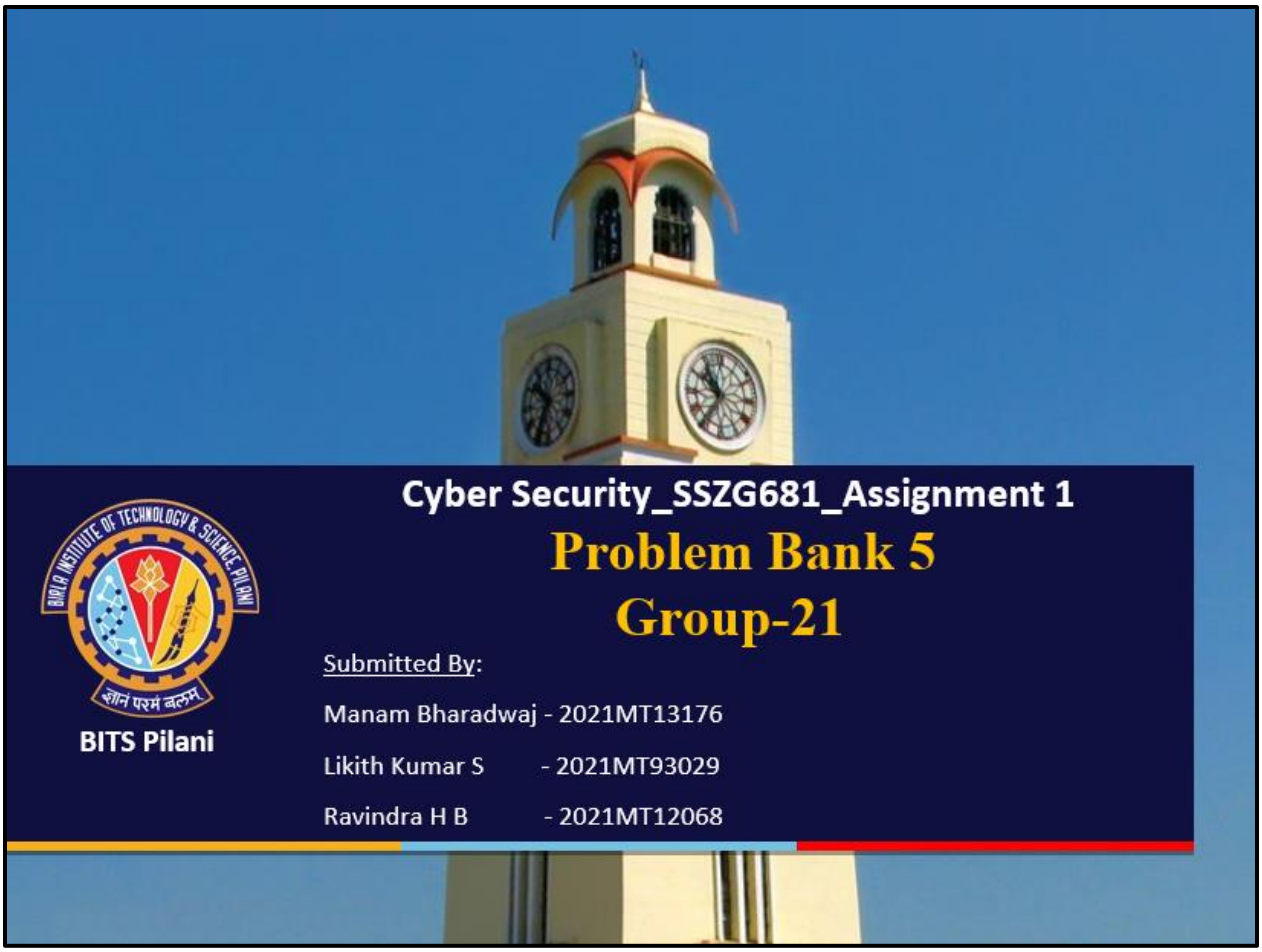



**Assignment Set Number:** **Problem Bank 5**

**Group Name:** **GROUP - 21**

**Contribution Table:**

| Sl. No. | Name (as appears in Canvas) | ID NO | Contribution |
|---|---|---|---|
| 1. | LIKITH KUMAR S | 2021MT93029 | Question no.1, Question no.2, Question no.3 |
| 2. | RAVINDRA H B | 2021MT12068 | Question no.1, Question no.2, Question no.3 |
| 3. | MANAM BHARADWAJ | 2021MT13176 | Question no.1, Question no.2, Question no.3 |

**Problem statement**:

**Question 1: Develop a construction to show that a system implementing the Chinese Wall Model can support the Bell-LaPadula Model.**

**Solution:**

Before we proceed with the implementation of the **Chinese Wall Model,** let's first try to understand what **Bell-LaPadula Model** is and what are the characteristics of the **Bell-LaPadula Model?**

**Bell-LaPadula Model (BLP)**:- This Model is described as **"**A state machine model which can be used to implement the access control in government and military applications areas.**"**

The main feature of this model is it mainly focuses on **"data confidentiality and controlled access",** which describes the rules for the protection of data integrity.

This model states 2 access control rules with 2 security properties:

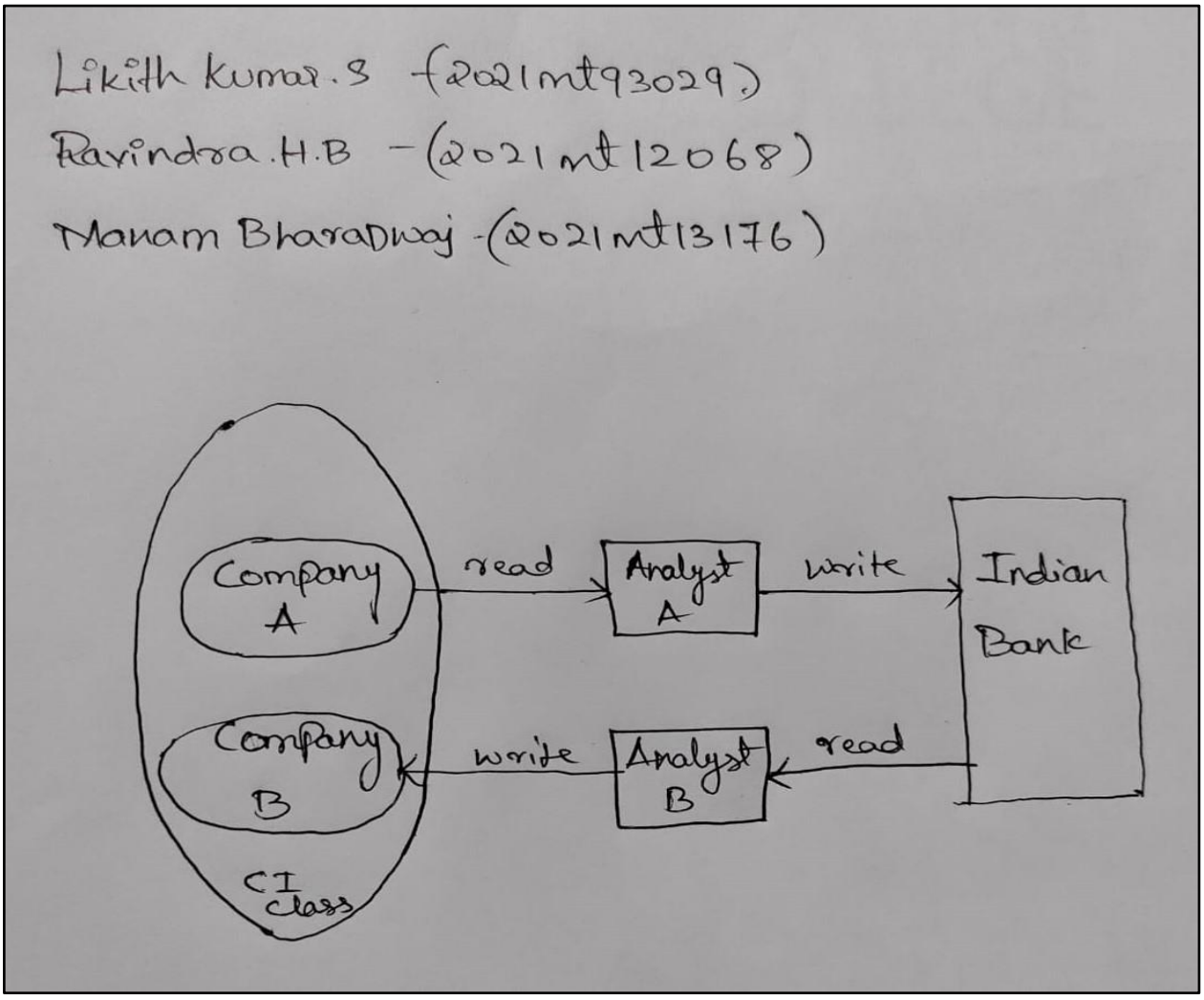
1. A subject which is given at a security level cannot read an object at the higher level of security.
2. A subject which is given at a security level cannot write to an object at a lower level of the security.

**Chinese Wall Model**: - The **Chinese Wall model** is also a safety model that focuses on confidentiality and will find the application in the commercial world. This model was developed by Brewer and Nash.

This model is used in the area of computer science and this **Chinese wall model** is used by the operating system for computer security and the US judicial system for protection against copyright infringement.

The computer security is a concern that the software is stable or not of the operating system. The same technique is there in an important business matter concerning the licensing of each of a computer's many software and hardware components.

Now to construct and show the system implementing **Chinese wall model** has been explained below:-




**NOTE :( we are considering a banking system to implement this model)**

To construct or to develop a system by implementing the **Chinese Wall model** and by using **Bell-LaPadula model**, I use a security category or a safety category to each **'(COI, CD)'** pair. There are 2 security or safety levels, **'S (for sanitized)' and 'U (for unsanitized)'.**

We assume that **'S dom U'** will demonstrate the mapping of the system for each data which is transferred as 2 objects and 1 sanitized and other 1 is unsanitized.

The data in the **Chinese Wall Model,** is assigned to clear the components such that they do not have multiple types of categories corresponding to the **"CD's"** which are in the same class of the **'coi'**.

Now let's try to implement an example for this model,

**Likith** will be able to read the **Indian bank "ARCO and CD's",** his purpose of idea would be to have clear for the **'(U, {a, n})'** compartment. There can be 3 possible ways to clear the bank **'coi'** class and 4 possible ways to clear the gasoline **'coi'** class company.

The combination is to give 12 possible ways of clearance for the proposed subjects. The subjects can read all the sanitized data. The **'cw-simple'** security data condition will be clearly holds the **'cw-*-property'** and also will hold the data because the **Bell-LaPadula model '*-propertyensures'** can be the category and the input of objects is also a subset of the category and the output of the objects.

The input objects can be sanitized and in the same category to that subject. This development will show that at any time the **Bell-LaPadula model** can also find the state of a system by using the **Chinese Wall model.**

**Summary:**

Security is the main thing in any system, so to construct a system we can implement the Chinese Wall model which has the similar characteristics of the Bell-LaPadula Model and adds on the constraint of conflict of interest of subjects.

**References:**


1. Recorded lecture
2. Lecture Slides
3. Textbook: T1- William Stallings & Lawrie Brown, **Computer Security: Principles and Practice**, 4th Edition, Pearson, 2018
4. Textbook: T2- Matt Bishop, **Computer Security**, 2nd Edition, Pearson, 2019


---

## Question 2: Show that the Clinical Information System model's principles implement the Clark-Wilson enforcement and certification rules.

**Solution:**

Any information system will have to have three major characteristics as far as security is concerned, i.e *Confidentiality*, *Integrity* and *Availability*. These are the paramount characteristics to be considered in most of the industries where security is the foremost element they need for the environment.

The elements used in **Clinical information systems should ensure the integrity of the data** is always being protected from the illegal accesses and corruption due to any software or hardware malfunction.

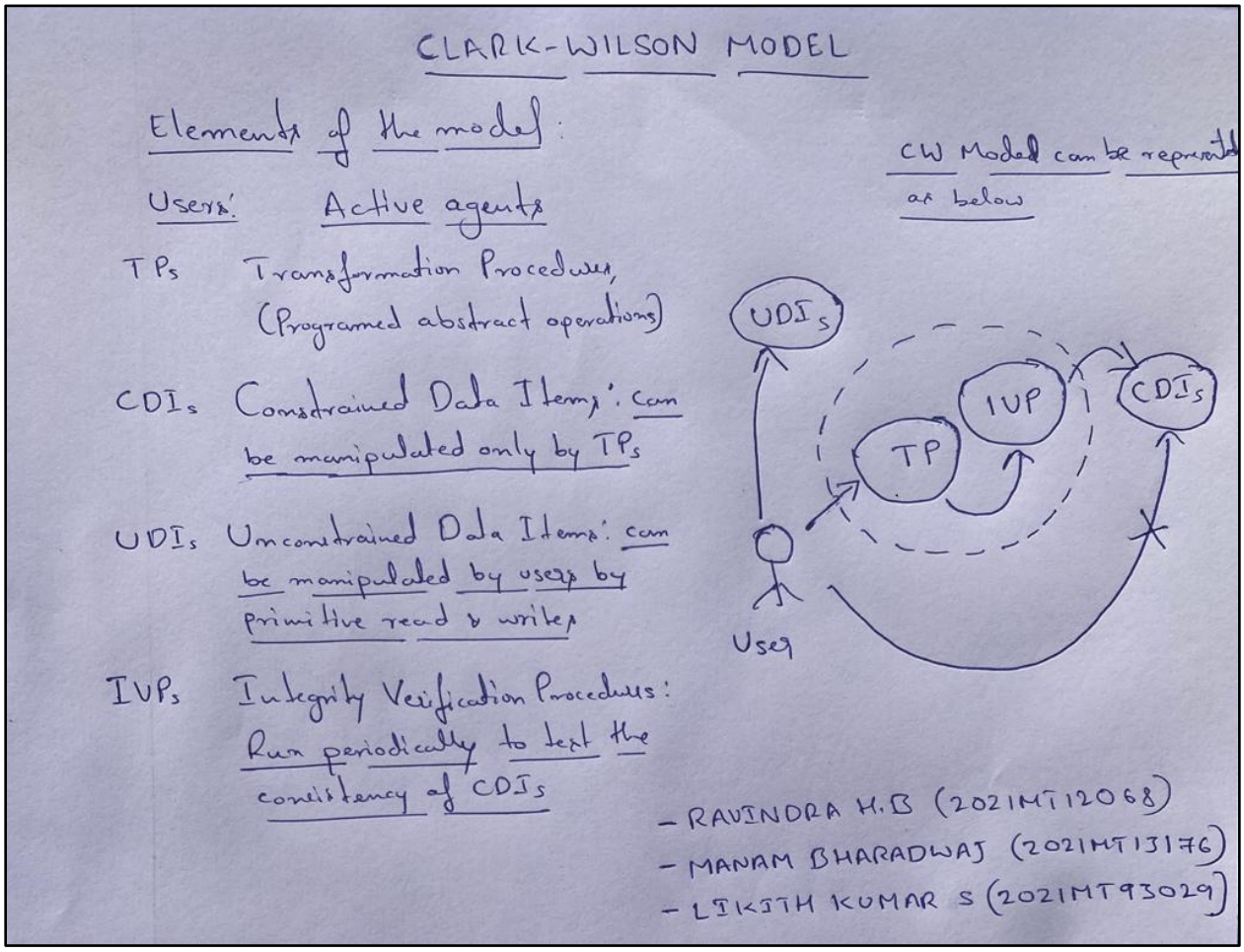
**Clark-Wilson Model**: **Clark-Wilson model focuses on Integrity of the system**. **Data Integrity of the system is defined as the correctness and authenticity of the information stored** in an information system. Integrity ensures the data that a system is processing is always correct.

The objective of an information system is to control or manage the access of subjects (users) to objects (data). This control will be governed by a set of rules.

The various goals of integrity include the following:

- **To prevent unauthorized accesses**
- **To maintain the data correctness**
- **To prevent authorized but illegal modification**

The Clark-Wilson (CW) model is an integrity, application-level model which attempts to ensure the integrity properties of commercial data and provides a framework for evaluating security in commercial applications like clinical systems.




**Certification Rules:**

1. C1 **(IVP Certification**)- The system will have an Integrity verification procedure (IVP) for validating the integrity of any Constrained data items(CDI)
2. C2 (**Validity**) - The application of a Transformation procedure (TP) to any CDI must maintain the integrity of that CDI. CDIs must be certified to ensure that they result in a valid CDI
3. C3 - A CDI should only be changed by a TP. TPs must be certified to ensure they implement the principles of separation of duties & least privilege
4. C4 (**Journal Certification**)- TPs must be certified to ensure that their actions are logged
5. C5 - TPs which act on Unconstrained data items (UDIs )must be certified to ensure that they result in a valid CDI

**Enforcement Rules:**

1. E1 (**Enforcement of Validity**)- Only certified TPs can operate on CDIs
2. E2 (**Enforcement of Separation of Duty**)- Users must only access CDIs through TPs for which they are authorized
3. E3 (**User Identity**)- The system must authenticate the identity of each user attempting to execute a TP
4. E4 (**Initiation**)- Only administrator can specify TP authorizations The CW model differs from the other models that allow subjects to gain access to objects directly, rather than through programs

**Summary:**

Integrity is an important characteristic in the Clinical Information System model. CW models implement specific mechanisms that can be followed to achieve the security model.
The Clark-Wilson model emphasizes how integrity is a key element to achieve the better security system in a Clinical Information System Model.

**References:**


1. Recorded lecture
2. "Introduction to COMPUTER SECURITY" by Matt Bishop
3. https://www.researchgate.net/figure/Application-of-the-Clark-Wilson-integrity-model-to-preserve-the-integrity-of-metadata_fig3_355644640


---

## Question 3: A physician who is addicted to a pain killing medicine can prescribe the medication for herself. Please show how RBAC (Role-Based Access Control) in general, and the Definition specifically can be used to govern the dispensing of prescription drugs to prevent a physician from prescribing medicine for herself

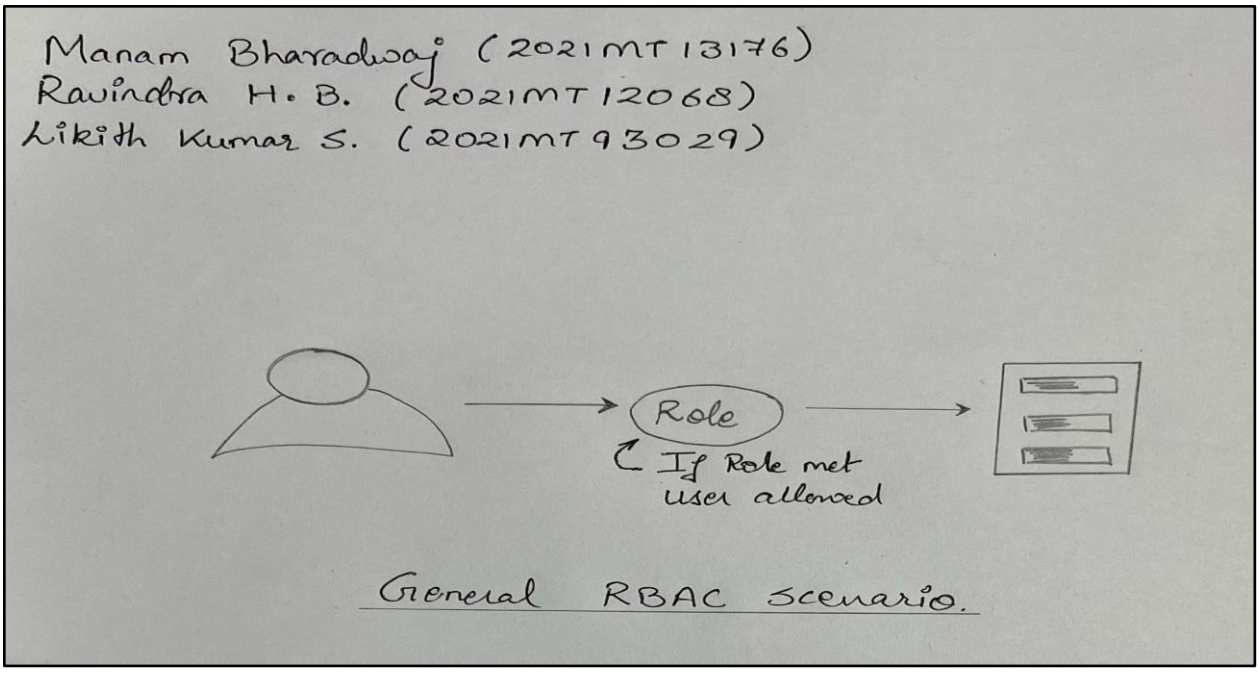
**Solution**:

**What is RBAC?**

Role-based access control (RBAC) is a **security approach** that authorizes and restricts system access to users **based on their role(s)** within an organization.

This allows users to access the data and applications needed to fulfill their job requirements and minimizes the risk of unauthorized employees accessing sensitive information or performing unauthorized tasks.

In addition to restricting access, RBAC can refine the **way a user interacts with data—permitting read-only or read/write access to certain role**s, thus limiting a user's ability to execute commands or delete information.




There are three types of access control under the RBAC standard: core, hierarchical, and constrained.

## Core RBAC

According to ANSI RBAC INCITS 359 the core model outlines the essential elements of every role-based access control system. RBAC must adhere to the following three rules:

- Role assignment
- Role authorization
- Permission authorization

## Hierarchical RBAC

A role hierarchy is a way to structure roles to reflect a complex organizational structure and enable sharing and inheritance of permissions between roles. A simple example of hierarchical RBAC is a series of roles, in which each role inherits the permissions of the previous one, and adds more permissions

## Constrained RBAC

This third RBAC standard adds separation of duties to the core model. Separation of duty relations fall under two headings: static and dynamic.

- Under **Static Separation of Duty (SSD) relations**, a single user cannot hold **mutually-exclusive roles** (as defined by the organization). This ensures, for example, that **one individual cannot both make and approve a purchase**.
- In the Dynamic Separation of Duty (DSD) model, a user *can* be a member of conflicting roles. However, the user may not function in both roles during a single session. This constraint helps control internal security threats by, for example, enforcing the two-person rule in which two distinct users are required to authorize an action.

In our case: The main concern is to **prevent a physician from prescribing medicine for herself.**

- Leads to Fundamental Design Principle for Separation of Privileges where a system cannot simply grant the **permissions to the subject/user based on just a condition to be met**. The Privileges are further divided to provide a holistic view of Defense-in-Depth condition.

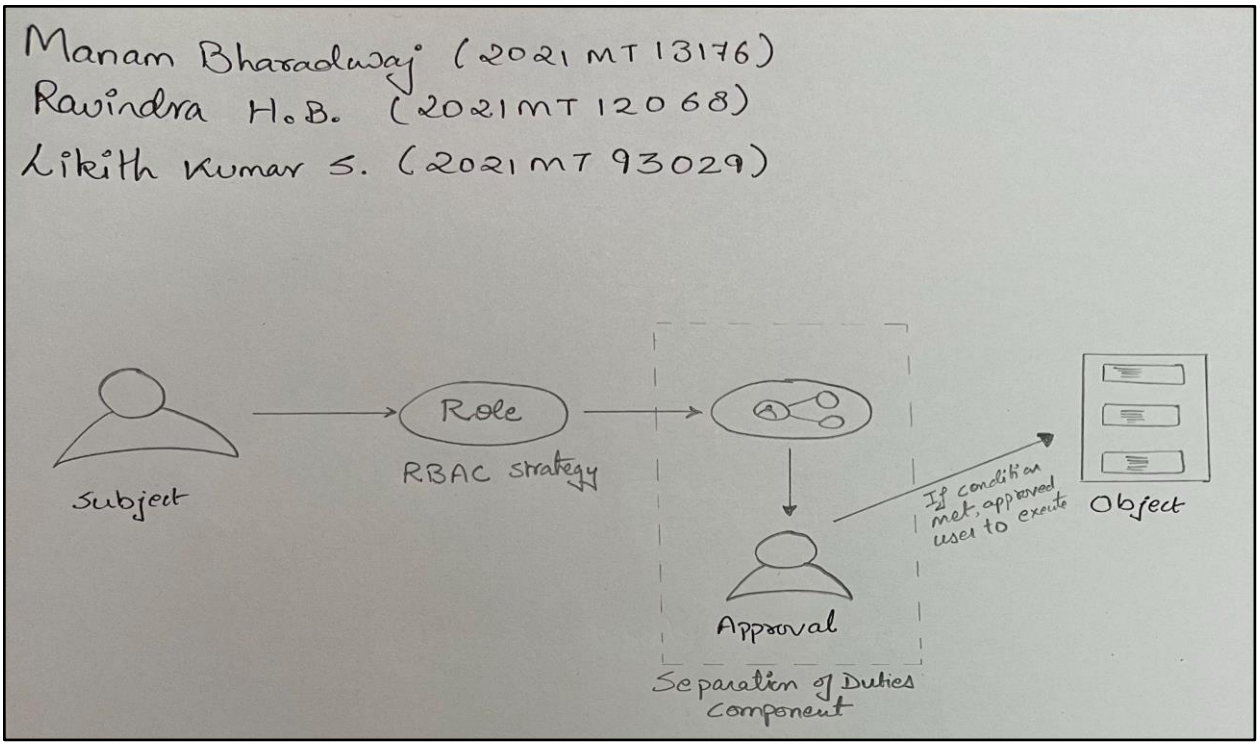
Role-based access control or RBAC is mandatory access control. Under RBAC, a transaction cannot be executed by a subject when its current role is not designated for it.

- A role is a collection of job functions. Each **role r** is authorized to perform one or more transactions (actions in support of a job function). The "set of authorized transactions" for r is written **trans(r)**.
- The active role of a subject s, written **actr(s)**, is the role that **s** is currently performing.
- The authorized roles of a subject s, written **authr(s)**, is the set of roles that s is authorized to assume.
- Let S be the set of subjects. Then the rule of role authorization is $(\forall s \in S)[\ actr(s) \subseteq authr(s)\ ]$
  This rule means that the subject must be authorized to assume its active role. It cannot assume an unauthorized role
- RBAC can model the separation of duty rule. The key is to recognize that the users in some roles cannot enter other roles. That is, for two roles r1 and r2 bound by separation of duty (so the same individual cannot assume both roles) $(\forall s \in S)\ [\ r1 \in authr(s) \rightarrow r2 \notin authr(s)\ ]$
- ***Capturing the notion of mutual exclusion requires a new predicate.***
  Let **r** be a **role**, and let **s** be a **subject** such that $\mathbf{r \in authr(s)}$. Then the predicate **meauth(r)** (for mutually exclusive authorizations) is the set of roles that s cannot assume because of the separation of duty requirement.
  The principle of separation of duty can be summarized as
  $\mathbf{(\forall r1, r2 \in R)\ [\ r2 \in meauth(r1) \rightarrow [\ (\forall s \in S)\ [\ r1 \in authr(s) \rightarrow r2 \notin authr(s)\ ]\ ]\ ]}$

According to the textbook in the RBAC model users who have some specific roles can't have other roles based on the separation of duty.

If r1 and r2 are bound by separation of duty it means that for mutually exclusive authorizations these two can't be in the same subject set of aurth(s). Therefore, the person in a role of prescribing a medicine 'can't have a second role of distributing it'.

It takes two different people for this process, which prevents one person from prescribing and distributing medicine for herself at the same time.




Role Based Access Control is a type of access control that gives permissions based on user's role, or position. So in a hospital.

- We can imagine three different positions from lowest to highest, Hospital Staff, Physician, Manager.
- This **disallows a role from initiating and approving the same process**. Such As our physician in the example prescribing pain killer medicines. The Separation of Duty requirement would allow her to write prescriptions to other people of the same level, but not to herself.
- Or if she could write a prescription to herself, but would **have to seek another person of the same role or higher to approve of the prescription.**

**Summary:**

Those systems that have existed and will come in near future support the **mutual exclusion** of roles that affect SOD policies. However the mutual exclusive rule is supplied more than one way and design will distress ease of use considerably.

**References:**

1. Recorded Lecture
2. https://ieeexplore.ieee.org/document/4299762 -Separation of Duty in Role-Based Access Control Model through Fuzzy Relations
3. https://www.strongdm.com/rbac
4. Text Book: Introduction to Computer Security - Matt Bishop
5. https://www.academia.edu/21928731/Permission_based_implementation_of_Dynamic_Separation_of_Duty_DSD_in_Role_based_Access_Control_RBAC_