**Scope and Objectives:**

The main objectives of this project are to develop a secure and efficient blockchain and smart contracts-controlled data sharing platform with multi-user access and role-based authentication. The platform aims to address the vulnerabilities in current data management practices by providing fine-grained access control, persistent metadata management, and robust end-point security measures.

1. Blockchain-Controlled Data Sharing:

Our primary goal is to create a decentralized data sharing platform leveraging blockchain technology. This will ensure a distributed and tamper-resistant network, eliminating single points of failure and unauthorized access. We will utilize smart contracts to automate data sharing and resource-provisioning processes, to promote transparency and accountability.

1. Multi-User Access and Role-Based Authentication:

This project will implement a comprehensive user authentication system with role-based access control (RBAC). Different user roles within the organization hierarchy will be granted specific access permissions, enhancing data security and minimizing the risk of unauthorized data exposure. The roles of individuals in the company will also be used to facilitate a Proof of Authority consensus mechanism.

1. Persistent Metadata Management:

Our platform will incorporate a robust metadata management system to facilitate policy-compliant data classification and access control. Metadata will store vital information related to data ownership, access permissions, update records, and usage policies, and much more, to ensure compliance with company policies and regulatory requirements.

1. End-Point Security Measures:

To enhance user interactions' security, our project will implement end-point security measures. Secure communication protocols will be employed to safeguard data transmission between clients and the platform.

1. Encryption with Integrity Controls:

To safeguard multi-user data, we will use encryption with integrity controls. Advanced cryptographic techniques will be used to ensure data confidentiality and integrity, protecting sensitive information from unauthorized access and tampering.

1. Fine-Grained File Sharing:

The project will analyze and implement access control mechanisms to enable fine-grained file sharing between various components of the organization hierarchy. Attribute-based access control (ABAC) will be explored to handle complex access control policies efficiently.

1. Notifications for Policy Non-Compliance or Violations:

An essential aspect of the platform will be the incorporation of a notification system to alert relevant users and administrators in case of policy non-compliance or access control violations. Real-time notifications will be sent through emails, messages, and in-app alerts to promptly address any security breaches or policy violations.

**Stakeholders:**

For the development of the application’s prototype, we will be taking up a ‘contract’ for a company ‘Eventopolis’.

Make note of the hierarchy of executives in this company. The following shows it, in decreasing order of precedence:

1. The CEO
2. Other C-level Executives - CTO, CFO, CISO, CHRO
3. Horizontal Heads (Hospitality, Public Relations, Logistics, Technology, and Security)
4. Project Managers ( specific for each new event)
5. Vertical Heads (specific for each of the departments for every event being planned)
6. Executives (the team under the vertical heads, responsible for carrying out the operations)
7. Third-party vendors (being contracted by the company)
8. Clients

(The Vertical Heads are responsible for their particular departments during an event, which falls under the immediate authority of that particular project’s manager. The department managers, i.e., the Horizontal Heads, however, are responsible for the entire company’s resources in that particular department.

To make this clear, here’s an example: As the company’s Logistics Manager, I will have access to the details of all the venues we have in our database. However, as part of a project (i.e., an event that the company has taken a contract for), my role as the Logistics Head for that particular event will only warrant me access to the details of the venue for my particular event.

The Department managers, i.e., the Horizontal Heads, of Hospitality, Public Relations, Logistics, Technology, and Security, are responsible for the entire company’s resources for their particular departments. They are responsible for monitoring all of said resources, their inflow and outflow, both, and allocate them accordingly for every project that the company undertakes. They are also responsible for authorizing the addition or removal of any dataset or entity from the company’s consolidated database. For example, no new catering company can be affiliated with the company for any event if not authorized by the Hospitality Manager.