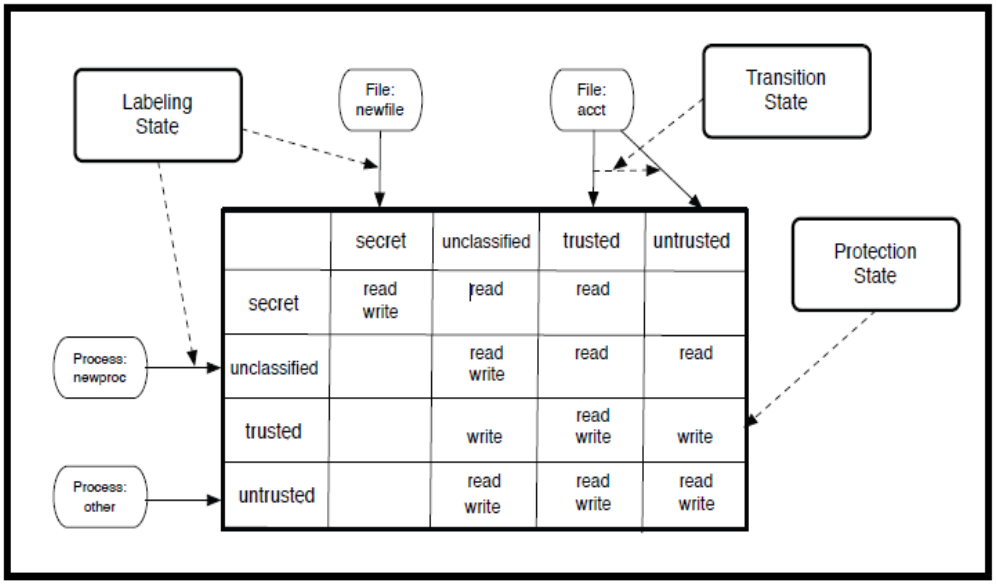


Figure 2.2 A Mandatory Protection System

A progress state may likewise change the name of a framework asset. A name progress for a document (i.e., item or asset) changes the openness of the record to security spaces. For instance, consider the document acct that is named confided in Figure 2.2 [The assurance state is characterized with regards to marks and is unchanging. The permanent naming state and change state empower the definition and the executives of marks for framework subjects and objects]. In the event that this document is changed by a cycle with an un-believed name, for example, other, a progress state might change

its mark to un-trusted too. An option is changing the security state to restrict un-confided in processes from altering believed documents, which is the situation for different approaches. Concerning the security state and marking state, in a safe working framework, the progress state should be characterized by confided in managers and unchanging during framework execution.

2.3 Reference Monitor

A ***reference monitor*** is the old-style access authorization component. Figure 2.3 presents a summed-up perspective on a reference screen. It takes a solicitation as info, and returns a paired reaction demonstrating whether the solicitation is approved by the reference screen's entrance control strategy. In distinguish three particular parts of a reference screen:

- its interface;
- its approval module; and
- its strategy store.

The point of interaction characterizes where the approval module should be summoned to play out an approval inquiry to the security express, a marking question to the naming state, or a change inquiry to the progress state. The approval module decides the specific inquiries that are to be made to the arrangement store. The arrangement store answers approval, naming, and progress inquiries in view of the security framework that it keeps up with.

Reference Monitor Interface: The reference screen interface characterizes where security framework questions are made to the reference screen. Specifically, it guarantees that all security-delicate tasks are approved by the entrance requirement instrument. By a security-delicate activity, we mean a procedure on a specific item (e.g., record, attachment, and so forth) whose execution might disregard the framework's security necessities. For instance, a working framework executes document access activities that would permit one client to peruse another's privileged information (e.g., confidential key) in the event that not constrained by the working framework. Marking and advances might be executed for approved activities.

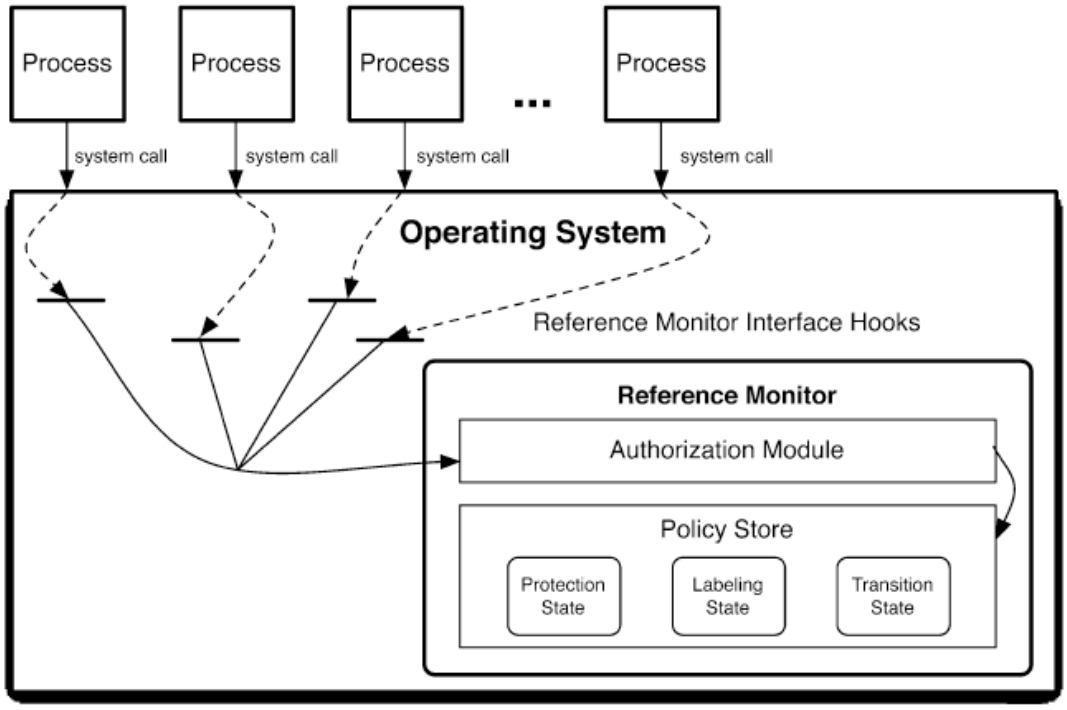


Figure 2.3 A reference monitor

The reference screen interface figures out where access implementation is fundamental and the data that the reference screen requirements to approve that solicitation. The reference screen interface should figure out what to approve where to perform such approvals, and what data to pass to the reference screen to approve the open. Mistaken interface configuration might permit an unapproved interaction to get close enough to a record.

Authorization Module: The center of the reference screen is its approval module. The approval module takes connection point's bits of feedbacks (e.g., process personality, object references, and framework call name), and converts these to a question for the reference screen's strategy store. The test for the approval module is to plan the cycle character to a subject mark, the item references to an item name, and decide the genuine tasks to approve (e.g., there might be various tasks per interface). The security framework decides the selections of names and tasks, yet the approval module should foster a method for playing out the planning to execute the "right" question.

For the open solicitation over, the module answers the singular approval demands from the connection point independently. For instance, when a catalog in the record way

is mentioned, the approval module fabricates an approval question. The module should get the mark of the subject liable for the solicitation (i.e., mentioning process), the name of the predetermined registry object (i.e., the index anode), and the insurance state activities suggested the solicitation (e.g., read or search the catalog). At times, on the off chance that the solicitation is approved by the strategy store, the module might make resulting solicitations to the approach store for naming (i.e., in the event that another item was made) or mark changes.

2.4 Policy Store

The strategy store is a data set for the insurance state, marking state, and change state. An approval inquiry from the approval module is replied by the strategy store. These inquiries are of the structure {subject name, object mark, activity set} and return a parallel approval answer. Marking questions are of the structure {subject name, resource} where the mix of the subject and, alternatively, some framework asset credits deciding the resultant asset mark returned by the inquiry. For changes, questions incorporate the {subject name, object mark, activity, resource}, where the approach store decides the resultant mark of the asset. The asset might be either a functioning element (e.g., an interaction) or a detached item (e.g., a document). A few frameworks execute inquiries to approve changes too.

2.5 Secure Operation System Definition

Characterize a solid working framework as a framework with a reference screen access implementation instrument that fulfills the necessities underneath when it upholds a compulsory insurance framework. The reference monitor concept defines the necessary and sufficient properties of any system that securely enforces a mandatory protection system. A secure operating system is one whose access enforcement satisfies these three guarantees:

1. **Final Mediation**: All operations that are sensitive to security are mediated by the system's access enforcement mechanism.

Complete Mediation Complete mediation of safety delicate tasks expects that all program ways that lead to a security-touchy activity be intervened by the reference screen

interface. The insignificant methodology is to intervene all framework calls, as these are the passage focuses from client level cycles. While this would without a doubt intervene all tasks, it is frequently inadequate. For instance, some framework calls carry out different particular activities. The open framework call includes the opening a bunch of catalog objects, and maybe record joins, prior to arriving at the objective document. The subject might have different consent for every one of these items, so a few, different approval inquiries would be vital. Additionally, the registry, connection, and record objects are not accessible at the framework call interface, so the point of interaction would need to register them, which would bring about repetitive handling (i.e., since the working framework as of now maps document names to such articles). Be that as it may, to top it all off, the planning between the document name passed into an open framework call and the catalog, connection, and record articles might be changed between the beginning of the framework call and the genuine open activity (i.e., by a very much coordinated rename activity). This is known as a period of-check-to-season of-purpose (TOCTTOU) assault, and is innate to the open framework call.

2. **Tamperproof:** The framework guarantees that its entrance implementation component, including its security framework, can't be changed by un-confided in processes.

Tamperproof: Confirming that a reference screen is carefully designed requires checking that all the reference screen parts, the reference screen interface, approval module, and strategy store, can't be changed by processes outside the framework's confided in figuring base (TCB). This likewise infers that the TCB itself is high honesty, so we eventually should check that the whole TCB can't be altered by processes outside the TCB.

3. Verifiable: The entrance authorization instrument, including its security framework, "should be adequately little to be dependent upon investigation and tests, the fulfillment of which can be guaranteed". That is, we should have the option to demonstrate that the framework upholds its security objectives accurately.

Verifiable: At long last, we should have the option to check that a reference screen and its strategy truly uphold the framework security objectives. This requires confirming the accuracy of the connection point, module, and strategy store programming, and assessing

whether the compulsory assurance framework genuinely implements the planned objectives.

The reference screen idea characterizes the important and adequate prerequisites for access control in a safe working framework. Initial, a solid working framework should give total intercession of all security-touchy tasks. In the event that this multitude of tasks are not interceded, then a security prerequisite may not be upheld (i.e., a mystery might be spilled or believed information might be changed by an un-believed process). Second, the reference screen framework, which incorporates its execution and the assurance framework, should all be sealed. If not, an aggressor could change the authorization capability of the framework, again evading its security. At last, the reference screen framework, which incorporates its execution and the assurance framework, should be adequately little to check the right implementation of situation security objectives. If not, there might be blunders in the execution or the security approaches that might bring about weaknesses. A test for the originator of secure working framework is the manner by which to accomplish these prerequisites unequivocally.

2.6 Mandatory Access Control

Mandatory access control is defined as "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (e.g., clearance) of subjects to access information of such sensitivity" by the United States Department of Defense Trusted Computer System Evaluation Criteria.The security level at which a single client or user can access information is called clearance. Based on National Security Information, we will use the four exceptional status values that are listed below:

• High-Priority (T): shall apply to information whose unauthorized disclosure is likely to cause exceptionally serious harm to national security.

• The Secret (S)shall be applied to information whose unauthorized disclosure is likely to have a significant negative impact on national security.

• Protected (C): shall be applied to information whose unauthorized disclosure is likely to significantly compromise national security.

• Uncategorized (U): no restrictions on security

The security level that is assigned to data in light of strategy, we will use similar grouping levels utilized for clearances to relegate characterizations. Freedom and grouping go together, in that, a client's leeway is a breaking point to the entrance of data in view of the data's characterization.

Order connection is invalid < U < C < S < T. Every security level is said to overwhelm itself and all others beneath it in this progressive system.

The idea of required admittance control was first formalized by Bell and LaPadula Model [4, 7]. The Bell-LaPadula Model backings compulsory access control by deciding the entrance privileges from the security levels related with subjects and articles. The accompanying two principles characterize the required admittance:

- **Simple-security property** (*ss-property*): A subject can read an object only if the security level of the subject is higher or equals to the security of the object (*read-down*).
- ***. property:** A subject can write on an object only if the security level of the object is higher or equals to the security level of the subject. (*Write up*).

MAC strategy looks at the responsiveness mark at which the client is working to the awareness name of the item being gotten to and declines access except if certain MAC checks are passed. It is generally expected that the security marks on subjects and articles, once relegated, can't be changed (besides by the security chairman). This supposition that is known as quietness [6]. This is the explanation that MAC is compulsory. With obligatory controls, just heads and not proprietor of assets might settle on choices that bear on or get from strategy. Just an executive might change the class of an asset, and on one might concede a right of access that is expressly prohibited in the entrance control strategy. Macintosh requires every one of the individuals who make, access and keep up with data to adheres to guidelines set by head.

MAC strategy looks at the responsiveness level at which the client is working to the delicate mark of the item being gotten to and declines except if certain MAC checks are passed. Macintosh is required in light of the fact that the marking of data happens naturally, and normal clients can't change names except if a chairman approves them. Responsiveness names are allotted to documents, gadgets, windows, hosts, organizations, and to other framework protests that client access. Executive demonstrate the degree of

trust or occupation obligation of anybody getting to the framework by relegating a leeway that sets the upper bound of a bunch of responsiveness names at which the client can work. Executive likewise doles out a base responsiveness mark that sets the lower bound. Managers can design clients to work at a solitary name. With obligatory control, just managers and not proprietors of assets might settle on choices that bear on or get from strategy. Just a manager might change the classification of an asset, and nobody might give a right of access that is unequivocally taboo in the entrance control strategy MAC requires every one of the people who make, access, and keep up with data to observe guidelines set by directors.

The limitations put on document control (perusing, composing, making, erasing) are those that are by and large acknowledged while executing a MAC strategy:

- To read a file, the label of the process must dominate the label of the file.
- To write a file, the label of the process must be dominated by the label of the file.

An interaction can make a record to the level of the name Rule-based admittance controls: This kind of control further characterizes determines conditions for admittance to a mentioned object. All MAC based frameworks execute a straightforward type of rule-based admittance ought to be conceded or denied by coordinating with an item's responsiveness mark and a subject's awareness name.

Table2.1 List of the Bell-LaPadula Properties

Bell-LaPadula Properties		
Property	Common Name	Description
Simple security rule	No read up	A subject of a given security clearance cannot read data from a higher security level.
* -property (star property)	No write down	A subject of a given security clearance cannot write to an object at a lower security level.

2.7 Role-based Access Control

Role-based Access Control (RBAC) directs a client's admittance to specific assets in light of a client job. A client job is an assortment of consents the client needs to achieve that job. A client might play numerous parts, with every job having a bunch of consents.

The significant benefit of job-based framework is adaptability [1, 9]. Job based way to deal with assurance and the board of framework honor offers more adaptability than different frameworks like staggered security (the most well-known approach of MAC) and DAC, while demonstrating comparative degrees of security for objects in a framework. In job-based applications, a client's entrance privileges can be shifted through various means. For example, renouncing a client's approval to a job removes the honors in that job from the client. Fine-grained honor the board can be acknowledged by eliminating/adding honors related with a given job.

One more benefit of job-based framework connects with the granularity of framework honor the executives. Considering that framework honors can be essentially as fine-grained as one can pick, jobs offer a method for their gradual administration.

2.8 Combination of MAC and RBAC

Role-base access control facilitates the organization of honors because of the adaptability with what jobs can be arranged and reconfigured. With jobs, we can uphold the standard of least honor where a job is doled out just adequate usefulness to understand the expected obligation prerequisites [2].

Customary job-based security finds application in conditions where the more prominent concern is data trustworthiness rather than mystery [2]. However, this doesn't block the abuse of the upsides of job-based assurance to acknowledge mystery. With extra guidelines on update and read tasks, and the data they access, we can understand the prerequisites of compulsory access control, or MAC. It's out goal to show the way that a MAC-like degree of insurance can be acknowledged utilizing job-based security.

By the mix of MAC and RBAC, the framework can give secrecy limitation. In this proposed situation, the Role and Access Rights for clients, MAC grouping levels for

tables in Departments and MAC level got access to clients are characterized ahead of time. Furthermore, this framework limits the compose access by job. In this way, just the client who has full set up access can embed new accounts. Besides, every client is allocated to just a single job. It doesn't permit numerous jobs task for client. Besides, the overseer plans the job level and functional level of the framework. In any case, the director is additionally confined the perused/set up admittance to accounts of the other level client in the event that they don't give the authorization on their information. In this way, the blend of the MAC and RBAC give areas of strength for the on delicate information.

2.9 The System Authentication

Authentication is the demonstration of laying out or affirming something (or somebody) as credible, that will be that cases made by or about the subject are valid. This could include affirming the character of an individual, following the starting points of a relic, guaranteeing that an item is the thing it's bundling and name professes to be, or guaranteeing that a PC program is a confided in one. The framework will allow the framework clients if their login name and secret phrase is right. And afterward the framework client can get to the information by their level characterized by head. This is called approval.

2.10 The System Authorization

The ability to determine who has access to assets is known as authorization, and it is related to computer security and data security as a whole as well as control specifically. For instance, HR personnel frequently receive permission to access representative records, and in most PC frameworks, access control rules formalize this strategy. The structure uses the entrance control rules to decide whether (confirmed) customers' access requests will be granted or denied during activity. Individual records, or alternatively, information about things, computer programs, PC gadgets, and the utility provided by PC applications are examples of assets. Clients, software, and other PC-based devices are examples of buyers.

CHAPTER 3

LATTICE BASED ACCESS CONTROL

Access control policies shield data assets from unapproved access. Since security approaches are very basic for a venture, it is vital to control how strategies are refreshed. Refreshing strategy in an ad hoc way might bring about irregularities and issues with the arrangement determination; this, thusly, may make different issues, for example, security breaks, inaccessibility of assets, and so on. As such, arrangement updates ought not be through ad hoc activities however finished through obvious exchanges that have been recently examined.

In addition, such updates ought to be completed exclusively by security managers or other high-positioning staff. A significant issue that should be remembered about strategy update exchanges is that a few arrangements might demand continuous updates. the term continuous update of a strategy to imply that the strategy is changed while it is active and this change should be upheld right away. Such constant updates of access control strategies are required by unique conditions that are answering global emergency, like help or war endeavors. As a rule, in such situations, framework assets need reconfiguration or functional modes require change; this, thusly, requires strategy refreshes. The refreshed strategies ought to be consequently upheld.

A data set comprises of a bunch of items that are gotten to and changed through exchanges. Exchanges performing procedure on information base items should have the honor to execute those tasks. Such honors are determined by access control approaches; access control arrangements are put away as strategy objects. Exchanges executing by ideals of the honors given by a strategy object are said to convey the strategy object. As well as being sent, a strategy item can likewise be gotten to and changed by exchanges. A climate wherein various types of exchanges execute simultaneously some of which are strategy update exchanges. All in all, a strategy might be refreshed while exchanges are executing by righteousness of this strategy. Permitting the exchanges to execute in situations where the changed strategy no longer gives these exchanges the execution honors bring about a security break.

Security alludes to exercises and measures to guarantee the secretly, uprightness, and accessibility of a data framework and its primary resource, information. In an organization of PC framework, security of framework assets is significant for performing data the executives. In some business framework, there are different staff levels as per their jobs. Thus, there are different data levels as indicated by the staff levels. In the event that such a business utilizes a mechanized data framework, there is a need of safety control to deal with data level for multi-client levels.

3.1 Lattice-based access control

These can be utilized for complex access control choices including different articles or potentially subjects. A cross section model is a numerical design that characterizes most prominent lower-bound and upper headed values for a couple of components, like a subject and an item. a cross section-based approach is utilized to classify strategy update exchanges as strategy relaxations or strategy limitations. Strategy relaxations increment the entrance control honors of a subject. A strategy update that isn't an arrangement unwinding is treated as an arrangement limitation. Strategy unwinding, in contrast to limitation, doesn't need cut short of exchanges that are executing by prudence of the arrangement. The cross section-based approach permits one to grammatically decide whether the strategy update is an unwinding or limitation.

This cross-section calculation manages what is going on when numerous strategies are determined over a subject and an item and needs are indicated with arrangements. A strategy update might change the entrance privileges related with the arrangement or its need. A cross section-based approach is utilized to decide whether the strategy update is a limitation or unwinding. The fascinating thing to note is that a strategy unwinding doesn't influence exchanges executing by prudence of that strategy yet may require cut short of exchanges executing by temperance of different arrangements that are determined over a similar subject and item.

3.1.1 Lattice Based Access Control Model

A *database* is specified as a collection of objects together with a set of *integrity constraints* on these objects. At any given time, the *state* of the database is determined by the values of the objects in the database. An adjustment of the worth of a data set object impacts the state. Trustworthiness imperatives are predicates characterized over the state. An information base state is supposed to be predictable on the off chance that the upsides of the items fulfill the given trustworthiness requirements.

A *transaction* is an activity that changes the data set starting with one predictable state then onto the next. To keep the information base from becoming conflicting, exchanges are the main means by which information objects are gotten to and changed. An exchange can be started by a client, a gathering, or another cycle. An exchange acquires the entrance honors of the substance starting it. An exchange can execute a procedure on an information base item provided that it has the honor to perform it. Such honors are indicated by access control approaches.

An approval strategy determines what tasks an element can perform on another substance. Regard for frameworks that utilization the shut approach supposition and backing positive approval arrangements as it were. This implies that the approaches just determine what tasks a substance is permitted to perform on another element. There is no unequivocal approach that determines what tasks an element isn't permitted to perform on another substance. The shortfall of an unequivocal approval strategy approving an element to play out some procedure on another substance is deciphered as not being permitted to perform procedure on element.

Straightforward sorts of approval strategies that are determined by subject, article, and activities. A subject can be a client, a gathering of clients or a cycle. An item, in our model, is an information object or a gathering of information objects. A subject can perform just those procedure on the item that are determined in the tasks.

3.2 Defining Policies and Access Rights

I. Defining [Policy]

A *policy* is a function that maps a subject and an object to a set of operations. Lattice policy formally denoted this as follows:

$$P : S \times O \rightarrow \mathbb{P}(R)$$

Where P represents the policy function, S, represents the set of subjects, O represents the set of objects, P(R) represents the power set of operations. In a database, policies are stored in the form of policy objects.

II. Defining [Policy Goal]

A policy object Pi consists of the triple <Si, Oi, Ri> where
Si, Oi, Ri denotes the subject, the object, and the operations of the policy respectively. Subject Si can perform only those operations on the object Oi that are specified in Ri.

A subject is permitted to carry out a set of operations on an object by a policy. The subject will be able to carry out a different set of operations on the object after this policy is updated. Knowledge of the kind of policy update is used in the algorithms we propose in the following sections. We must represent the various sets of allowable operations on an object in order to comprehend the effect of a policy update operation. This is accomplished by the organizer by using a lattice to represent an object's access rights.

III. Defining [Representing an Object's Access Right]

The set of all possible operations that are specified on Object Oi should be Opi = "Op1, Op2,..., Opn."Opi's set of operations are arranged in the form "Op1, Op2,..., Opn."Any right to access the object Oi in the form of an n-element vector (i1, i2,..., in).The operation Opk cannot be carried out on the object Oi in some access right Rj if the k-th element of this vector is zero (ik = 0). When the k-th element of an access right Rm reaches 1 (ik = 1), it indicates that the access right Rm permits the operation Opk to be carried out on the object Oi. The maximum number of access rights that an object Oi can have been equal to 2n.

IV. Defining [Access Rights Lattice of an Object]

The set of all conceivable access privileges on an item Oi can be addressed as a cross section which we term the entrance freedoms grid of article Ri. The documentation ARL (Oi) signifies the arrangement of all hubs in the entrance freedoms cross section of item Oi. All conceivable access control honors relating to an article can be addressed as the hubs on the entrance privileges cross section of the item. Every hub in the grid addresses a particular access control honor.

The lower bound on this grid (named as Hub 0) signifies the shortfall of any entrance privileges on this article. The upper bound means the presence of the multitude of privileges; any subject having these freedoms can play out every one of the procedures on the article. Different focuses in the grid signify the moderate honors. Figure 3.1(a) shows the conceivable access privileges related with a document having just two tasks: Read and Compose. The main digit means the Read activity and the most un-huge cycle indicates the Compose activity.

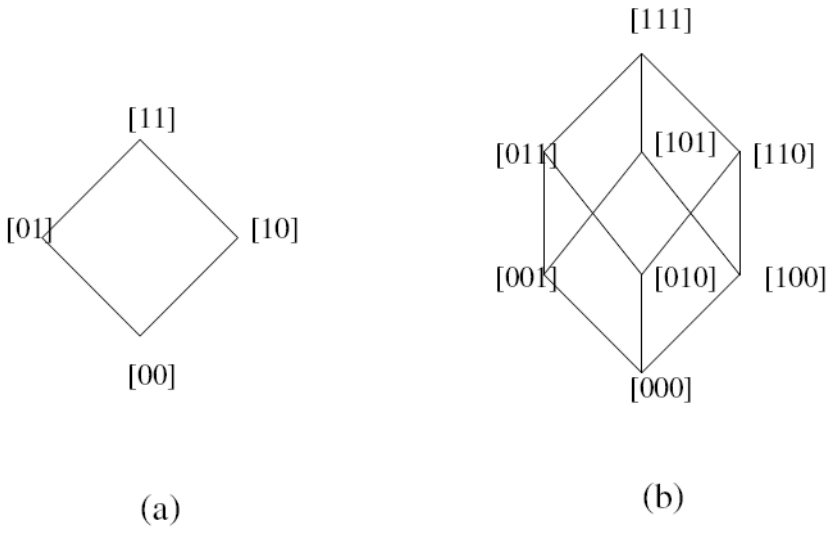


Figure 3.1 Representing Possible Access Control Rights of Objects

The lower bound named as Hub 00 means the shortfall of Perused and Compose honor. The Hub 01 means that the subject has Compose honor yet doesn't have Understood honors. The Hub 10 connotes that the subject has Perused honor yet no Compose honor. The Hub 11 demonstrates that the subject has both Perused and Compose honors. Figure 3.1(b) shows the conceivable access freedoms related with an article having three tasks.

3.3. System Configuration by Lattice

A lattice model offers more assurance to information. This makes it to be not quite the same as different techniques talked about in the above segment. Different security levels or values are utilized to shape the grid L. The security values have a superior relationship among themselves. The L accepts the structure as given in (1)

$$L = Ci * Y \quad (1)$$

where, Y is a set of additional constraints$1 \leq i \leq n$ and C1> C2> C3 …. > Cn is security values.

The application in medical care was taken for instance and various archives are accessible in this framework. Every one of the records characterized in the framework go under a report set called object O which is characterized by (2).

$$O = Di \text{ where } 1 \leq i \leq n \quad (2)$$

There are different roles in a healthcare system such as manager, administrator, chief doctors, etc. Of them, each role is defined as the subject S given in (3).

$$S = Ri \text{ where } 1 \leq i \leq n \quad (3)$$

The security value is given to document and it takes the form v = Ci y where $1 \leq i \leq n$ and y contained in Y.

If v1 = C1 and v2 = C2 then v1 "superior than" v2. Based on the security value, the read or write operations are applied by different subjects. The lattice L is represented in the following diagram (Figure 3.2).

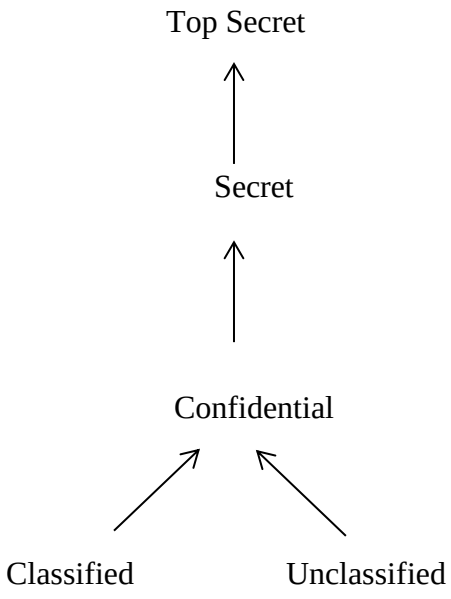


Figure 3.2 Lattice Model for Proposed Method

In the proposed method, we are making the cross section for the association involving chart as portrayed in Calculation 1 which shows the relationship of the association components in Eqn. (1).

The understudy's records and different reports are considered as items Eqn. (2). In the wake of producing the relationship chart, access control framework for the patient records has been built utilizing Cross section model as portrayed in Calculation 2.

In which, the subjects in Eqn. (3) are accessible in some level li and approaching freedoms to certain subjects obj. While framework clients are putting away the record into the got framework capacity, each report is doled out a security esteem.

Each subject should make validation certifications through the point of interaction. At the point when the subject is attempting to recover the substance, their accreditations would have been checked and in the event that the validation has been succeeded, just the verified clients might get to the record, alongside one really checking, called approval. Approval would have been accomplished through access control lattice as referenced.

To store information, access control grid ought to be refreshed with new information objects in the wake of doing the approval cycle. After approval the clients are permitted to store the information in secure structure. This sort of coordination has been finished away stage. In the recovery stage, prior to getting to the information, access control network must be checked and either grant to get to the information or deny the entrance. After the effective finishing of the cross-section stage, then the client will be permitted to get to the information.

In the proposed technique, a bunch of methods is utilized to major areas of strength for accomplish for delicate reports. Methods are as per the following.

Table 3.1 Proposed Lattice construction Algorithm

Input: System security values

Output: Lattice

Procedure:

for each value i do

place the values in the respective level

end for

Table 3.2 Access Control generation Algorithm

Input: The roles defined in EDC System

Output: Access control matrix based on Lattice

Procedure:

for each role i do

assign the subject and object relationship

enter matrix value in the corresponding row and column

end for

Table 3.3 Authorization Algorithm

Input: Enter username and password

Output: Authorization success or failed

Procedure:

Check username and password with the existing records

if matching then

allow the user to either upload or download records

else

forward the request to either registration process or re-enter the credentials

Lattice model gives insurance against unapproved revelation and furthermore it offers assurance on adjustment of content, high accessibility through access control. These sorts of content assurance have been characterized by the information arrangement structure. Moreover, the layering model gives classification. This suggests no trade-off is engaged in the security settings in light of the fact that the coordinated system gives assurance against information breaks.

CHAPTER 4

SYSTEM DESIGN AND IMPLEMENTATION

Due to the rapid development of Computer and Internet technology, an ever-increasing number of resources of an organization or an association are put away in computerized design in data set. Data sets are additionally broadly utilized in each individual's day to day routine of each and every association. These associations are threated to open data set frameworks which is the procedures to be thought about while getting a data set and how to get a data set in various uprightness levels of significant layers. The proposed framework will control the protected information access on understudies' instructive information of Education Degree College.

This system will be developed as a secure data access control system using Lattice-Based Access Control in Education Degree College. Grid based admittance control gives Approval and forestalls approval assault. Cross section-based admittance control is additionally offering access control and used to protect unapproved revelation, adjustment, guarantee accessibility. These sorts of exercises have been characterized by the information characterization system. In this framework, in view of the jobs of the association, an entrance control strategy is ready in which various freedoms are allocated to the clients of the association. The fundamental errand of this framework is making a confined admittance as far as access control strategy.

Grid model is developed and access control strategy has been characterized in light of the cross section to give limited admittance for the information. At the point when security is compromised at the opposite end, then it turns into a test to guarantee secrecy and uprightness of the client information on EDC framework. In this manner, to defeat the security issues, information should be done the approval cycle prior to put away it. In this framework, an adaptable and powerful information security plot is proposed to safeguard client information in view of access control strategy (Lattice Based).

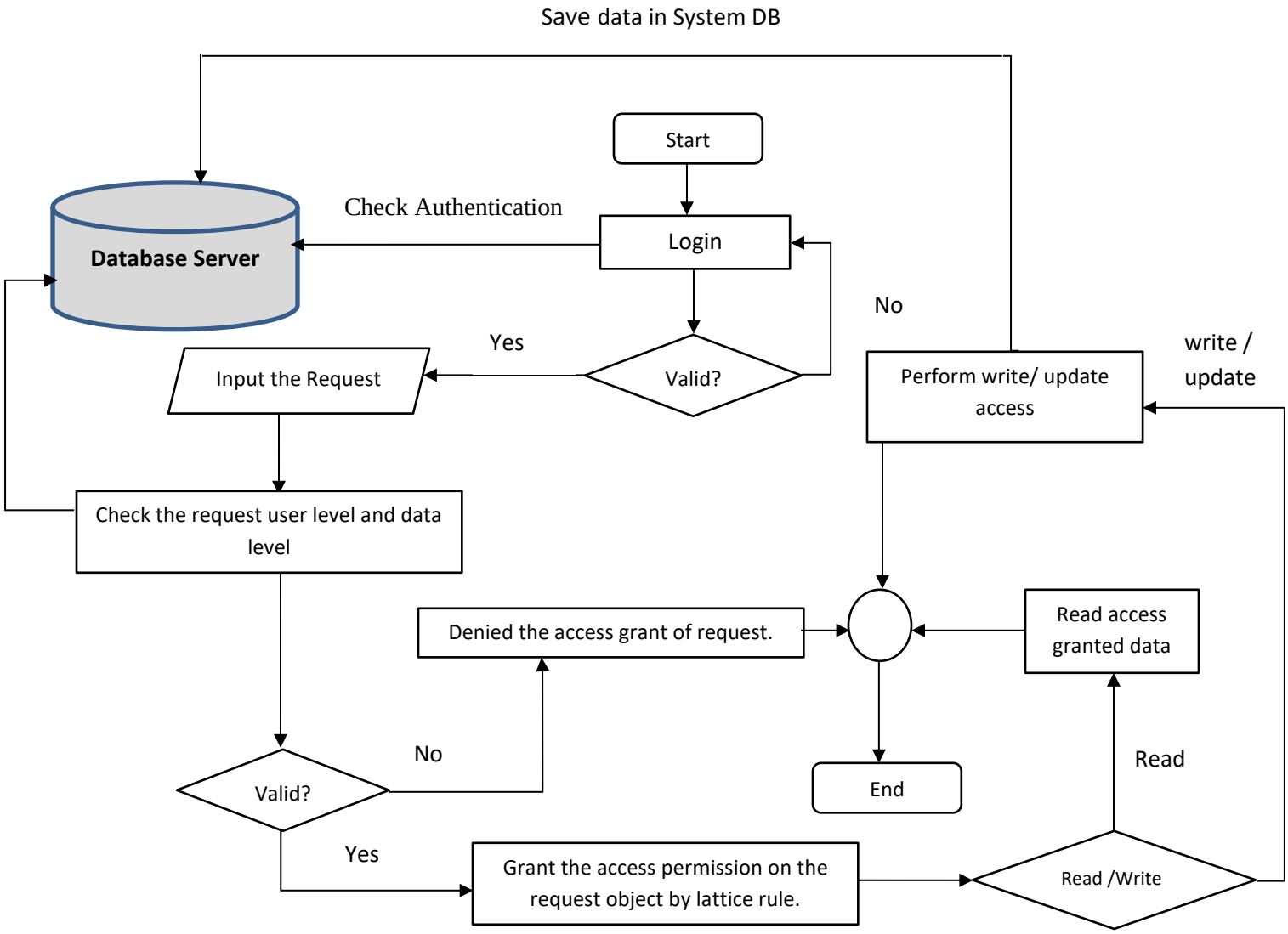


Figure 4.1 The System Flow

4.1 The Organization Structure of Proposed EDC System

Departments of EDC (Department of Proposed System): There are seven main departments in proposed education collage as shown below.

1. Educational Studies
2. Methodology
3. Myanmar
4. English
5. Mathematics
6. Science
7. Social Studies

Syllabus structure for EDC students: There are fourteen different subjects which are derived from above mentioned seven departments.

1. Educational Studies (Psychology+ Theory)
2. Myanmar
3. English
4. Mathematics
5. Science (Chemistry+ Physics+ Biology)
6. Social Studies (History + Geography+ Economics)
7. Physical Education
8. Life Skills
9. Art (Performing Art and Visual Art)
10. Morality and Civics

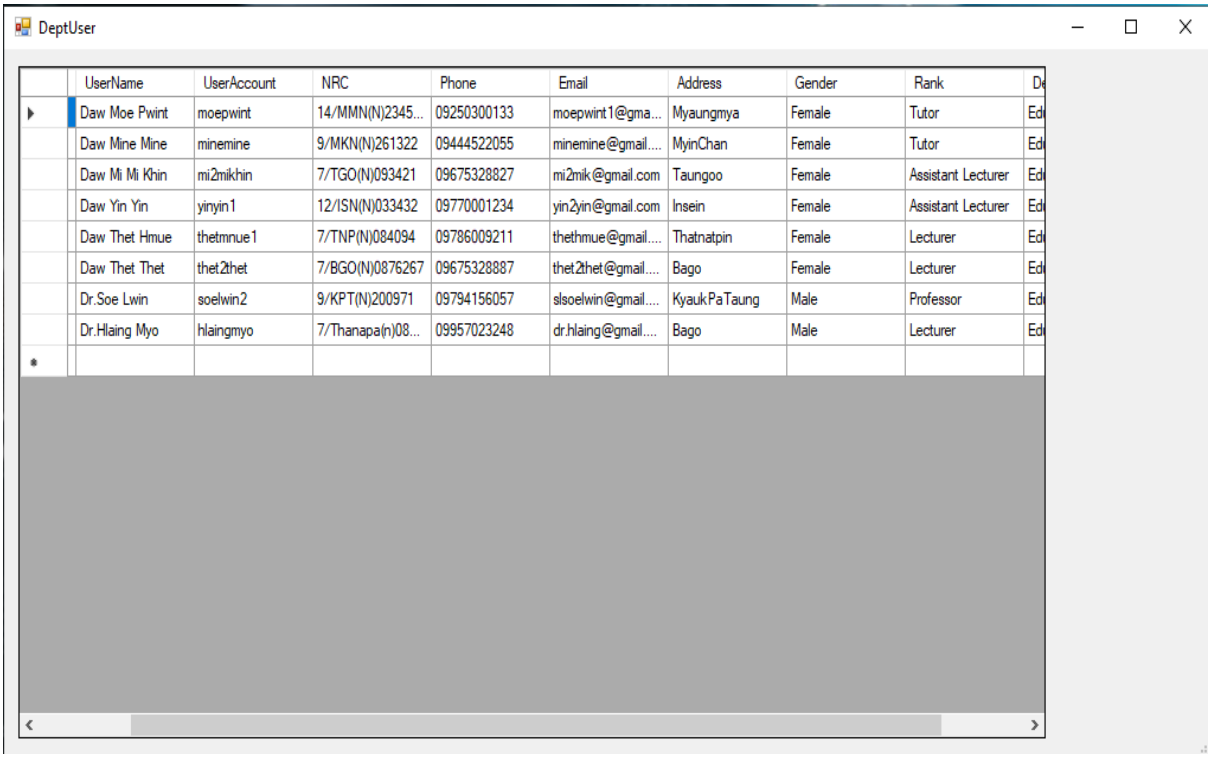
11. Local curriculum

12. Information and Communication Technology (ICT)

13. Practicum

14. Reflection

User Level for Proposed System: There are three different user levels for each department. In each department: Teacher level, Senior Teacher level and Head of Department. All department authority level is controlled by one admin of system. Sample data of department user is organized as shown in Figure 4.1.



UserName	UserAccount	NRC	Phone	Email	Address	Gender	Rank	De
Daw Moe Pwint	moepwint	14/MMN(N)2345...	09250300133	moepwint1@gma...	Myaungmya	Female	Tutor	Edu
Daw Mine Mine	minemine	9/MKN(N)261322	09444522055	minemine@gmail....	MyinChan	Female	Tutor	Edu
Daw Mi Mi Khin	mi2mikhin	7/TGO(N)093421	09675328827	mi2mik@gmail.com	Taungoo	Female	Assistant Lecturer	Edu
Daw Yin Yin	yinyin1	12/ISN(N)033432	09770001234	yin2yin@gmail.com	Insein	Female	Assistant Lecturer	Edu
Daw Thet Hmue	thetmnue1	7/TNP(N)084094	09786009211	thethmue@gmail....	Thatnatpin	Female	Lecturer	Edu
Daw Thet Thet	thet2thet	7/BGO(N)0876267	09675328887	thet2thet@gmail....	Bago	Female	Lecturer	Edu
Dr.Soe Lwin	soelwin2	9/KPT(N)200971	09794156057	slsoelwin@gmail....	Kyauk Pa Taung	Male	Professor	Edu
Dr.Hlaing Myo	hlaingmyo	7/Thanapa(n)08...	09957023248	dr.hlaing@gmail....	Bago	Male	Lecturer	Edu

Figure 4.2 Department User View Page

4.2. System Implementation

The proposed framework affirms that the different degree of secrecy is upheld at the reason behind information handling through grid and does the anticipation against unapproved divulgence. Grid based admittance control gives the characterization of access strategy in view of the proprietor of the archive and various jobs in the EDC staff who are qualified to get to the record. By this way the security controls for every grouping are additionally been accomplished.

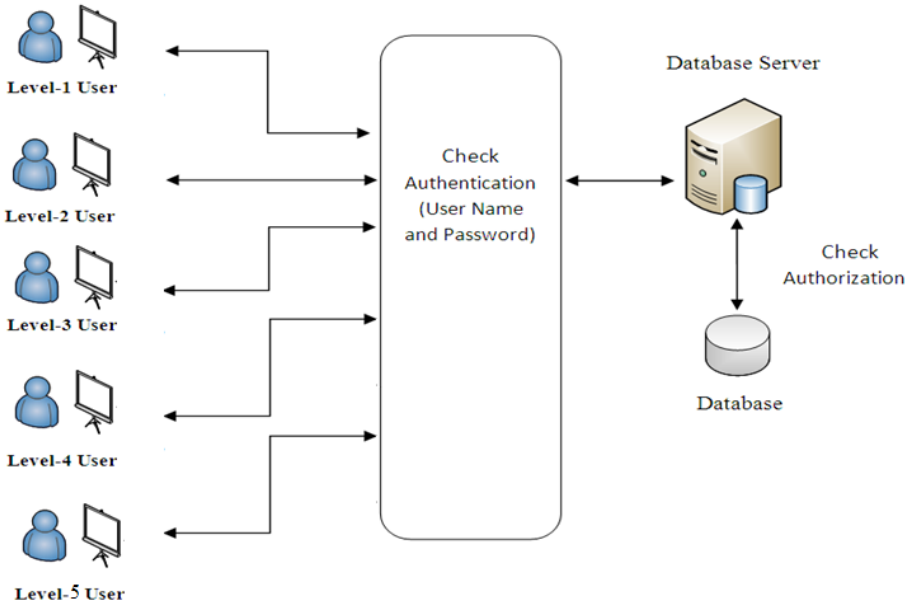


Figure 4.3 System Overview

In the proposed system, administrator can access all data and can make all transaction of the whole system and the data occupation of the respective level. The users of the proposed system are Admin User (level-1), Department Head (level-2), Senior Teacher (level-3), Teaching Staff (level-4) and Student Affair (level-5). These levels are defined by system administrator or board of the organization. The assigned category of the admin on the object accesses are:

- Essential data submission,
- Data Management (Limited by System Rules), and

- User management (Subject management).

Authentication: Authentication is the act of establishing or confirming something (or someone) as *authentic*, that is, claims made by or about the subject are true. The system will permit the system users if their login name and password is correct. And then, the system user can access the data by their level defined by administrator. This is called authorization. The authentication process of the system is shown in following figure 4.3(a) and figure 4.3(b).

Figure 4.4 (a) System Login Page [Authentication Pass]

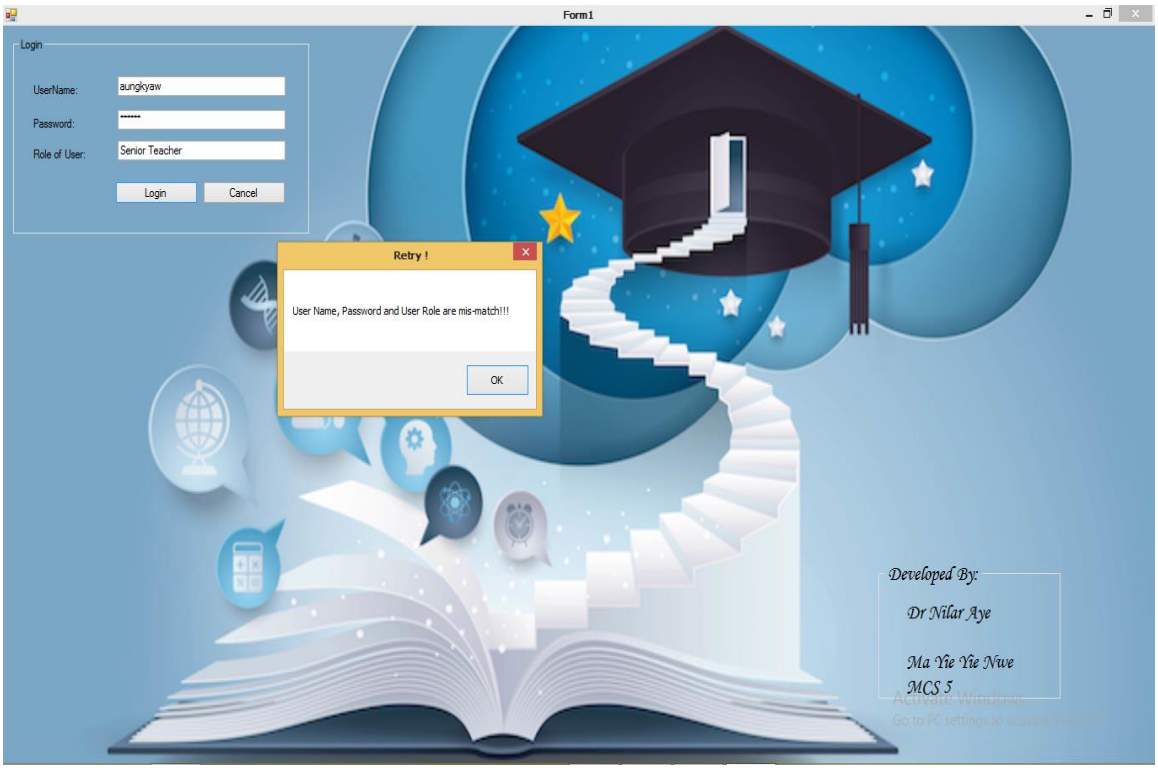


Figure 4.4 (b) System Login Page [Authentication Fail]

System Authorization: The process of determining that has access to a resource is known as authorization, and it is connected to access control in particular as well as information security and computer security as a whole. To put it another way, "to authorize" means to set access policy. Human resources staff, for instance, have permission typically to access employee records, and this policy is typically codified in computer system access control rules. The system uses the access control rules to decide whether to grant or deny access requests from consumers who have been authenticated during operation. As depicted in figures 4.5 and 4.6, authorization for the proposed system can be granted or denied.

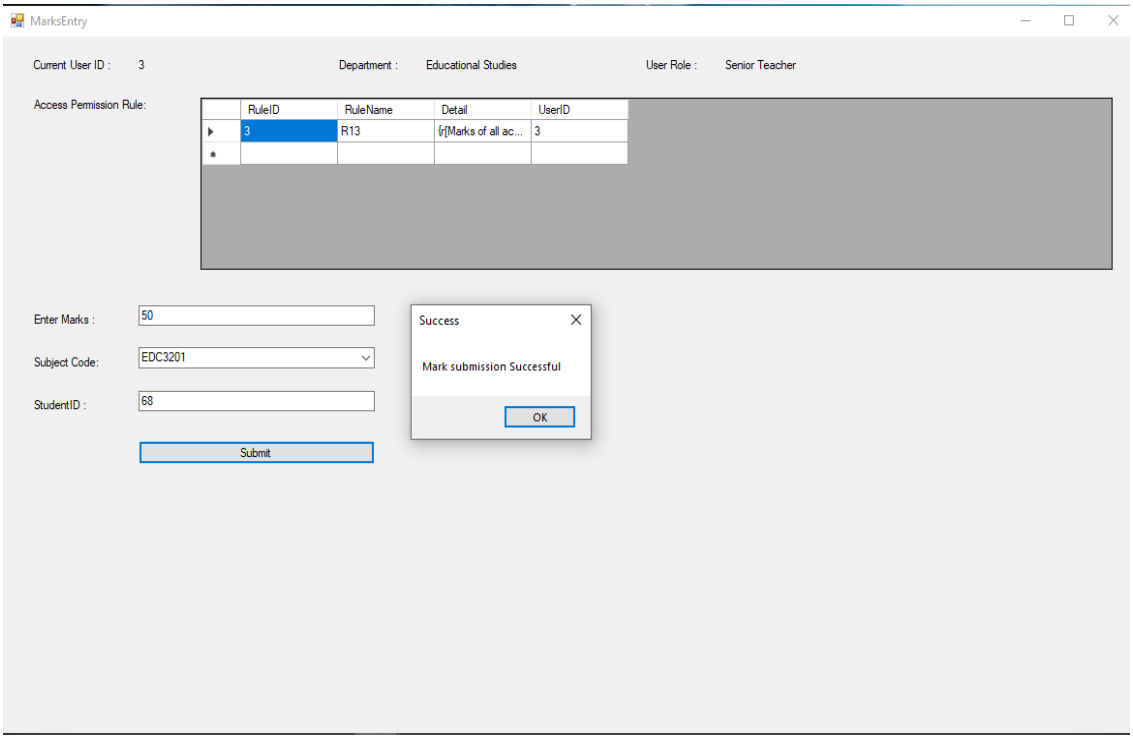


Figure 4.5 Access Grant (Authorization process) for New Mark Entry

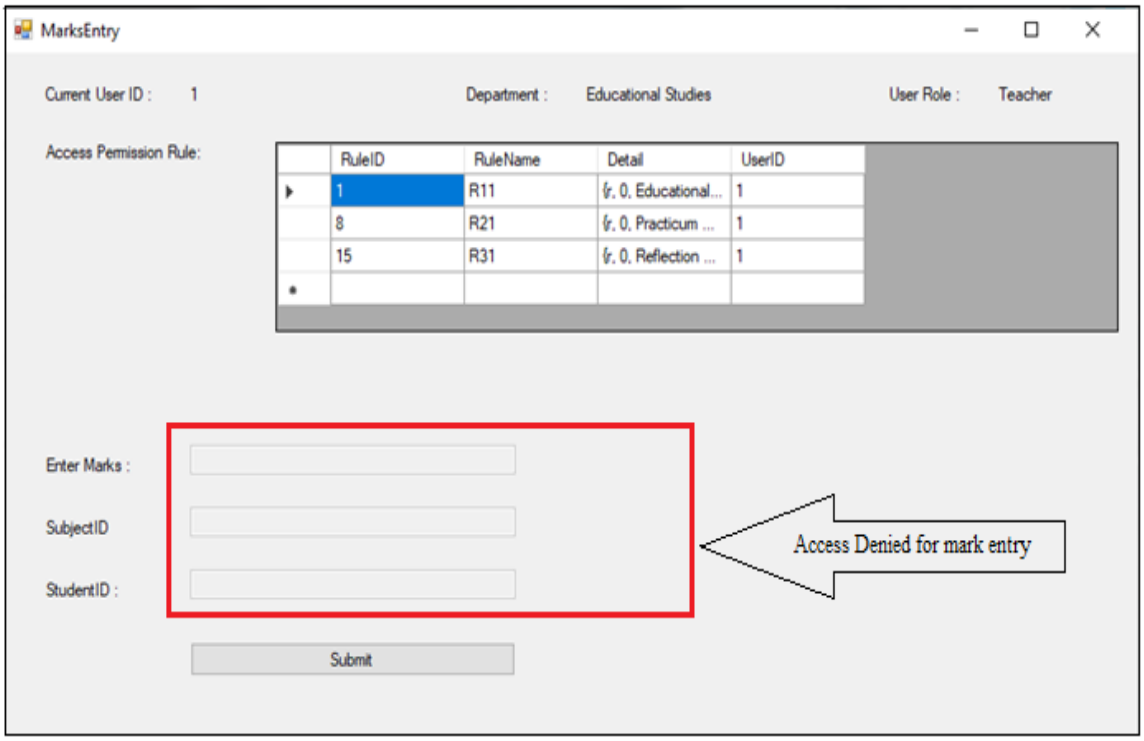
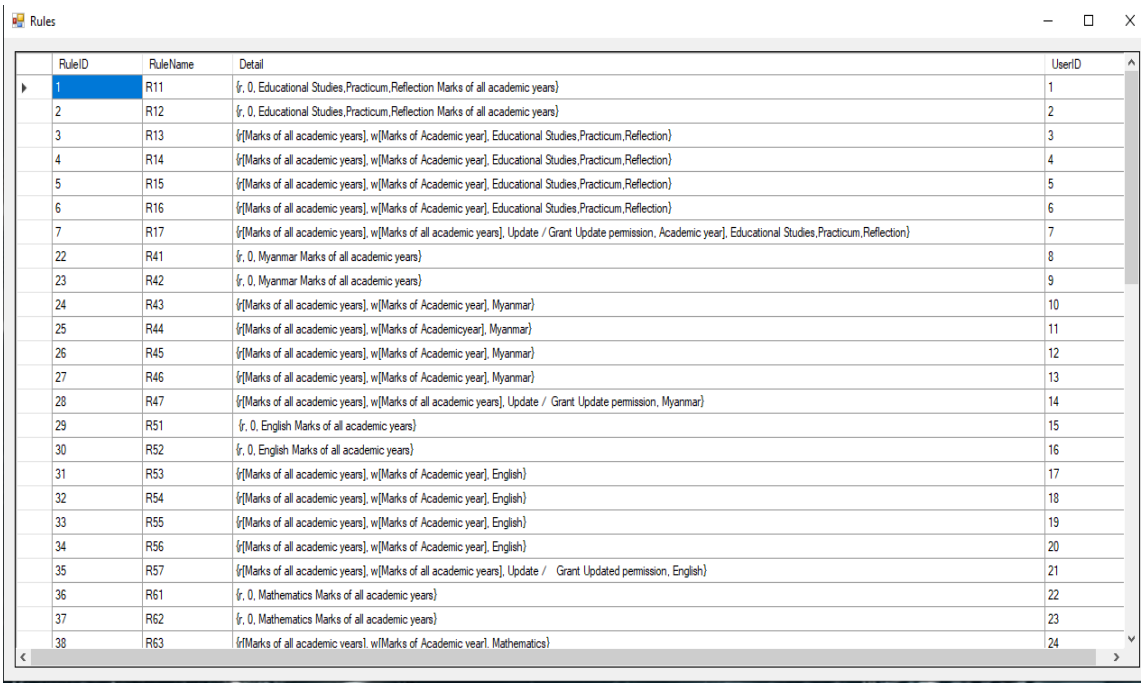


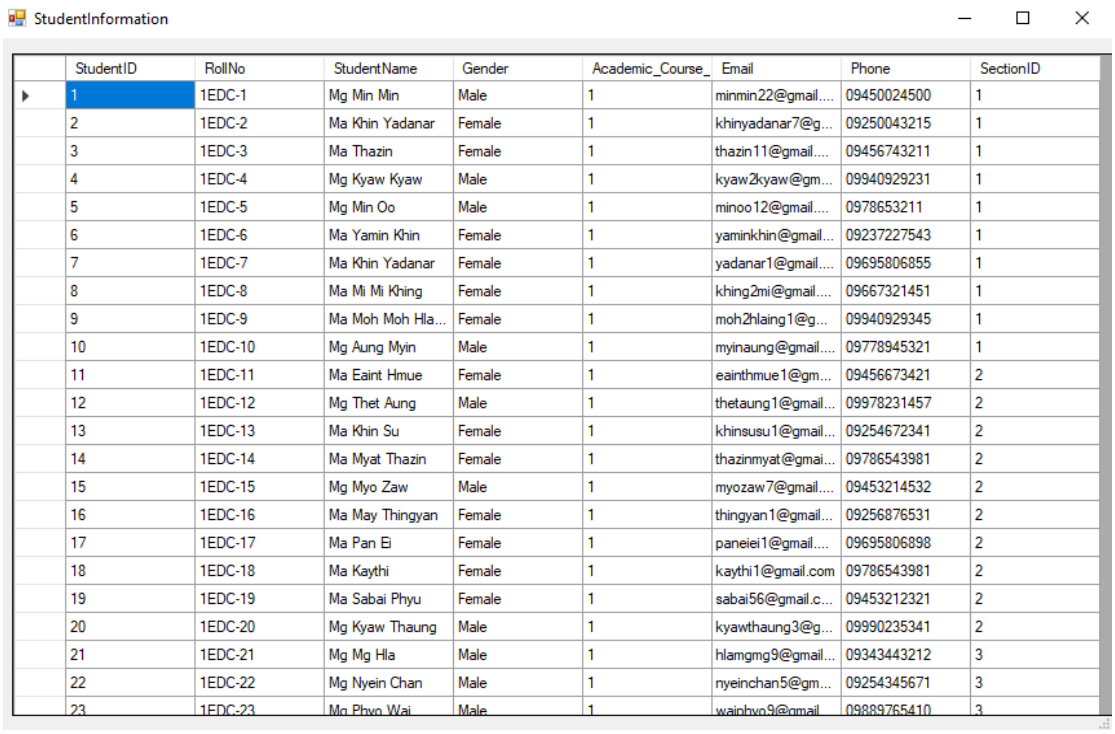
Figure 4.6 Access Denied (Authorization process) for New Mark Entry



RuleID	RuleName	Detail	UserID
1	R11	{r, 0, Educational Studies,Practicum,Reflection Marks of all academic years}	1
2	R12	{r, 0, Educational Studies,Practicum,Reflection Marks of all academic years}	2
3	R13	{r[Marks of all academic years], w[Marks of Academic year], Educational Studies,Practicum,Reflection}	3
4	R14	{r[Marks of all academic years], w[Marks of Academic year], Educational Studies,Practicum,Reflection}	4
5	R15	{r[Marks of all academic years], w[Marks of Academic year], Educational Studies,Practicum,Reflection}	5
6	R16	{r[Marks of all academic years], w[Marks of Academic year], Educational Studies,Practicum,Reflection}	6
7	R17	{r[Marks of all academic years], w[Marks of all academic years], Update / Grant Update permission, Academic year], Educational Studies,Practicum,Reflection}	7
22	R41	{r, 0, Myanmar Marks of all academic years}	8
23	R42	{r, 0, Myanmar Marks of all academic years}	9
24	R43	{r[Marks of all academic years], w[Marks of Academic year], Myanmar}	10
25	R44	{r[Marks of all academic years], w[Marks of Academicyear], Myanmar}	11
26	R45	{r[Marks of all academic years], w[Marks of Academic year], Myanmar}	12
27	R46	{r[Marks of all academic years], w[Marks of Academic year], Myanmar}	13
28	R47	{r[Marks of all academic years], w[Marks of all academic years], Update / Grant Update permission, Myanmar}	14
29	R51	{r, 0, English Marks of all academic years}	15
30	R52	{r, 0, English Marks of all academic years}	16
31	R53	{r[Marks of all academic years], w[Marks of Academic year], English}	17
32	R54	{r[Marks of all academic years], w[Marks of Academic year], English}	18
33	R55	{r[Marks of all academic years], w[Marks of Academic year], English}	19
34	R56	{r[Marks of all academic years], w[Marks of Academic year], English}	20
35	R57	{r[Marks of all academic years], w[Marks of all academic years], Update / Grant Updated permission, English}	21
36	R61	{r, 0, Mathematics Marks of all academic years}	22
37	R62	{r, 0, Mathematics Marks of all academic years}	23
38	R63	{r[Marks of all academic years], w[Marks of Academic year], Mathematics}	24

Figure 4.7 Rules defined the system

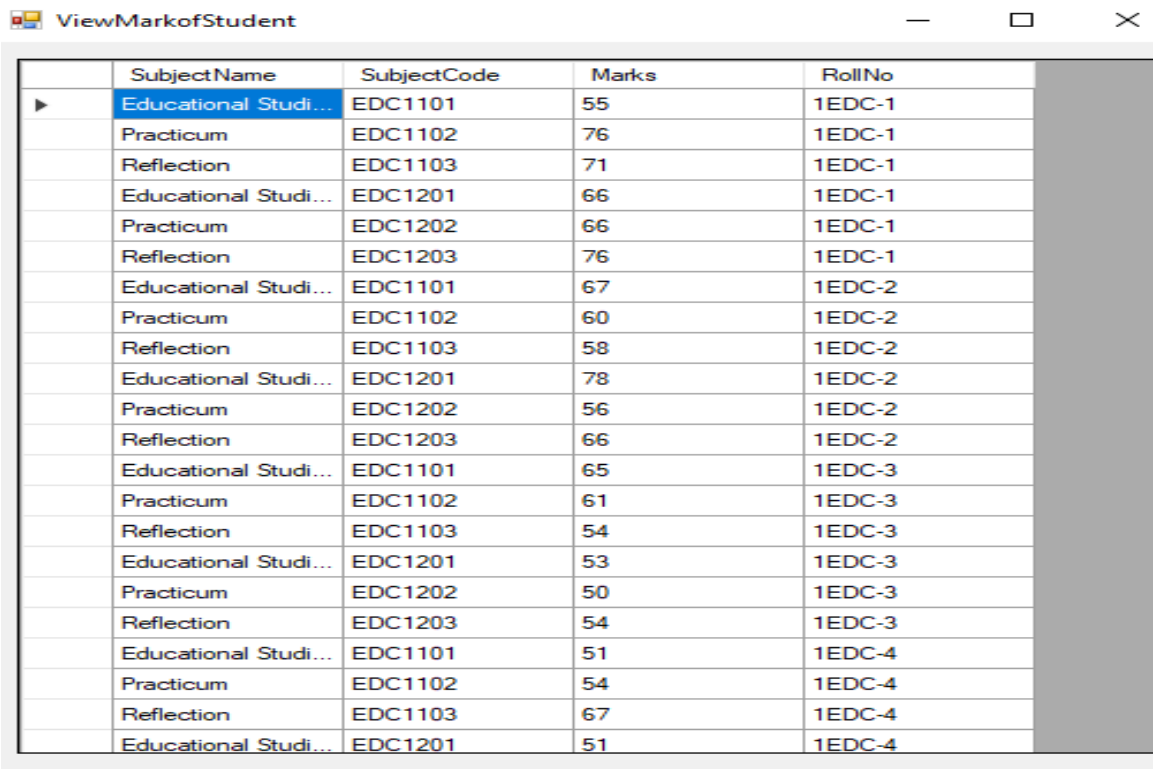
The access control rules which are organized by Lattice Based theory is shown in figure 4.7. The rules are unique for each role of user on each department.



StudentID	RollNo	StudentName	Gender	Academic_Course_	Email	Phone	SectionID
1	1EDC-1	Mg Min Min	Male	1	minmin22@gmail....	09450024500	1
2	1EDC-2	Ma Khin Yadanar	Female	1	khinyadanar7@g...	09250043215	1
3	1EDC-3	Ma Thazin	Female	1	thazin11@gmail....	09456743211	1
4	1EDC-4	Mg Kyaw Kyaw	Male	1	kyaw2kyaw@gm...	09940929231	1
5	1EDC-5	Mg Min Oo	Male	1	minoo12@gmail....	0978653211	1
6	1EDC-6	Ma Yamin Khin	Female	1	yaminkhin@gmail...	09237227543	1
7	1EDC-7	Ma Khin Yadanar	Female	1	yadanar1@gmail....	09695806855	1
8	1EDC-8	Ma Mi Mi Khing	Female	1	khing2mi@gmail....	09667321451	1
9	1EDC-9	Ma Moh Moh Hla...	Female	1	moh2hlaing1@g...	09940929345	1
10	1EDC-10	Mg Aung Myin	Male	1	myinaung@gmail....	09778945321	1
11	1EDC-11	Ma Eaint Hmue	Female	1	eainthmue1@gm...	09456673421	2
12	1EDC-12	Mg Thet Aung	Male	1	thetaung1@gmail...	09978231457	2
13	1EDC-13	Ma Khin Su	Female	1	khinsusu1@gmail...	09254672341	2
14	1EDC-14	Ma Myat Thazin	Female	1	thazinmyat@gmai...	09786543981	2
15	1EDC-15	Mg Myo Zaw	Male	1	myozaw7@gmail....	09453214532	2
16	1EDC-16	Ma May Thingyan	Female	1	thingyan1@gmail...	09256876531	2
17	1EDC-17	Ma Pan Ei	Female	1	paneiei1@gmail....	09695806898	2
18	1EDC-18	Ma Kaythi	Female	1	kaythi1@gmail.com	09786543981	2
19	1EDC-19	Ma Sabai Phyu	Female	1	sabai56@gmail.c...	09453212321	2
20	1EDC-20	Mg Kyaw Thaung	Male	1	kyawthaung3@g...	09990235341	2
21	1EDC-21	Mg Mg Hla	Male	1	hlamgmg9@gmail...	09343443212	3
22	1EDC-22	Mg Nyein Chan	Male	1	nyeinchan5@gm...	09254345671	3
23	1EDC-23	Mg Phyo Wai	Male	1	waiphyo9@gmail...	09889765410	3

Figure 4.8 Student Information Page

Figure 4.8 is the Student Information Page of Proposed system, in which all of the student information are listed but marks are described. Because of the student mark is confidential for each department. Only the respective subject user (teacher/senior teacher/ Head of Department of respective Subject) can be viewed as shown in figure 4.9.



SubjectName	SubjectCode	Marks	RollNo
Educational Studi...	EDC1101	55	1EDC-1
Practicum	EDC1102	76	1EDC-1
Reflection	EDC1103	71	1EDC-1
Educational Studi...	EDC1201	66	1EDC-1
Practicum	EDC1202	66	1EDC-1
Reflection	EDC1203	76	1EDC-1
Educational Studi...	EDC1101	67	1EDC-2
Practicum	EDC1102	60	1EDC-2
Reflection	EDC1103	58	1EDC-2
Educational Studi...	EDC1201	78	1EDC-2
Practicum	EDC1202	56	1EDC-2
Reflection	EDC1203	66	1EDC-2
Educational Studi...	EDC1101	65	1EDC-3
Practicum	EDC1102	61	1EDC-3
Reflection	EDC1103	54	1EDC-3
Educational Studi...	EDC1201	53	1EDC-3
Practicum	EDC1202	50	1EDC-3
Reflection	EDC1203	54	1EDC-3
Educational Studi...	EDC1101	51	1EDC-4
Practicum	EDC1102	54	1EDC-4
Reflection	EDC1103	67	1EDC-4
Educational Studi...	EDC1201	51	1EDC-4

Figure 4.9 Student Marks View

4.2.1 Rules of system users

P_i = < Subject (Si), Data Object (Oi), Operation (Ri)>

R_i = {read Y/N, write Y/N, Premium permission/ Null, Data Range or Data Area}

[Lower bound ➔ read Y/N: Upper bound ➔ write Y/N, Premium permission]

Rules for Teacher role

P_{ij} = < Subject (Si), Data Object (Oi), {r, 0, Related Data Object of academic years}>

R_{ij} = {r, 0, (Data Object) Related Data Object of academic years}

[Lower bound ➔ read (r): Upper bound ➔ read (w)]

Rules for Senior Teacher role

P_{ij} = < Subject (Si), Data Object (Oi), {r [Data Object of all academic years], w [Data Object of Academic year], Related Data Object of academic years}>

R_{ij} = {r [Data Object of all academic years], w [Data Object of Academic year], Related Data Object of academic}

[Lower bound ➔ read (r): Upper bound ➔ write (w)]

Rules for Head of Department role

P_{ij} = < Subject (Si), Data Object (Oi), {r [Data Object of all academic years], w/ Update permission [Data Object of Academic year], Related Data Object of academic years}>

R_{ij} = {r [Data Object of all academic years], w/ Update permission [Data Object of Academic year], Related Data Object of academic}

[Lower bound ➔ read (r): Upper bound ➔ update (u)]

4.3. The Database Design of the System

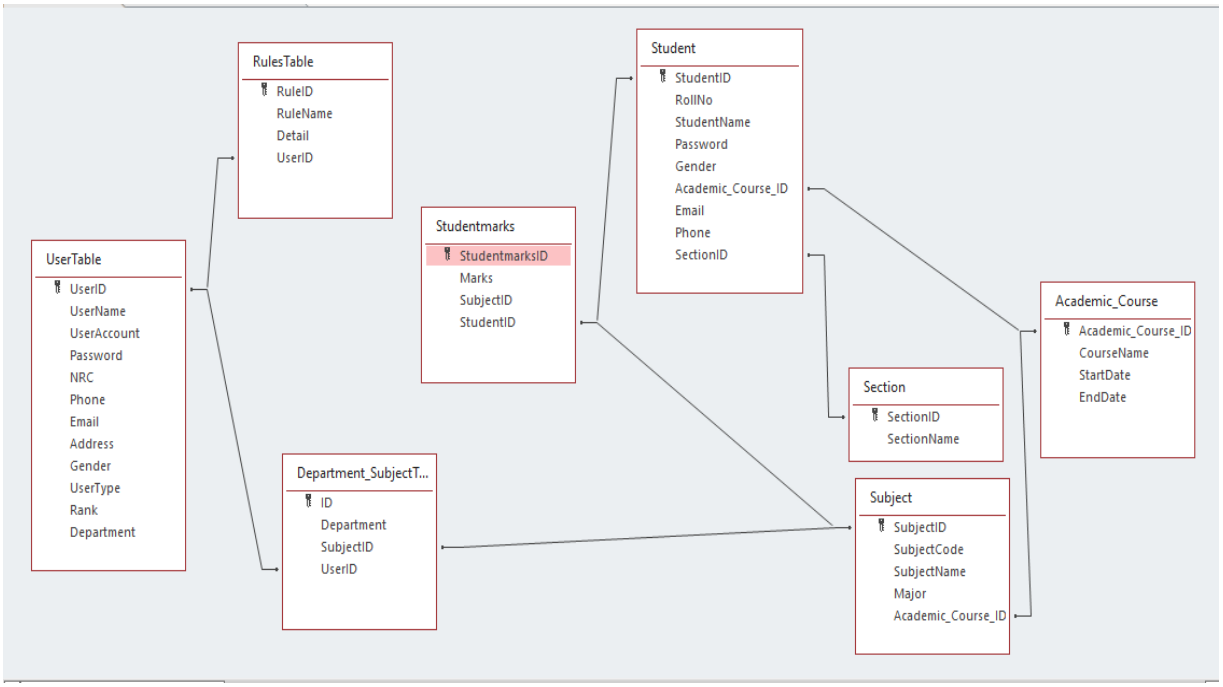


Figure 4.10 The Database Design of the System

Figure 4.10 shows the database design of the system. In which, all of the stored data are not freely granted. The data tables are under the control of Lattice Based Access Control.

4.4 Testing and Discussion

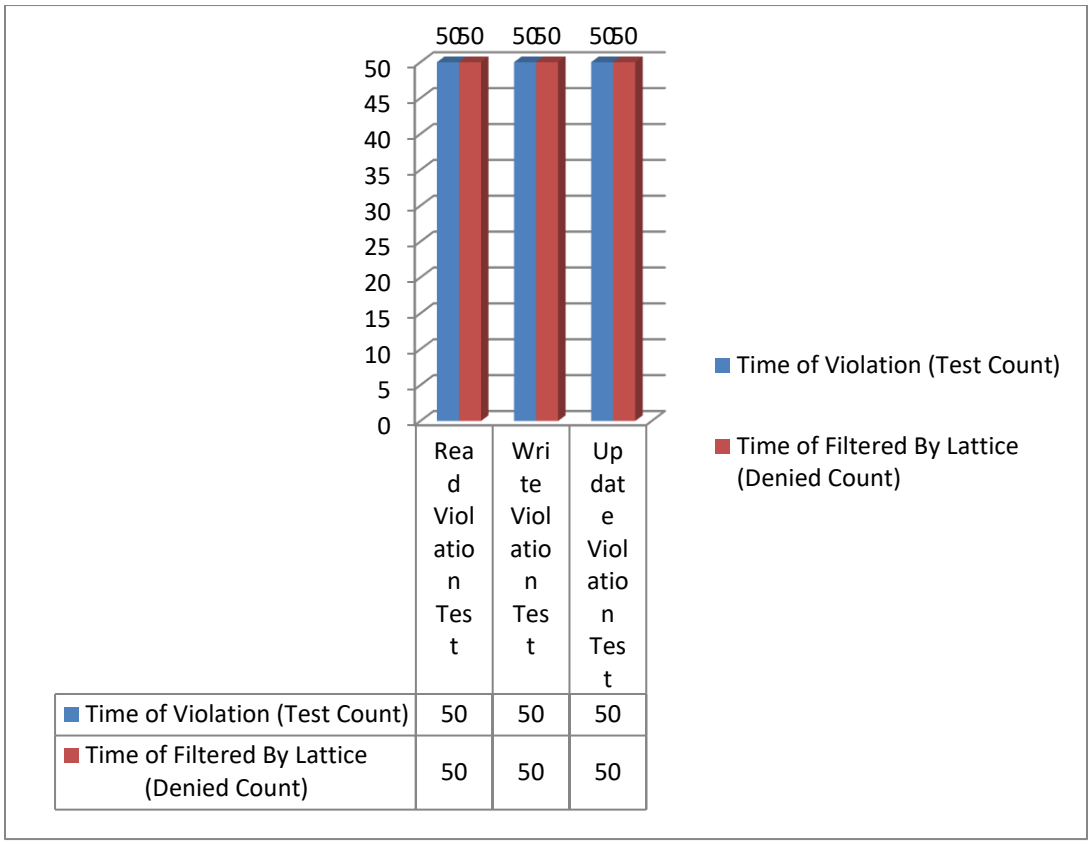


Figure 4.11 Test for Violation and Filtering by Lattice

This System tested three points of view: (1) Violating read access request are made fifty times but this system denied that violated access request (2) Violating write access request are made fifty times but this system denied that violated access request. (3) Violating update access request are made fifty times but this system denied that violated access request.

CHAPTER 5
CONCLUSION, LIMITATION AND FURTHER EXTENSION

5.1 Conclusion

Having access control, only the responsible person has the right to read, write and amend the data (marks) for their own subject. Other users (TEs) could not have the chance to access the marks of other subjects. Each head of department is fully permission the authorized person for their related subjects. Access control faces new challenges in dynamic environments. Access control policies need to be updated in real time as entities, configurations, and operational modes change in such circumstances. Cross section model gives security against unapproved revelation and furthermore it offers insurance on change of content high accessibility through access control. These sorts of content security have been characterized by the information arrangement system. The proposed model also gives classification. This access control of EDC system has multilevel to protect in relational database. These lattice rules will cooperate together to get secure strengthened. Authentication and authorization play a very important role in database security.

5.2 Benefits of the System

The system can provide confidentiality restriction. Moreover, the administrator and owner of the system can more effectively manage and maintain the important information resources in a manner consistent with security policies. Finally, the sensitive data in the database can be saved securely. Distributed access can be granted. The main advantage of the system is to reduce time-consuming for inputting marks. There is no need to wait for members of exam-board as each department will be given password to insert marks for particular subject.

5.3 Limitations

This system restricts the write access by attributes. Thus, only the user who has full write access can insert new records. Moreover, each user is assigned to only one role. It does not allow multiple rows assignment for the user.

5.4 Further Extension

For sensitive data, security is more important. The data can be made to secure by using various methodologies. This system user has only data facilities to control security. This system is only implemented to control unauthorized access to data in the process to safeguard sensitive data, another facility – data encryption by using Cryptographic technique – is suggested as future work of this thesis. This system can also be extended hybrid structure of cryptography and access control techniques. This system will be helpful to the examination process in EDCs for distributed data sharing. The exam result will be announced on the web-page. Every-one can access result in different place at the same time.

AUTHOR'S PUBLICATION

[1] Yie Yie Nwe, Nilar Aye, "Secure Educational Data Management Using Lattice Based Access Control", Parallel & Soft Computing, University of Computer Studies, Yangon, 2022.

REFERENCES

[1] "A Lattice-Based Approach for Updating Access Control Policies in Real-Time", Tai Xin Indrakshi Ray Department of Computer Science Colorado State University, 2003.

[2] Bell, D.E & LaPadula, L.J.(1976). Secure Computer Systems: Unified Exposition and Multics Interpretation (MTR-2997 Rev.1) MITRE Corp., Bedford,MA.

[3] Database Server Security for Banking Information System, Zayar Aung, Htay Htay Thaung, University of Computer Studies, Yangon,2009.

[4] I.Ray and T.Xin. Implementating Real-Time Update of Access Control Policies. In Proceedings of the 18th IFIP WG 11.3 Working Conference on Data and Applications Security, 2004.

[5] I Ray. Real Time Updation of Security Policies. Data and Knowledge Engineering, 49(3):287-309, June 2004.

[6] Katsumata, S. and Yamada, S. [2019]. Group signatures without NIZK: From lattices in the standard model, in Y. Ishai and V. Rijmen (eds), EUROCRYPT 2019, Part III, Vol. 11478 of LNCS, Springer, Heidelberg, pp. 312–344.

[7] Lattice Based Access Control for Protecting User Data in Cloud Environments with Hybrid Security, Saravanan, Dr. Umamakeswari, SASTRA University, India, 2021.

[8] Ling, S., Nguyen, K., Wang, H. and Xu, Y. [2017b]. Lattice-based group signatures: Achieving full dynamicity with ease, in D. Gollmann, A. Miyaji and H. Kikuchi (eds), ACNS 17, Vol. 10355 of LNCS, Springer, Heidelberg, pp. 293– 312

[9] R. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. Role Based Access Control Models, *IEEE* Computer, 29(2):38-47, 1996.

[10] Steven A. Demurjian Multi-Level Security in Healthcare Using a Lattice-Based Access Control Model, University of Connecticut, Storrs, USA, International Journal of Privacy and Health Information Management (IJPHIM),2019.

[11] Sandhu,R. (1993). Lattice Based Access and Representations of Security Semantics for Database Applications [Doctoral Dissertation]. George Mason University.

[12] Steve Demurjian Fall Jin Ma, "Implementation of Mandatory Access Control in Role-based Security System", Computer Science & Engineering the University of Connecticut, 2001.