Software Requirement Specification

for

'Online Police Verification System'

Prepared by

Abdullah Al Rafi ASH2025030M

Jannatun Nur Etu BFH2025009F

Mithun Chandra Sarkar MUH2025029M

Rubya Rashed MUH2025014M

Institute of Information Technology

Noakhali Science and Technology University

07.06.2023

Table of Contents

1.List of Tables

2. List of Figures

1. Introduction

The Online Police Verification System is a software solution designed to streamline and automate the process of verifying the background and credentials of individuals, newly appointed or currently employed for government or private jobs. This system aims to replace the traditional manual verification process, which is time-consuming, error-prone, and often leads to delays in the appointment of individuals to government positions. By providing an efficient and secure online platform, the system facilitates collaboration between the Special Branch of Police, various government and private institutions, and the newly appointed individuals or currently employed employees.

1.1 Problem statement

The police verification process is an essential aspect of ensuring the safety and security of individuals and society as a whole. It is usually required during various applications such as passport issuance, employment background checks, job promotional purpose etc. Currently, this process is done manually, the applicant has to fill up a form and submit it to relevant authority (may be any govt. Office, organization, ministry etc.). The form is sent to the SB office then DSB office and a police officer is assigned to verify the applicant and the officer has to manually find out the individual and make one to one contact which can be time-consuming, error-prone, and inefficient. Then the process is rolled back.
The verification for passport issuance is already done online. The information that one gives while making an e-passport is sent for police verification automatically. No one has to do any additional or manual work for this. So, it reduces the extra headache.
The system will be designed to gather information from applicants, including their personal information, employment details, residential address, etc. This information will be verified by the police authorities to ensure its authenticity.
Online verification system will fasten the process of verification and the applicant will receive a message that which police officer will verify his/her information and the police officer also will know the details of the applicant and they could make one to one communication. Overall, the verification system will reduce the headache of any individuals, costs and time.

1.2 Purpose

The purpose of this Software Requirement Specification (SRS) document is to provide a comprehensive description of the requirements and functionality of the Online Police Verification System. It serves as a guide for the development team, stakeholders, and other relevant parties involved in the project. The SRS outlines the system's features, interfaces, constraints, and performance requirements, ensuring a common understanding of the project's scope and objectives.

1.3 Project Scope

The Online Police Verification System is intended to cover the entire process of verifying the background and credentials of individuals who are newly appointed for government jobs. The system will facilitate the exchange of information and documents between the Special Branch of Police, various government or private institutions and the individual undergoing verification. It will provide a secure and user-friendly online interface for submitting, processing, and tracking verification requests, ensuring efficient communication and reducing the overall time and effort required for the verification process.

1.4 Glossary

This subsection contains definitions of all the terms, acronyms, and abbreviations used in the document. Terms and concepts from the application domain are defined.

- SRS - Software Requirement specification
- UI - User Interface
- OPVS – Online Police Verification System

1.5 References

IEEE. IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.

1.6 Overview

An online police verification system is a digital platform that enables individuals and organizations to request and conduct background checks and verifications through law enforcement agencies. It streamlines the process of verifying the credentials and criminal records of individuals by leveraging online technologies and databases. Here's an overview of how an online police verification system typically works:

1. User Registration: Individuals or organizations seeking verification services usually need to register on the platform by providing their personal or institution details.

2. Verification Request: After registration, users can submit a request for a background check on a particular individual. They may need to provide relevant information about the person, such as name, address, identification details, etc.

3. Data Submission: The system collects the submitted data and sends it to the appropriate law enforcement agency responsible for conducting the verification.

4. Verification Report: Once the agency completes the search and analysis, they generate a verification report. The report typically includes details about the individual's criminal history, if any, along with any other relevant findings.

5. Report Delivery: The verification report is then sent back to the requesting user through the online platform. Depending on the system, the report may be available for download.

6. Result Interpretation: The institution reviews the verification report to assess the individual's background. Based on the findings, they can make informed decisions about employment, tenancy, or any other relevant context.

2. Stakeholders and Characteristics

2.1 Individual User/requestor

These are individuals that initiate the verification process by submitting a request for a background check. They provide the necessary information and have a vested interest in obtaining accurate and reliable verification reports.

2.2 Institutions (Government or Non-Government)

These are the organizations that want to verify the information of newly recruited employees or to verify the information of those who are going to be promoted in important positions. They collect the initial information from the individuals and give to the authorities (SB or DSB) to verify the information.

2.3 SB (Special Branch of Police)

Responsible for collecting the request of verification and send it to the DSB or their child branch in the district level. They just work as a coordinating body.

2.4 DSB (District Special Branch of Police)

These agencies are responsible for conducting the background checks and verifications requested by the users or institutions. They have access to criminal databases and other relevant sources of

information to generate the verification reports. The characteristics of law enforcement agencies can include:

- Expertise in law enforcement and data analysis.
- Compliance with privacy laws and regulations.
- Timeliness and accuracy in conducting verifications.
- Collaboration with other agencies like local police or NSI or DGFI to access necessary data sources.
- Maintaining the security and integrity of the verification process.

2.5 DSB officer/Local police station officer

The original verification process (background check, criminal record check, one to one communication with the applicant or the responsible person etc.) is done by them. In some cases, DSB officers are assigned to do the job and, in some cases, local police station's officers are responsible for doing the job done.

2.6 IT Administrators and Developers:

These individuals or teams are responsible for the technical implementation, maintenance, and security of the online police verification system. Their characteristics may include:

- Technical expertise in software development, database management, and system administration.
- Ensuring system availability, reliability, and performance.
- Implementing appropriate security measures to protect user data.
- Regular system updates and maintenance to address vulnerabilities.
- Collaborating with stakeholders to incorporate feedback and improve system functionality.

Here we, four students of IIT, NSTU 3rd batch along with our supervisor is the IT administrators and developers.

3. Design and implementation constraints

Design and implementation constraints are those that we have used to implement the project and make the project successful. It also describes the tools that enables developers and testers to view and interact with the user interface (UI) elements of this application.

3.1 Language

User interface design (UI Design) is the visual organization of the parts of a website or technological product that a user could interact with. In other words, it is the visual layout of a website and application. On the other hand, the code that enables a computer program or application to run and cannot be viewed by a user is referred to as the back end. The back end of a computer system is where the majority of data and operating syntax are kept and accessed. Typically, one or more programming languages are used for a successful project.

Front-end development

3.1.1 HTML

HTML (Hypertext Markup Language) is used to structure a web page and its content. Precisely, the coding that organizes a web page's content is called HTML (Hypertext Markup Language). With the help of HTML, you can tell a web page whether it should be recognized as a paragraph, list, heading, link, image, multimedia player, form, or any other of the many other components that are now supported, or even a new element that you design. It is the programming language for formatting web pages that is widely accepted. Small and medium-sized businesses are the main users, as they do not actually require extensive functionality on their websites. The option to utilize HTML to design the structure of our web pages was made since it is free, works with all browsers on the client's machine, and is simple to use and understand.

3.1.2 CSS

CSS (Cascading Style Sheets), a style sheet language used for describing the look and formatting of a document written in HTML. It's used to separate the presentation of a web page from its content, making it easier to change the style of a large website without having to make changes to its HTML.

3.1.3 Bootstrap (Front-end framework)

Bootstrap is a free and open-source front-end web framework for designing websites and web applications. It includes optional JavaScript extensions along with HTML and CSS-based design templates for navigation, buttons, forms, and other interface elements. It only addresses front-end development, unlike many web frameworks. Along with CSS, Bootstrap would be utilized to create the application's styling. Bootstrap is important in the application for the following reasons: Easy to use: Anyone can begin using Bootstrap with just a basic Knowledge of HTML and CSS. Responsive features: The responsive CSS in Bootstrap adapts to mobile devices, tablets, and desktops. Mobile-first approach: The fundamental Bootstrap framework provides mobile-first styling. Browser compatibility: All current browsers are compatible with Bootstrap (Chrome, Firefox, Internet Explorer, Safari, and Opera).

3.1.4 JavaScript

JavaScript is a text-based programming language used both on the client-side and server-side that allows you to make web pages interactive. JavaScript adds interactive elements to online pages that keep users engaged, whereas HTML and CSS are languages that give web pages' structure and style. The prototype is a built-in property that every JavaScript object has. The prototype is itself an object, so the prototype will have its own prototype, making what's called a prototype chain. When we get to a prototype that contains null for its own prototype, the chain comes to an end.

(Back-end development)

3.1.5 Node.js

Node.js is a JavaScript runtime that allows to run JavaScript code on the server-side. We can use Node.js with Express.js to build the server logic of your application, handle incoming requests, and interact with the MongoDB database.

3.1.6 MERN stack

MERN Stack is a collection of technologies that enables faster application development. It is used by developers worldwide. The main purpose of using MERN stack is to develop apps using JavaScript only. This is because the four technologies that make up the technology stack are all JS-based. Thus, if one knows JavaScript (and JSON), the backend, frontend, and database can be operated easily.

(Database)

3.1.7 MongoDB

MongoDB is an open source NoSQL database management program. NoSQL (Not only SQL) is used as an alternative to traditional relational databases. NoSQL databases are quite useful for working with large sets of distributed data. MongoDB is a tool that can manage document-oriented information, store or retrieve information.

3.1.8 Express

Express is a minimal and flexible Node.js web application framework that provides a robust set of features for web and mobile applications**.**

3.2 Server-Side Technology

When an application is used, server-side development refers to the processes that happen in the background. Databases, scripting, website architecture, backend logic, APIs, and servers are the main topics covered.

3.2.1 Database Server

MySQL is an open-source relational database management system (RDBMS). A relational database arranges data into one or more tables where it is possible for the data to be connected to one another. Programmers use the SQL language to create, change, and extract data from relational databases and to manage user access to the databases.

4. Requirement specification

4.1 Functional Requirement

Functional requirements are those that serve as examples for the system's internal operation, its description, and an explanation of each subsystem. It comprises the task that the system should complete, the associated processes, the data that the system should store, and the user interfaces.

4.1.1 User registration and login

Table 1 FR-1

FR-1	Individual user or requestor or institution or DSB/police officers registration and login		
Description	Individual user or requestor or institution or DSB/police officers should create an account for the first time. Once a user completes registration then he/she will be able to login to the account.		
Stakeholders	Individual user or requestor or institution or DSB/police officers.	**Priority**	High

4.1.2 Status tracking

Table 2 FR-2

FR-2	Status tracking		
Description	The requestor should be able to see the status of his/her verification process. It might be pending/undergoing/completed.		
Stakeholders	Individual requestor, Institutions	**Priority**	High

4.1.3 Document Upload

Table 3 FR-3

FR-3	The requestor (could be individual or institution) have to upload the necessary document.		
Description	The system should provide a feature for users to upload relevant documents, such as identification cards, address proofs, or employment letters, signature of institution head etc. to support the verification process.		
Stakeholders	Individual user, Institution	**Priority**	High

4.1.4 Help desk

Table 4 FR-4

FR-4	The user finds a help desk.		
Description	The user should see a help desk, a support center that assists users with any issues, questions, or concerns they may have regarding the verification process. It serves as a primary point of contact for users who need assistance or information related to the online police verification system.		
Stakeholders	Individual requestor	**Priority**	Low

4.1.5 Institution basis form submission

Table 5 FR-5

FR-5	The user should be able to fill the covetable institutions form		
Description	The user should be able to select the desired institution for which he/she wants to initiate the verification process and after selecting the institution the prescribed form of that institution would be available and user should be able to submit required information and document in the form. The institutions also should be able to submit their information for their purpose (promotion or recruitment purpose). The institutions should be able to find their suggested form.		
Stakeholders	Individual requestor, institution	**Priority**	Medium

4.1.6 Purpose selection

Table 6 FR-6

FR-6	The user should be able to select the purpose of their verification		
Description	As the verification process vary from case to case. DSB handles verification process on the basis of verification type. So, the user should be able to select the purpose of the verification so that it becomes easier and clear for making decision to DSB or SB.		
Stakeholders	Individual requestor, institution	**Priority**	High

4.1.7 Assigning officer

Table 7 FR-7

FR-7	The in-charge of DSB should be able to assign officer for verification.		
Description	The in-charge of DSB or higher authorities should be able to assign the DSB officer or in some cases local police station officer to perform the verification.		
Stakeholders	DSB, SB	**Priority**	High

4.1.8 View available officer list

Table 8 FR-8

FR-8	The in-charge of DSB should be able to see available the officer list.		
Description	The DSB in-charge or operator of the system should be able to see the available police/DSB officer to whom the verification case could be handed over.		
Stakeholders	DSB	**Priority**	Medium

4.1.9 Notifying Users

Table 9 FR-9

FR-9	The system sends notifications to the users.		
Description	In two cases the system should send notification to users. First, if the verification is completed then the system should send the notification of verification result to the institutions. Secondly, the system should send the notification to the officer who is assigned for any verification case.		
Stakeholders	Institution, DSB/police officer	**Priority**	High

4.1.10 See overall verification cases

Table 10 FR-10

FR-10	The user should be able to see the total cases of verification.		
Description	From DSB module of the system, the user should be able to see the total number of verification cases, pending cases, new requests for verification or undergoing cases in a table. New request bar should be red when new request will arrive.		
Stakeholders	SB, DSB	**Priority**	High

4.1.11 Approval or rejection option

Table 11 FR-11

FR-11	The user should be able approve or reject the request.		
Description	The in-charge of DSB or SB should be able to approve or reject the applications based on the documents provided. They should be able to add comments or notes to justify their decisions		
Stakeholders	SB, DSB	**Priority**	High

4.2 Data Requirement

The Data Requirements section provides information on the data used by the software application/system. This is limited to creating tables and referencing existing tables relative to the storage of data.

4.2.1 User Information

Table 12 DR-1

DR-1	The user provides information
Description	1. Personal Information: ○ Full name ○ Date of birth ○ Gender ○ Nationality ○ Current address ○ Permanent address ○ Contact information (phone number, email)

	2. Identification Documents: o Government-issued ID card (e.g., passport, driver's license, national ID) o Proof of address (e.g., utility bill, bank statement) 3. Criminal History: o Any previous criminal records or convictions o Details of the offense(s), if applicable o Court case numbers, if applicable 4. Employment History: o Current and previous employers o Job titles and durations of employment o Contact information of employers for verification purposes 5. Educational Background: o Schools attended o Degrees obtained		
Stakeholders	Individual requestor, Local police station, Institutions	**Priority**	High

4.2.1 DSB/ Available police officer list

Table 13 DR-2

DR-2	The DSB and police authority provides the available police officers list.		
Description	The DSB and police authority provides the available police officers name, designation, posting etc.		
Stakeholders	SB, DSB	**Priority**	High

4.3 Performance Requirement

It is important to maintain the performance of the system. To ensure the best performance of the system we must maintain the following steps:

4.3.1 Speed and Latency Requirements

Table 14 PR-1

PR-1	Faster Response Time		
Description	The system should provide prompt responses to user requests, such as account creation, document submission, and verification checks. The response time should be within acceptable limits to ensure a smooth user experience.		
Stakeholders	Developer	**Priority**	High

4.4 Maintainability Requirements

The term "maintenance" describes how simple it is to fix, enhance, and comprehend software code. After the user has received the product, the software maintenance phase of the software development cycle begins.

4.4.1 Maintenance Requirements

Table 15 MR-1

MR-1	Develop maintainable code

Description	Maintainability must be ensured so that it can be modified later and will be readable.		
Stakeholders	Developers	**Priority**	Low

4.4.2 Supportability Requirements

This system satisfies the supportability requirements for testability, maintainability, compatibility, configurability, serviceability, and install ability.

4.5 Security requirements

Information security is far more crucial for a system to gain user's trust. Here are some security requirements are given below:

4.5.1 Access Requirements

The system will apply some authorization approaches when granting access to information to make sure the right user is using the right data.

4.5.2 Integrity Requirements

Integrity requirements relate to a security system that ensures an expectation of data quality. It also ensures that no data on the system will ever be exposed to malicious modification or accidental deletion.

4.6 Usability and Human Integrity Requirements

Usability in software engineering refers to how well a piece of software may be used by a specific target audience to accomplish goals. A user-friendly environment will be provided by the system.

4.6.1 Ease of Use Requirements

Our system will be easier to use by any type of stakeholder and they don't need any training to use the system.

4.6.2 Accessibility Requirements

The system provides authorization / authentication to get access to it. Numerous modules are used in this system.

Table 16 SR-1

SR-1	Safeguards are provided by the system.		
Description	The system is designed in a way that allows all modules to access a mechanism that provides security services.		
Stakeholders	Developers	**Priority**	High

4.7 Look and Feel Requirements

Look and feel requirements mainly refer to how the system will appear. The "look" of a graphical user interface in software design refers to elements like colors, shapes, layouts, and typefaces. It also refers to the behavior of dynamic elements like buttons, boxes, and menus (“The Feel”).

4.7.1 Appearance Requirements

Table 17 AR-1

AR-1	Text color and font

Description	Our system has to be different and attractive from another existing library using a better look and feel.		
Stakeholders	Developers	**Priority**	Medium

4.8 Style Requirements

There are no style requirements in our system.

4.9 Legal Requirements

Legal requirements often refer to an organization's terms and conditions or privacy policy. No third-party software or individual is permitted to use our data for commercial purposes, according to the terms and conditions of our application.

5. Requirement Engineering Process

Software requirements are established using requirements engineering (RE), which considers customer wants or requirements. Requirements elicitation, needs modeling, requirements analysis, requirements assurance & validation, and requirements management are all parts of the requirements engineering process.

5.1 Requirement Elicitation Techniques

Requirements elicitation, often known as "requirement gathering," is the process of investigating and discovering system requirements for users, clients, and other stakeholders. Contacting participants directly or conducting research, analysis, and testing are two ways to elicit requirements.

5.1.1 Hold Interviews

.

Sample of requirement collection

Requirement collection -1

This report summarizes the results of the stakeholder interviews conducted to gather requirements for the online police verification system. The objective of the interviews was to identify the key needs and expectations of the stakeholders and to use this information to develop a comprehensive set of requirements for the system.

Methodology

The interviews were conducted with stakeholders from various departments and roles, including officers of district special branch of police, newly recruited government employee. The interviews were conducted in a one-to-one and one-to-many format, lasting approximately 1-2 hours per session.

Participants

- OC, DSB, Noakhali
- Some officers of DSB, Noakhali
- Some newly recruited government employee

Findings

The following are the key findings from the interviews:

1. User-Friendly Interface:
    - The system should have a user-friendly interface that is easy to navigate and understand.
    - Users should be able to easily access and interact with different features and functionalities of the system.
2. Status Tracking:
    - Users should be able to track the progress and current status of their requests or tasks within the system.
3. Help Desk:

- The system should include a help desk or support feature to assist users in case they encounter any issues or require guidance.
- Users should have access to a help desk for submitting queries or seeking assistance related to the system.

4. Institution Basis Document Submission:
    - The system should support the submission of documents on an institution basis.
    - Users should be able to submit required documents specific to their institution or organization.
5. Purpose Selection:
    - The system should allow users to select the purpose for their request or task.
    - Users should be able to choose from predefined purposes that align with their needs or objectives.
6. User Authentication by Phone OTP:
    - The system should authenticate users using a phone-based one-time password (OTP) mechanism.
    - Users should receive an OTP on their registered phone number for authentication during the login or account access process.
7. Authenticate Request:
    - The system should authenticate and validate each request or task submitted by users.
    - Requests should be verified for authenticity and correctness before further processing.
8. Assign Police/DSB Officers:
    - The system should facilitate the assignment of police or DSB officers to specific requests or tasks.
    - Officers should be assigned based on their availability, jurisdiction, or other relevant criteria.
9. Approval/Rejection Option:
    - The system should provide the option for approving or rejecting requests or tasks.
    - Authorized personnel should be able to review and either approve or reject submitted requests within the system.
10. Auto Fill of Higher Authority Signature:

- The system should automatically populate the signature or approval of higher authorities for certain requests or tasks.
- Once approved, the system should automatically fill in the signature or approval of higher authorities without manual intervention.

11. Integration with Other Systems:
    - The system should support integration with other relevant systems or databases.
    - Integration should enable seamless data exchange, synchronization, or interoperability between the system and external systems.
12. Reporting and Analytics:
    - The system should have reporting and analytics capabilities to generate relevant reports and gather insights.
    - Users should be able to generate reports based on different parameters or criteria and access analytical data related to system activities.
13. Security and Scalability:
    - The system should ensure robust security measures to protect user data and maintain confidentiality.
    - The system should be scalable to accommodate an increasing user base and growing book collection without compromising performance or stability.

Key Requirements

Based on the findings from the interviews, the following are the key requirements for the book sharing system:

1. Individual user/institution/DSB, police officer should be able to register, log in and log out from the system.
2. The user should be able to track the current status of verification process.
3. The system should provide a help desk to the users to understand the procedure of doing things.
4. The user should be able to submit their documents and information on the institution basis and should be able to submit their purpose.
5. The system admin should be able to authenticate the request coming from various sources.
6. The system admin or in-charge of DSB should be able to assign any police or DSB officer to perform the verification.
7. The system should notify its user after completion of any verification or in assignment of any officer.

8. The system should allow the admin to approve or reject any request. It also should allow to decline any request.
9. The system should generate a verification report based on the outcome of the background check. The report can include details such as verification status, remarks, and recommendations.
10. The system should provide reporting and analytics features to generate insights and track the performance of the verification process.

Assumptions

It was assumed during the interview process that the online police verification system will be accessible via the web and we must develop an android app further for the system.

Limitations

1. Authentication Challenges: Ensuring the authenticity and accuracy of user information and documents can be challenging in an online environment. There is a risk of fraudulent submissions or impersonation, which can undermine the effectiveness of the verification process.
2. Data Security Risks: Online systems are vulnerable to cybersecurity threats, such as data breaches and hacking attempts. Sensitive personal information and verification documents are at risk of being compromised if the system does not have robust security measures in place.
3. Reliance on Existing Databases: The accuracy and effectiveness of the online verification system depend on the quality and reliability of the existing databases it integrates with. If the data in those databases is outdated or incomplete, it can lead to inaccurate verification outcomes.
4. Technical Challenges: Technical glitches or system downtime can disrupt the verification process and cause delays for users. Maintenance and updates to the system may also require temporary suspension of services, affecting the overall efficiency and user experience.
5. Legal and Regulatory Considerations: Implementing an online police verification system may require compliance with various legal and regulatory frameworks. These include data protection laws, privacy regulations, and adherence to specific standards, which can introduce complexities and delays in the implementation process.
6. Resistance to Change: Introducing an online system may face resistance from individuals who are accustomed to traditional verification processes. Some may be reluctant to trust the security and reliability of online systems, which can result in a slower adoption rate.

Conclusion

The stakeholder interviews provided valuable insights into the requirements for the online police verification system. The key findings and requirements will be used to develop a comprehensive set of requirements for the system.

Sample of requirement collection
Requirement collection 2

5.1.2 Field observation

Field observations may indicate that an online police verification system improves the overall efficiency of the verification process. Online submission and document upload can save time and resources compared to manual paperwork. This may result in faster processing times and reduced administrative burden for both users and verification authorities.

Methodology:

The field observation was conducted by observing the process of police verification in several cases. We went to DSB office, Noakhali and saw how verification process is done manually. In this case some officers helped use and explained us the procedure.

Participants:

1. DSB officer
2. OC, DSB

Findings:

The following are the key findings from the field observation:

1. We have seen that various requests of verification come to DSB from various sources as file and handed over to DSB.
2. Some officials organized the files and the in-charge then assign officers to perform the verification.

3. The files are sent to officers' hand to hand.
4. A register book is maintained to keep track of the verifications.
5. Receiving and sending dates are recorded.
6. The result of the verification is accepted by DSB from officers and again sent to the adhering institutions.

Problems in the system:

1. The process is done manually and a time-consuming process
2. The cost of verification process is high because of transportation cost.
3. Everything is done manually so there is a risk of error.
4. The user doesn't know the current status of the verification so there could be an availability issue.

5.2 Requirement Validation

Requirement validation criteria make sure they are accurate and match the standard you desire from this program. Our requirements initially appeared to be good, but after reading them and attempting to implement them, we discovered that they contained gaps and ambiguities.

5.2.1 Review the Requirements

Among the techniques that produce the highest quality software now accessible, negative peer review, particularly the rigorous type known as evaluation, is exceptional. We carefully looked at documented needs, analysis models, and related disability information with a team of reviewers from various viewpoints.

5.2.2 Simulate the Requirements

We can use trading tools to simulate a suggested system in place or to add specifics to textual specifications in order to stimulate requirements. The simulation advances the concept of prototyping.

6. Requirement Prioritization using 3 level model:

Functional and non-functional requirements are:

1. Individual user/institution/DSB, police officer should be able to register, log in and log out from the system.

2. The user should be able to track the current status of verification process.
3. The system should provide a help desk to the users to understand the procedure of doing things.
4. The user should be able to submit their documents and information on the institution basis and should be able to submit their purpose.
5. The system admin should be able to authenticate the request coming from various sources.
6. The system admin or in-charge of DSB should be able to assign any police or DSB officer to perform the verification.
7. The system should notify its user after completion of any verification or in assignment of any officer.
8. The system should allow the admin to approve or reject any request. It also should allow to decline any request.
9. The system should generate a verification report based on the outcome of the background check. The report can include details such as verification status, remarks, and recommendations.
10. The system should provide reporting and analytics features to generate insights and track the performance of the verification process.

The Three Level Technique of prioritization in requirement engineering is a method used to prioritize the requirements of a software system. The technique categorizes requirements into three levels: Must-Have, Should-Have, and Nice-To-Have.

Level 1 (Must-Have Requirements): These are the requirements that are considered critical for the system to function and meet its basic objectives. Without these requirements, the system cannot be considered successful.

Level 2 (Should-Have Requirements): These are the requirements that are considered important for the system, but not critical. If some of these requirements are not met, the system will still function, but may not meet the desired level of quality or have all the desired features.

Level 3 (Nice-To-Have Requirements): These are the requirements that are considered desirable but not essential. If these requirements are not met, the system will still function, and the user will still be able to perform the desired tasks.

By categorizing the requirements into these three levels, the development team can focus on the most critical requirements first and then move on to the less critical ones. This helps to ensure that the most important requirements are met, while still allowing room for some flexibility and innovation.

Level 1 (Must-Have Requirements/High):

1. Individual user/institution/DSB, police officer should be able to register, log in and log out from the system.
2. The user should be able to track the current status of the verification process.

3. The user should be able to submit their documents and information on the institution basis and should be able to submit their purpose.
4. The system admin or in-charge of DSB should be able to assign any police or DSB officer to perform the verification.
5. The system should notify its users after the completion of any verification or in assignment of any officer.
6. The system should generate a verification report based on the outcome of the background check. The report can include details such as verification status, remarks, and recommendations.

Level 2 (Should-Have Requirements/Medium):

1. The system should allow the admin to approve or reject any request. It should also allow declining any request.
2. The system admin should be able to authenticate requests coming from various sources.
3. The system should provide reporting and analytics features to generate insights and track the performance of the verification process.

Level 3 (Nice-To-Have Requirements/Low):

1. The system should provide a help desk to users to understand the procedure of doing things.

This prioritization assumes that the basic functionality of the platform is to allow users to borrow and share books, and that other features are secondary. If there are any specific requirements that are more important, they can be moved up to a higher priority level.

7.Traceability Matrix (TCRM)

Use Cases:

UC1-User access control
UC2-Apply for verification
UC3- Submit required information
UC4-View verification status
UC5-receive verification request
UC6- Forward to SB/DSB
UC7-Assign officer
UC8-Report submission

UC9-Decline request

Functional requirements:

FR-1: Individual user/institution/DSB, police officer should be able to register, log in and log out from the system.

FR-2: The user should be able to track the current status of verification process.

FR-3: The system should provide a help desk to the users to understand the procedure of doing things.

FR-4: The user should be able to submit their documents and information on the institution basis and should be able to submit their purpose.

FR-5: The system admin should be able to authenticate the request coming from various sources.

FR-6: The system admin or in-charge of DSB should be able to assign any police or DSB officer to perform the verification.

FR-7: The system should notify its user after completion of any verification or in assignment of any officer.

FR-8: The system should allow the admin to approve or reject any request. It also should allow to decline any request.

FR-9: The system should generate a verification report based on the outcome of the background check. The report can include details such as verification status, remarks, and recommendations.

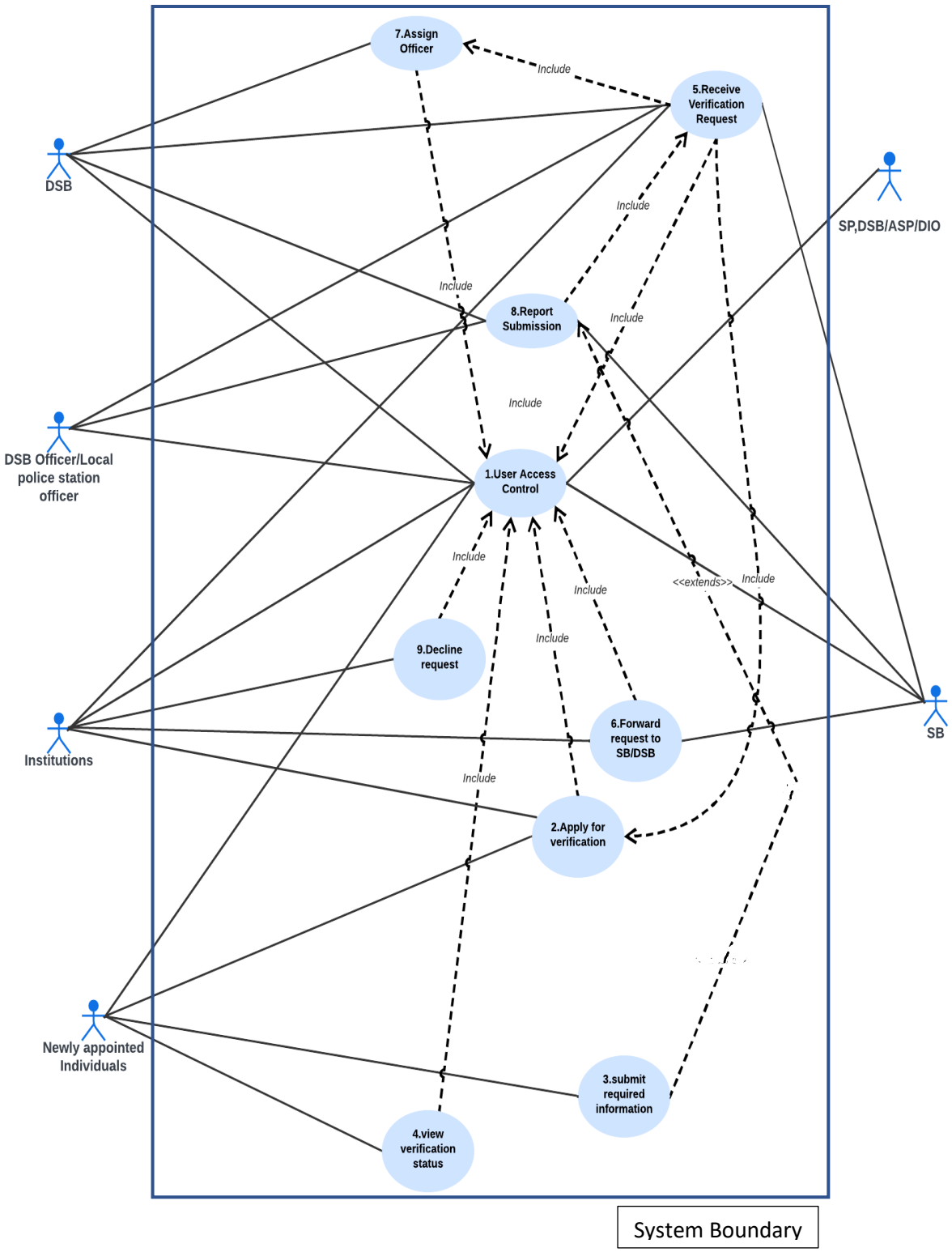
FR-10: The system should provide reporting and analytics features to generate insights and track the performance of the verification process.

A traceability matrix is a table that shows the relationship between use cases and functional requirements. It helps to track the status of requirements and ensure that all requirements are covered in the use cases. Here is the traceability matrix of our system:

Table 18 Traceability matrix

	UC1	UC2	UC3	UC4	UC5	UC6	UC7	UC8	UC9
FR1	✓								
FR2				✓					
FR3									
FR4									✓
FR5									
FR6							✓		
FR7				✓					
FR8									✓
FR9				✓					
FR10								✓	

8. Use Case diagram



9. Use Case Descriptions

Table 19 UC-1

Use Case No.	01	
Use Case	Enter into the system	
Goal	A user creates an account to have access into the system	
Preconditions	None	
Success end condition	'Registration' successfully and an account in created for user	
Success failed condition	Account is not created	
Primary actor:	Newly Individuals appointed, institution, Officer	
Secondary actor:	N/A	
Trigger	User clicks Register option or clicks Login option	
Main success flow	**Step**	**Action**
	01	The user enters the system
	2a	Enter as an Individual requestor
	2.a.1 **2.a.2** **2.a.3** **2.a.4** **2.a.5** **2.a.6**	The user selects 'Sign-up' option The user gives joining ID The user gives code The user gives phone number The user Selects Institution The user selects purpose
	2b	Enter from institution
	2.b.1 **2.b.2** **2.b.3**	The user selects 'Sign-up' option The user gives Institution official mail The user gives Institution name

	2.b.4 **2.b.5** **2.b.6**	The user gives unique institutional id The user Upload legal document The User upload the Signature (head of institution).
	2c	Enter as an Officer
	2.c.1 **2.c.2** **2.c.3** **2.c.4** **2.c.5**	The user selects 'Sign-up' option The user gives Police id The user gives password The user gives designation The User gives posted branch
	3	The user submits the OTP (sent via phone or Mail)
Alternative Flows	**Step**	**Action**
	01	The user enters the system
	2a	Enter as an Individual requestor
	2.1 **2.2**	The user gives joining ID The user gives code
	2b	Enter from institution
	2.1 **2.2**	The user gives Institutional mail The user gives password
	2c	Enter as an officer
	2.1 **2.2**	User gives police id User gives password
Quality Requirements	**Step**	Requirement
	4	The system should be available and accessible to applicants at all times

Table 20 UC-2

Use Case No.	02	
Use Case	Apply for verification	
Goal	Newly appointed individual or promotion purpose verification form is successfully submitted.	
Preconditions	The online verification system must be functional and accessible.	
Success end condition	The applicant has accurately filled in all the necessary personal information in the application form.	
Success failed condition	The applicant does not attach the necessary supporting documents as specified.	
Primary actor:	Newly appointed Individuals, Institution	
Secondary actor:	N/A	
Trigger	"New" option from institution side "My info'' option from individual side	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	The user selects 'My Info' option
	03	User fill up necessary information which include in the form.
	04	User press submit button.
Alternative Flows	**Step**	**Action**
	01	User choose 'new option'
	02	User choose the purpose from purpose drop down box options.
	03	User fill up the appeared form with necessary information.
	04	User press submit button.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 21 UC-3

Use Case No.	03	
Use Case	Submit required information	
Goal	Newly Individuals appointed submits their required information	
Preconditions	The Applicant must be filled up their verification form.	
Success end condition	The applicant successfully fills up their verification form	
Success failed condition	The verification form is incomplete ,submission is failed	
Primary actor:	Newly Individuals appointed	
Secondary actor:		
Trigger	User clicks “Submit” option	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	The user selects ‘Submit’ option
	3.1	User views message of successfully submission
Alternative Flows	**Step**	**Action**
	1	The system prompts them to complete the missing information before proceeding with the submission.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 22 UC-4

Use Case No.	04	
Use Case	View verification status	
Goal	Newly appointed Individuals can see status that in what position their verification form in that time.	
Preconditions	The Applicant or institutions must be submitted their verification form.	
Success end condition	The applicant or institutions can see and understand the verification status information.	
Success failed condition	The verification status information is not available, resulting in outdated or incomplete information being displayed to the applicant.	
Primary actor:	Newly appointed Individuals or institution	
Secondary actor:	Institutions	
Trigger	"Status" option	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	The user selects 'Status' option
	03	User views their status
Alternative Flows	**Step**	**Action**
	1	In case the online verification system experiences technical the applicant may be informed about the issue and requested to try again later.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 23 UC-5

Use Case No.	05	
Use Case	Receive Verification Request	
Goal	The institutions or SB or DSB receives verification requests that require thorough examination.	
Preconditions	The applicant or institution must send their verification form and request for verification.	
Success end condition	The verification request successfully received.	
Success failed condition	Verification request did not receive for technical problem.	
Primary actor:	Institutions (government or private), SB/DSB	
Secondary actor:	Individual requestor	
Trigger	'Verification requests' options	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	The user selects 'Verification Request' option
	3.1 **3.2**	User views request of verification User accepts the verification request
Alternative Flows	**Step**	**Action**
	1	If the applicant encounters difficulties or errors while entering or submitting the verification request, they may seek assistance from the system's help resources or contact the support team for guidance.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 24 UC-6

Use Case No.	06	
Use Case	Forward request to SB/DSB	
Goal	Sending information form or file to the responsible authorities to verify.	
Preconditions	The institution must have the necessary access rights and authorization to initiate and forward verification requests.	
Success end condition	The institutions successfully forward the request for verification to the responsible authority (SB/DSB).	
Success failed condition	The institution failed to forward the request for verification.	
Primary actor:	Institutions (government or private)	
Secondary actor:	Individual requestor.	
Trigger	"Forward" option.	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	The user clicks 'Verification Request' option
	3.1 **3.2** **3.3**	User (institution) views request of verification User (institution) selects the region User (institution) selects Forward option for the file arrived.
Alternative Flows	**Step**	**Action**
	3.1 **3.2** **3.3**	User (SB) views request of verification User (SB) selects the region User (SB) selects Forward option for the file arrived.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 25 UC-07

Use Case No.	07	
Use Case	Assign Officer	
Goal	Assigning a DSB or local police station officer to conduct the verification.	
Preconditions	DSB must be accepted the request of verification.	
Success end condition	DSB successfully assign officer for verify the verification information.	
Success failed condition	DSB failed to assign officer. may be officer is unavailable.	
Primary actor:	DSB	
Secondary actor:		
Trigger	"Assign" option	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	User selects new request and can see the arrived verification request.
	3.1 **3.2** **3.3**	The user selects assign option User can see available officer list User selects an officer of DSB.
Alternative Flows	**Step**	**Action**
	3.1 **3.2** **3.3**	The user selects a local police station User can see available police officer User selects an officer from the list.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 26 UC-8

Use Case No.	08	
Use Case	Report Submission	
Goal	To submit the result of verification after required investigation.	
Preconditions	Police officer or local police station officer must be sent of complete information.	
Success end condition	DSB successfully send verification result to the institution.	
Success failed condition	DSB failed to send of complete verification status.	
Primary actor:	DSB, SB	
Secondary actor:	N/A	
Trigger	"Send" option	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	User selects my cases option
	3.1 **3.2** **3.3** **3.4**	User can see the files he/she is working in. User selects update option User write down the result of the verification. User selects send option.
Alternative Flows	**Step**	**Action**
	1	In case the officer encounters technical difficulties while submitting the report, they can seek assistance from the support team or try again later.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

Table 27UC-9

Use Case No.	09	
Use Case	Decline Request	
Goal	If verification form is incomplete then institution decline the verification request to verify.	
Preconditions	The applicant must be filled up the verification form and send the request for verify	
Success end condition	Institution Check the request and decline it	
Success failed condition	Verification request did not receive for error.	
Primary actor:	Institution	
Secondary actor:	N/A	
Trigger	User clicks “Decline” option	
Main success flow	**Step**	**Action**
	01	The user enters the system
	02	Institution selects new request.
	3	If The Applicant information did not match with the proper format, then institution decline the request
Alternative Flows	**Step**	**Action**
	1	In case the officer encounters technical difficulties while submitting the report, they can seek assistance from the support team or try again later.
Quality Requirements	**Step**	Requirement
	1	The system should be available and accessible to applicants at all times

11. Activity Diagrams

Figure 1: Enter into the system

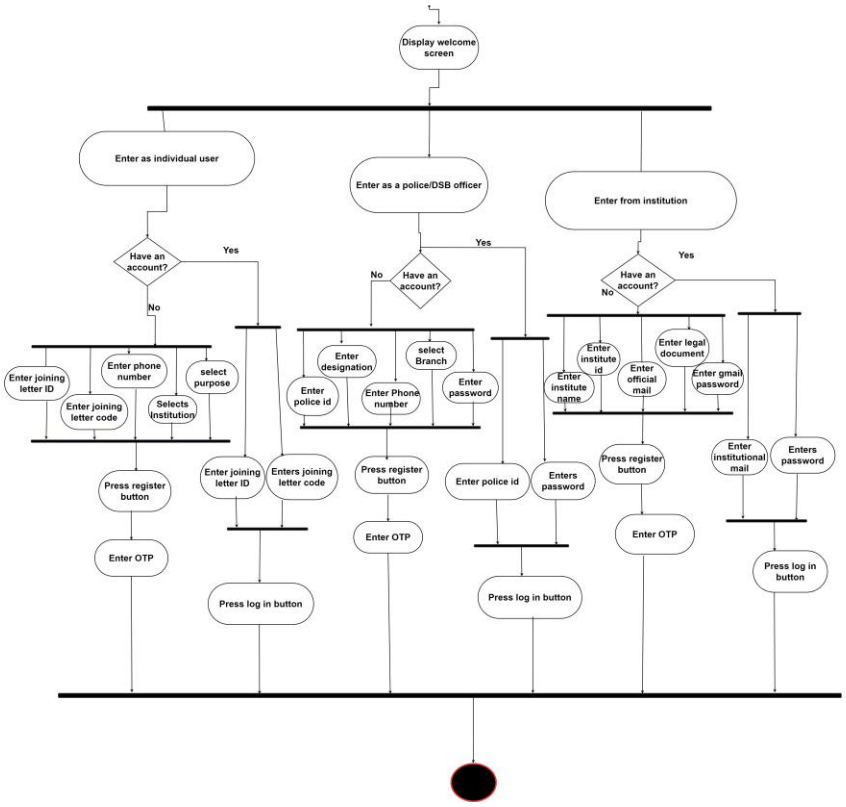


Figure 2: Apply for verification

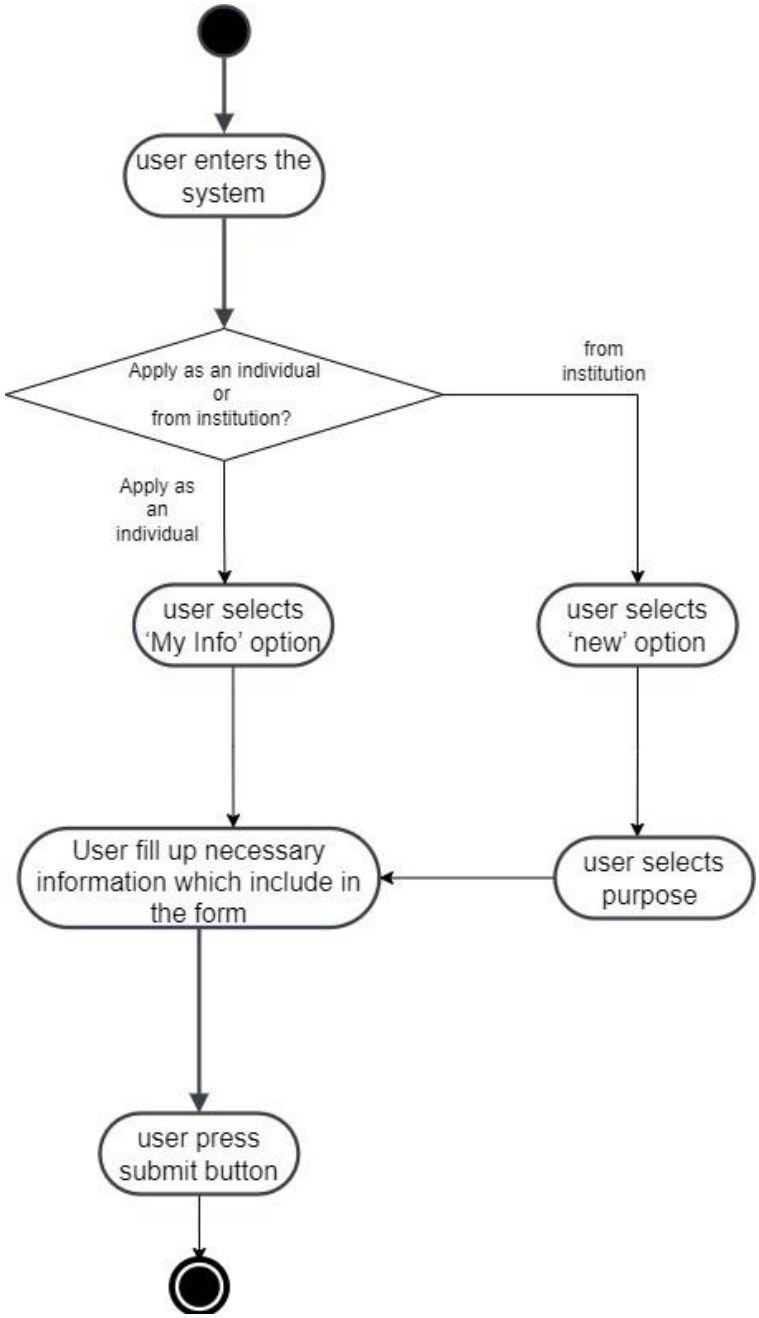


Figure 3: Submit required information

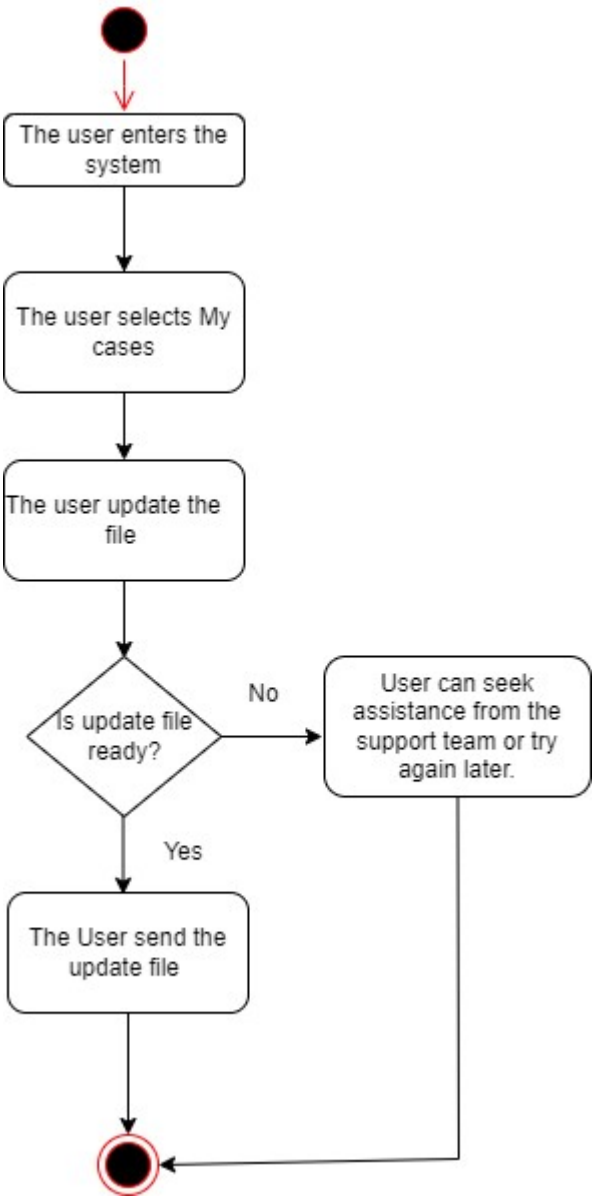


Figure 4: View verification status

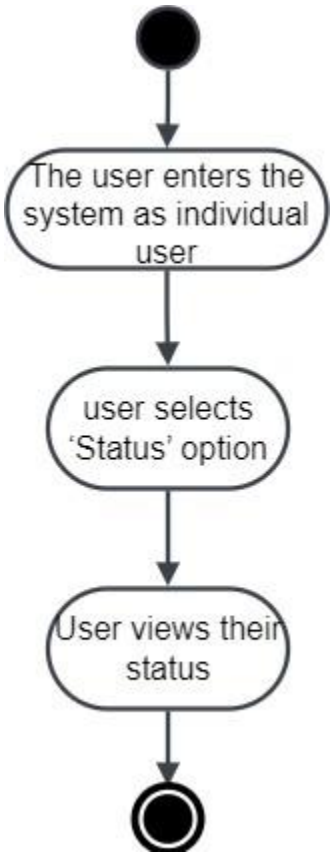


Figure 5: Receive Verification Request

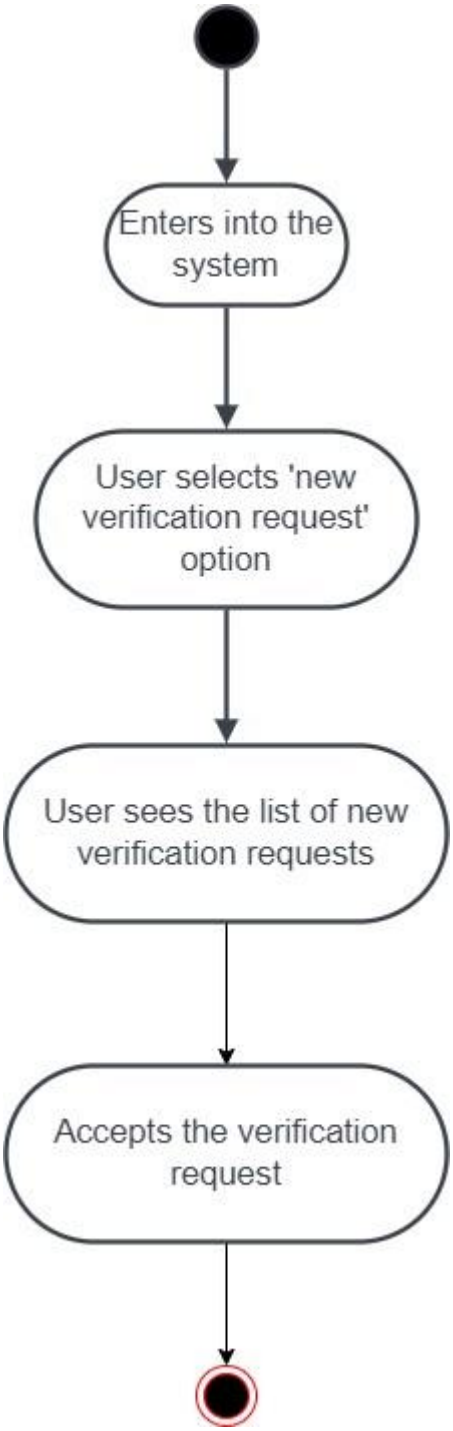


Figure 6: Forward request to SB/DSB

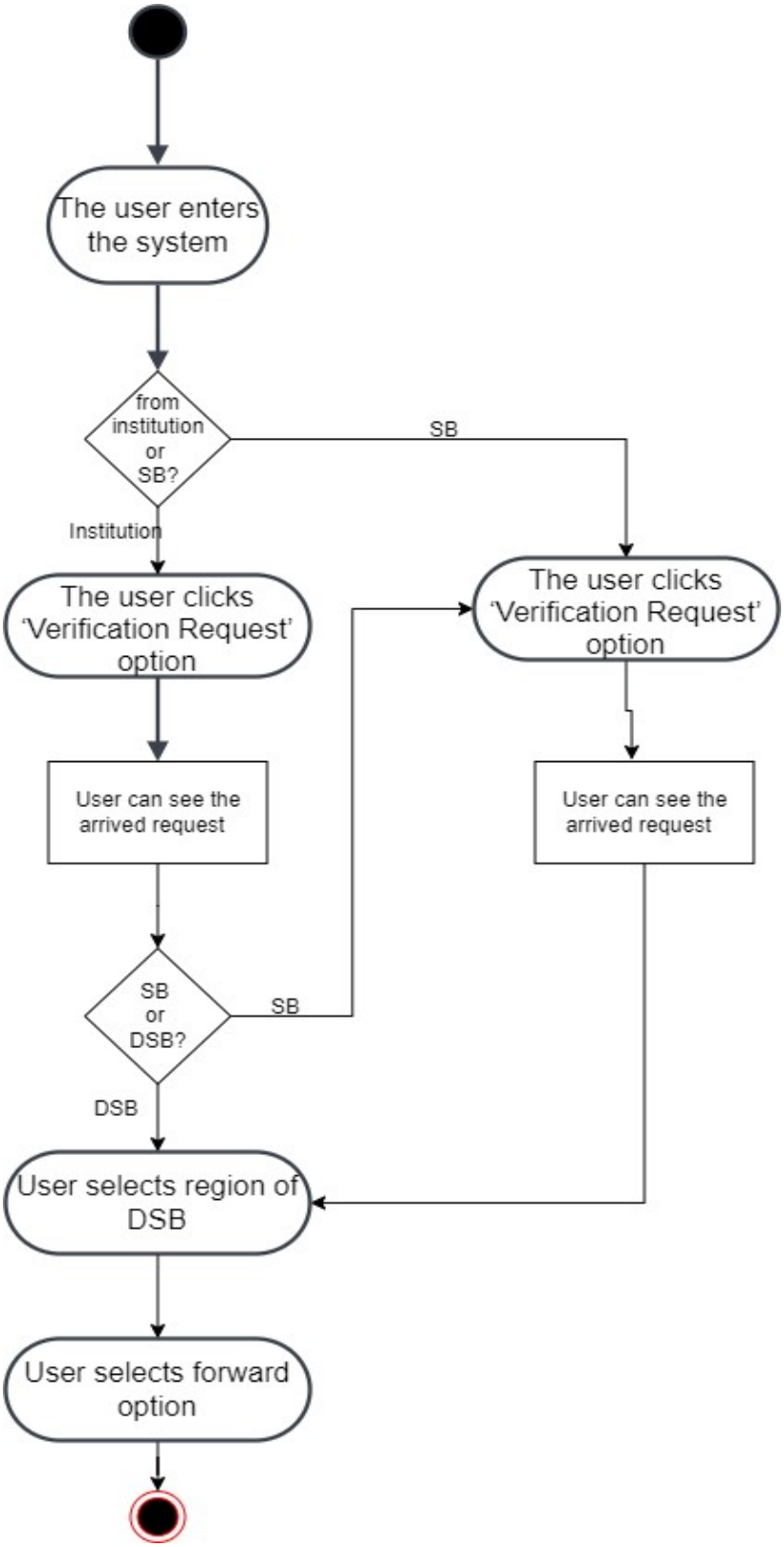


Figure 7: Assign Officer

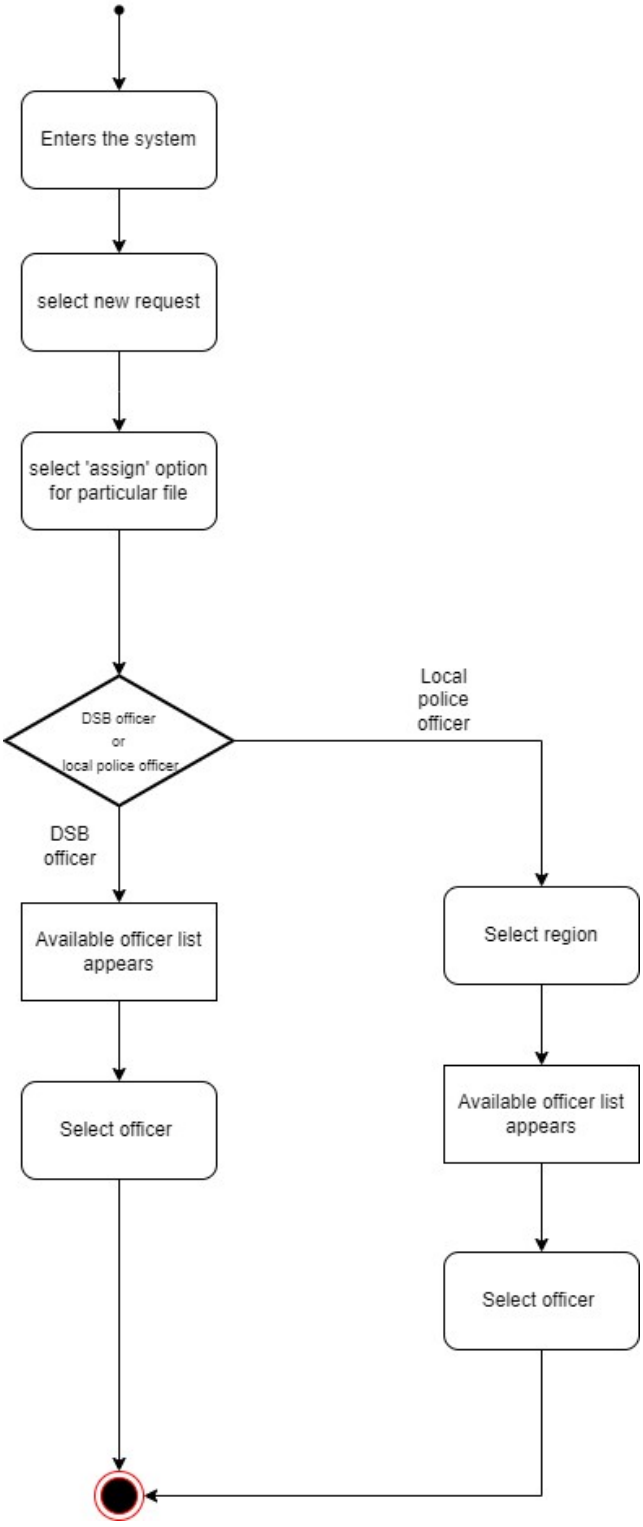


Figure 8: Report Submission

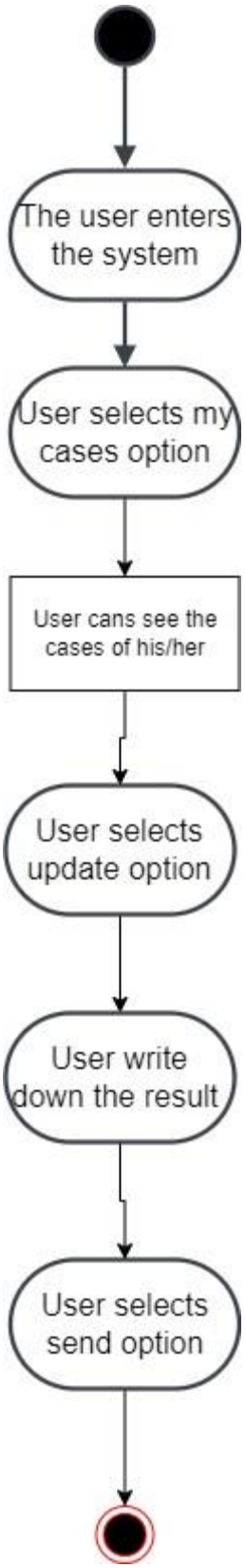


Figure 9: Decline Request