**Rajarambapu Institute of Technology, Rajaramnagar**



**Department of Information Technology**

1. **Y. 2022-23**

***Software Requirements Specification (SRS) document***

| **Area of the Project** | Blockchain Technology |
| --- | --- |
| **Title of the project** | Hyperledger for Public Data Management: Connecting Identities and Streamlining Updates. |
| **Project Guide Name** | Dr. A.C.Adamuthe |
| **Team Leader’s Name** | Swaroop Chandrakant Mane |
| **Group Number** | 11 |

**Members**

| **Sr. No.** | **Roll No.** | **Name** | **Email** | **Phone** | **Sign** |
| --- | --- | --- | --- | --- | --- |
| 1 | 2010005 | Chinmay Santosh Pawar | 2010005@ritindia.edu | 7498840432 |  |
| 2 | 2010008 | Malik Sajid Mujawar | 2010008@ritindia.edu | 8668379318 |  |
| 3 | 2010018 | Samrat Shivaji Mali | 2010018@ritindia.edu | 9022605088 |  |
| 4 | 2010015 | Swaroop Chandrakant Mane | 2010015@ritindia.edu | 9503247242 |  |

|  |  |  |
| --- | --- | --- |
| **Sign of Project Guide** | **Sign of Project In-charge** | **Sign of HOD, IT** |

1. Introduction

The introduction of Hyperledger blockchain technology in the government sector can lead to more efficient, secure, and transparent document management systems that provides a comprehensive overview of the implementation of decentralized, immutable ledger for updating different attributes in various government documents, such as Aadhaar card, PAN card, voter ID card, and ration card. This proposed solution mainly focuses on five commonly changed attributes including name, date of birth, and other considering Aadhaar card as the primary document. This Software Requirements Specification (SRS) document outlines the sequence diagram and describes how the entire process will work, along with the necessary functions required for successful implementation.

1.1. Purpose

The purpose of this SRS document is to define the requirements and specifications for the development of a system that leverages Hyperledger technology to facilitate seamless updates of attributes in government documents. By using a distributed ledger technology, we aim to enhance the efficiency, security, and transparency of the update process, ensuring accuracy and minimizing fraud.

1.2. Scope

This system will primarily focus on the selected government documents, namely Aadhaar card, PAN card, voter ID card, and ration card. It will specifically address the update of five commonly changed attributes, including name, date of birth, address, Gender, Phone No across these documents. The system will allow authorized entities to initiate attribute updates, verify the changes, and maintain an immutable record of all transactions on the Hyperledger blockchain.

1.3. Overview

The oftware Requirements Specification (SRS) involves the analysis and design of the system, which includes the creation of a sequence diagram to illustrate the flow of events and interactions among various components. The sequence diagram will showcase how different functions and entities interact during the attribute update process. These functions include user authentication, attribute verification, update request initiation, approval workflow, blockchain transaction recording, and confirmation to the user.

2. Objectives: -

* To Identify processes and functions for updating common attributes in government documents using Hyperledger technology.
* To Develop a comprehensive and efficient sequence diagram illustrating the flow of the system, highlighting interactions and dependencies among different components.
* To Ensure integration and synchronization of updates across multiple government documents.
* To Design a secure and robust system that maintains data integrity, confidentiality, and authenticity during the attribute update process.

**3. Literature Survey**

The proposed solution was discussed in the research paper "Blockchain for Government Services: Applications and Challenges" by Amrutha M. R. and K. B. Shylaja is to use blockchain technology to improve the efficiency, transparency, and security of government services. Blockchain is a distributed ledger technology that can be used to create a secure and tamper-proof record of transactions. This can be used to improve government services in a number of ways, such as efficiency,Transparency,security,Social welfare,reduced cost etc.[1]

The research paper "Hyperledger Fabric for Government Use Cases: A Survey" by Bhargavi and Mehtre proposes the use of Hyperledger Fabric, a blockchain framework developed by the Linux Foundation, for government use cases. Hyperledger Fabric is a permissioned blockchain, which means that only authorized parties can participate in the network. This makes it a good fit for government use cases, where security and privacy are paramount.

The research paper discusses a number of potential applications of Hyperledger Fabric for government, such as:

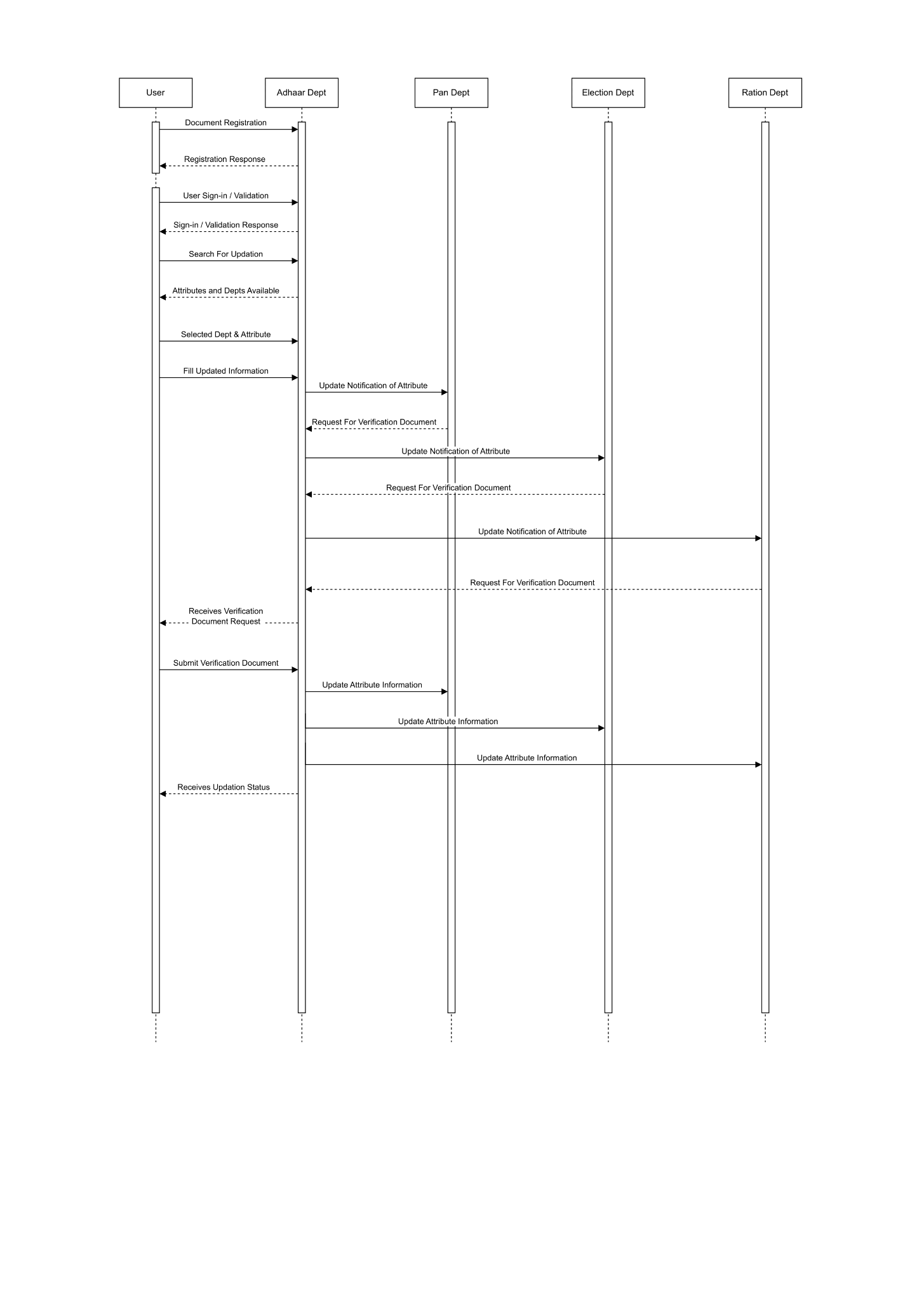
1. E-voting: Hyperledger Fabric can be used to create a secure and transparent system for e-voting. This can help to increase voter turnout and reduce fraud.
2. Land registry: Hyperledger Fabric can be used to create a secure and transparent system for land registration. This can help to reduce fraud and disputes over land ownership.
3. Social welfare: Hyperledger Fabric can be used to create a secure and transparent system for social welfare payments. This can help to reduce fraud and ensure that payments are made to the correct people.
4. Supply chain management: Hyperledger Fabric can be used to track the movement of goods through a supply chain. This can help to improve efficiency and reduce fraud.
5. Healthcare: Hyperledger Fabric can be used to store and share medical records in a secure and transparent way. This can improve patient care and reduce the risk of medical errors.
6. Education: Hyperledger Fabric can be used to track student progress and manage educational records. This can help to improve student outcomes and reduce fraud.
7. Taxation: Hyperledger Fabric can be used to track tax payments and ensure that taxes are paid correctly. This can help to improve tax collection and reduce tax evasion.[2]

The proposed solutions from the paper "Blockchain in Public Administration: A Systematic Literature Review and Research Agenda" by Marchesi, Barra, Cimmino, and Grasso:

Use blockchain to improve transparency and accountability in government. Blockchain can be used to create a tamper-proof record of government transactions, which can help to improve transparency and accountability. This can be done by making government data more accessible to the public and by making it more difficult for government officials to commit fraud or corruption.

Use blockchain to improve efficiency and effectiveness of government services. Blockchain can be used to automate government processes, such as processing of payments and approvals. This can save time and money, and it can also improve the accuracy of data. For example, blockchain can be used to automate the process of issuing and renewing driver's licenses. This would save the government time and money, and it would also reduce the risk of fraud.[3]

4. System Sequence Diagram



**Figure no.1**: **System Sequence Diagram**

5. Process Identification

1. Document Registration : The user initiates the registration process by submitting their documents (e.g., Aadhaar card, PAN card, voter ID card, ration card) to the primary entity (Aadhaar department). This step involves providing necessary identification and personal information.
2. Registration Response : The primary entity (Aadhaar department) verifies the submitted documents and sends a registration response to the user. This response confirms whether the documents are valid and the user is successfully registered in the system.
3. User Sign-in / Validation : The user signs in to the system using their registered credentials. This step involves authentication and validation of the user's identity and access rights.
4. Sign-in / Validation Response : The system responds to the user's sign-in/validation request, granting access if the provided credentials are valid and the user is authenticated successfully.
5. Search For Updation : The user searches for the specific attribute(s) they want to update in their government documents (e.g., name, date of birth). This step involves the user identifying the attribute(s) they want to modify.
6. Attributes and Depts Available : The primary entity (Aadhaar department) provides the user with a list of available attributes and corresponding departments that can update those attributes. This information helps the user make informed choices regarding the attribute updates they wish to proceed with.
7. Selected Dept & Attribute : The user selects the desired department and attribute from the provided options. This selection determines where the update request will be forwarded within the system.
8. Update Notification of Attribute : The primary entity (Aadhaar department) notifies the relevant departments (e.g., PAN department, election department, ration department) about the attribute update requested by the user. This step ensures that all involved departments are aware of the upcoming changes.
9. Request For Verification Document : The other departments (e.g., PAN department, election department, ration department) send a request to the primary entity (Aadhaar department) for verification documents related to the user's attribute update. This request is made to validate the authenticity and accuracy of the update.
10. Receives Verification Document : The primary entity (Aadhaar department) informs the user about the verification document request made by the other departments. The user is prompted to provide the necessary verification documents to support their requested attribute update.
11. Submit Verification Document : The user submits the required verification document(s) to the primary entity (Aadhaar department). These documents serve as evidence to authenticate the requested attribute update.
12. Update Attribute Information : The primary entity (Aadhaar department) updates the attribute information in all relevant departments (e.g., PAN department, election department, ration department) using a smart contract. This ensures consistency and synchronization of the attribute updates across multiple entities.
13. Update Attribute Information : The primary entity (Aadhaar department) notifies the user about the successful update of their requested attribute(s) in the government documents. The user is informed that the update process has been completed and the relevant departments have been notified accordingly.

6. Specific Requirements:

6.1. Functional Requirements:

1. User Authentication: The system should incorporate a robust user authentication mechanism to ensure that only authorized individuals can access and initiate attribute updates. This may involve methods such as two-factor authentication, biometric verification, or digital signatures.
2. Attribute Verification: The system needs to implement checks and validations to ensure the authenticity and correctness of the attribute updates. This may involve validating the submitted data against government databases, performing data consistency checks, and verifying the identity of the user initiating the update.
3. Update Request Initiation: The system should provide a secure and user-friendly interface for users to initiate attribute update requests.that should be replicated in all desirable documents.This interface should capture the necessary information required for the update, validate the data entered.
4. Approval Workflow: The system must facilitate a well-defined workflow for the approval of attribute updates by the appropriate authorities. This workflow may involve multiple levels of approval, with designated officials verifying and validating the requested updates before granting approval.
5. Blockchain Transaction Recording: All approved attribute updates should be recorded as immutable transactions on the Hyperledger blockchain. This ensures transparency, tamper-proof record-keeping, and traceability of all attribute changes made to the government documents.
6. Confirmation to User: The system should provide timely notifications and confirmations to users regarding the status of their attribute update requests. This includes informing users about the approval or rejection of their requests and providing updates on the progress of their updates through different stages of the workflow.

6.2. Non- Functional Requirements:

1. Security: The system needs to implement strong security measures to protect sensitive user data and prevent unauthorized access. This includes encryption of data during transmission and storage, secure user authentication mechanisms, and access control mechanisms to ensure that only authorized personnel can access the system.
2. Performance: The system should be capable of handling a significant volume of attribute update requests efficiently. It should be designed to handle concurrent user requests, minimize response times, and ensure smooth performance even during peak load periods.
3. Scalability: The system should be designed to accommodate potential future expansions, allowing the addition of more attributes and government documents. It should be able to handle increased user loads and data storage requirements without significant degradation in performance.
4. Usability: The user interface of the system should be intuitive, user-friendly, and easily navigable. It should provide clear instructions to users, guide them through the attribute update process, and minimize the need for extensive training or technical expertise.
5. Maintainability: The system should be designed in a modular and extensible manner, facilitating easy maintenance and future enhancements. It should have well-documented code and configuration, allowing for efficient troubleshooting, bug fixes, and updates as required.

**References**

1. Amrutha M. R. and K. B. Shylaja. (2019). Blockchain for Government Services: Applications and Challenges. International Journal of Innovative Technology and Exploring Engineering, 8(12), 149-154.
2. Bhargavi, V., and Mehtre, B. M. (2020). Hyperledger Fabric for Government Use Cases: A Survey. International Journal of Advanced Computer Science and Applications, 11(2), 334-339.
3. Marchesi, M., Barra, M., Cimmino, M. A., and Grasso, A. (2021). Blockchain in Public Administration: A Systematic Literature Review and Research Agenda. Journal of Public Administration Research and Theory, 31(2), 343-362.

**Sign of Project Guide Sign of Project In-charge Sign of HOD, IT**