



Mukesh Patel School of Technology Management & Engineering




Topic Approval Form

Department: B. Tech Computer Science Engineering

Program: Cybersecurity

Semester: 7th

Project Team Details:

| S. No. | SAP ID | Roll No. | Name | Signature |
|--------|-------------|----------|----------------|---|
| 1 | 70102000011 | K007 | Yash Burshe |  |
| 2 | 70102000024 | K035 | Ridhima Mishra |  |
| 3 | 70102000110 | K047 | Arushi Rai |  |

Type of Project:

Product

Project Details:

| | | |
|--------------------------|--|--|
| Project Title | Decentralized Data and Resource-Provisioning System with End-Point Security | |
| Introduction | <p>In the current data management practices still being implemented at leading organizations that process a plethora of data across thousands of employees, vendors, and customers, the manual allotment of data access and permissions introduces significant vulnerabilities, making the system prone to single points of failure and susceptible to various risks. For instance, human errors, disgruntled employees, “whistle-blowers”, etc. with unauthorized access pose serious threats to data security and integrity. These factors can lead to data breaches, leakage of sensitive information, and compromised data privacy, resulting in severe consequences for organizations.</p> <p>To mitigate these risks and enhance data security, our project proposes a decentralized file storage system, employing blockchain technology to revolutionise data access control. We want to replace the manual allocation process with a consensus-based system, controlled and maintained by smart contracts. The goal is to create a more secure, transparent, and tamper-resistant data management solution.</p> <p>Our proposed system utilises a Proof of Authority mechanism, and the smart contracts are pre-defined based on company policies, laws, guidelines, and regulations. This system ensures that only authorized entities are granted access to specific data based on their roles within the organization hierarchy. Each user's reputation is stored on the blockchain in line with that user’s position in the organization hierarchy, establishing a trust-based approach for data access and permission granting.</p> <p>By leveraging blockchain's decentralized nature and immutability, the system minimizes the risks associated with centralized authority and reduces the chances of data breaches due to human factors. The smart contracts act as self-executing protocols, eliminating the need for intermediaries, and ensuring that access control decisions are automated, transparent, and resistant to manipulation.</p> <p>The proposed system brings greater accountability and transparency, as all data access and permission changes are recorded on the blockchain, making it auditable and traceable. Any attempt to tamper with the data or modify access permissions without proper authorization will be immediately detected and flagged, ensuring data integrity and mitigating insider threats.</p> | |
| Literature Survey | <p>BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control</p> | <p>The paper presents BDSS-FA, a blockchain-based data security sharing platform with fine-grained access control for the Internet of Things (IoT). The platform is designed to address the challenge of establishing an effective data sharing mechanism between different organizations for IoT. BDSS-FA is based on blockchain and HABE, which provide a secure data sharing mechanism with traceability and fine-grained access control. The system framework includes Key Generation Center (KGC), Data Owner (DO), P2P based data distribution platform, IPFS Cluster, Fabric Blockchain and Data Consumer (DC). The paper also describes the system initialization process, the</p> |

| | | |
|-------------------------------------|--|---|
| | | functions of the six entities in the system framework, and the deployment of the Fabric blockchain. BDSS-FA can provide a secure and efficient data sharing mechanism for IoT. Further research is needed to explore the integration of BDSS-FA with existing data management systems and the mechanisms by which BDSS-FA facilitates decentralized data and resource-provisioning. |
| | Blockchain-Enabled Data Sharing in Supply Chains: Model, Operationalization, and Tutorial | This paper is about Blockchain-Enabled Data Sharing in Supply Chains. It discusses the challenges of data sharing in supply chains and how blockchain technology can be used to create a secure and trustworthy data-sharing mechanism. The paper proposes a new data-valuation and data-pricing mechanism called usage-based valuation, where the value of the data is determined based on its intended use. The paper also provides a step-by-step guide for setting up a blockchain-enabled data-sharing marketplace using Hashgraph. Additionally, the growing theoretical literature on data valuation and provides references to related studies is reviewed. The aim is to help readers overcome the challenges of data sharing in supply chains using blockchain technology. |
| | A Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology | This research paper proposes a medical data sharing scheme based on attribute cryptosystem and blockchain technology. The scheme addresses security risks associated with existing medical data sharing schemes and ensures the authenticity of data sources. The encrypted medical data is stored in the cloud, and the storage address and medical-related information are written into the blockchain, which ensures efficient storage and eliminates the possibility of irreversible modification of the data. The proposed scheme combines attribute-based encryption (ABE) and attribute-based signature (ABS), which achieves the sharing of medical data in many-to-many communications. The ABE achieves data privacy and fine-grained access control, and the ABS verifies the authenticity of the source of the medical data while protecting the signer's identity. The scheme also reduces the computational burden by outsourcing most of the operations of medical data ciphertext decryption to the cloud service provider (CSP). The paper concludes that the proposed scheme satisfies the requirements for confidentiality and unforgeability in the random oracle model and offers higher computational performance than other similar schemes. |
| Project Objectives and Scope | <p>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.</p> <p>1. Blockchain-Controlled Data Sharing:</p> | |

| | |
|---|---|
| | <p>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.</p> <p>2. 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.</p> <p>3. 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.</p> <p>4. 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.</p> <p>5. 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.</p> <p>6. 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.</p> <p>7. 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.</p> |
| Hardware and Software to be used | <p>Hardware:</p> <p>1. Server Infrastructure: Our project will rely on a robust server infrastructure to host the blockchain network, backend services, and the decentralized file storage system. High-performance servers with adequate processing power, memory, and storage capabilities will be deployed to ensure smooth and efficient data processing and storage.</p> <p>2. End-User Devices:</p> |

| | |
|----------------|--|
| | <p>The platform will cater to various end-user devices such as computers, laptops, tablets, and smartphones. Compatibility with a wide range of devices is crucial to ensure broad user accessibility and engagement.</p> <p>Software:</p> <ol style="list-style-type: none"> 1. Python and C++: Python and C++ will both serve as the primary programming languages for backend development. 2. IPFS (InterPlanetary File System): IPFS will be integrated as the decentralized file storage system to store files securely across the network. 3. NoSQL Database: A NoSQL database like Firebase will be employed to manage persistent metadata related to data classification, access control settings, user roles, and all the data itself. 4. React: For frontend web development, React will be used to create a user-friendly and interactive web interface. 5. Cryptography Libraries: Python's cryptography libraries will be utilized for data encryption, hashing, and digital signatures. 6. API Security Tools: To protect the system from potential security threats, API security tools such as token-based authentication and input validation will be employed. |
| Domains | <ol style="list-style-type: none"> 1. Blockchain Technology: Our project heavily relies on blockchain technology for creating a secure and decentralized data sharing platform. This domain involves understanding blockchain networks, consensus algorithms, smart contracts, and cryptographic techniques. 2. Data Security and Privacy: Ensuring data security and privacy is a critical domain in our project. It includes implementing encryption, access control mechanisms, and secure communication protocols to protect sensitive information from unauthorized access and tampering. 3. Decentralized Systems: The project's focus is on creating a decentralized file storage system and leveraging distributed networks to achieve our goals. 4. Access Control and Authorization: This involves designing and implementing fine-grained access control mechanisms, role-based authentication, and attribute-based encryption for granting data access to authorized users. 5. Performance Evaluation and Scalability: Evaluating the performance of the platform and ensuring its scalability to handle increasing data and user loads are vital to use for delivering an efficient and reliable system. |

| | |
|--------------------------|---|
| | <p>6. Cryptography: The domain of cryptography plays a key role in securing data through encryption, hashing, and digital signatures, safeguarding data integrity and confidentiality.</p> <p>7. Policy Compliance and Governance: The project involves implementing persistent metadata to facilitate policy-compliant data classification and access, which is part of the domain of policy compliance and governance.</p> |
| Motivation | <p>The motivation for our project stems from the vulnerabilities and risks present in current data management practices implemented by leading organizations. In such environments, where vast amounts of data are processed across numerous employees, vendors, and customers, the manual allotment of data access and permissions introduces significant challenges.</p> <p>The existing system's reliance on manual processes makes it prone to single points of failure, human errors, and potential threats from disgruntled employees or unauthorized individuals with access. These factors can lead to severe consequences such as data breaches, leakage of sensitive information, and compromised data privacy.</p> <p>To address these critical issues and enhance data security, privacy, and accessibility, our project proposes the development of a decentralized file storage system with blockchain and smart contracts-controlled data sharing. The primary motivation is to establish a more secure, transparent, and tamper-resistant data management solution that reduces the risk of unauthorized access, manipulation, and data breaches.</p> <p>By leveraging blockchain technology and smart contracts, our project aims to create a decentralized platform that eliminates centralized control and offers fine-grained access control. This will ensure that data access is granted based on specific attributes and policies, limiting exposure to only authorized users within the organization hierarchy.</p> <p>Ultimately, the motivation behind our project is to provide organizations with a robust, efficient, and user-friendly data sharing platform that empowers them to manage data securely, maintain data privacy, and enforce access control policies effectively. By adopting this innovative solution, organizations can significantly enhance their data security measures and mitigate the risks associated with manual data management practices, promoting a more secure and trustworthy digital ecosystem.</p> |
| Expected outcomes | <p>1. Enhanced Data Security: The implementation of blockchain technology and fine-grained access control will significantly enhance data security, reducing the risk of data breaches and unauthorized access. By leveraging cryptographic techniques and decentralized storage, we will ensure data confidentiality and integrity.</p> <p>2. Improved Data Privacy: The platform's fine-grained access control mechanisms and role-based authentication will empower organizations to enforce strict data privacy policies. This will enable them to grant access only to authorized personnel based on their specific roles, minimizing the chances of sensitive data exposure.</p> |

| | |
|--|--|
| | <p>3. Increased Transparency and Accountability: The use of blockchain technology will introduce transparency and immutability to data sharing transactions. All access control decisions and permission changes will be recorded on the blockchain, creating an auditable and traceable system, fostering accountability within the organization.</p> <p>4. Streamlined Data Sharing: The platform will provide a user-friendly interface for seamless and efficient data sharing. Users will have access to relevant data based on their roles and permissions, promoting collaboration and streamlining data exchange processes.</p> <p>5. Mitigation of Insider Threats: With access control measures in place, the platform will reduce the risk of insider threats posed by disgruntled employees or unauthorized personnel. Unauthorized data access attempts will be flagged, allowing for prompt action to prevent or respond to data breaches.</p> <p>6. Scalability and Performance: The project's evaluation of performance and scalability will ensure that the platform can handle a growing number of users and data volumes effectively. This will result in a reliable and efficient system that can accommodate organizational growth.</p> <p>7. Compliance with Policies and Regulations: The platform's persistent metadata management system will facilitate policy-compliant data classification and access. Organizations will be able to adhere to internal policies and regulatory requirements, avoiding potential legal and compliance issues.</p> <p>8. Real-time Notifications for Policy Violations: The incorporation of a notification system will provide timely alerts for policy non-compliance or access control violations. This feature will enable organizations to proactively address security breaches and maintain data integrity.</p> <p>9. Trust-Based Data Sharing: The introduction of a Proof of Reputation mechanism will establish a trust-based approach for data access and permission granting. This will foster trust among users, ensuring that only reputable individuals can access sensitive data.</p> <p>10. Practical Application in IoT: The platform's efficiency and adaptability make it well-suited for practical application scenarios in the Internet of Things (IoT). Organizations can securely share IoT-generated data with authorized stakeholders, enabling data-driven decision-making and innovation.</p> |
|--|--|

Latest References

| S. No. | Publication |
|--------|-------------|
|--------|-------------|

| | |
|---|---|
| 1 | Xu, H., He, Q., Li, X., Jiang, B., & Qin, K. (2020). BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control. IEEE Access, 8, 88863-88875. doi: 10.1109/access.2020.2992649 |
| 2 | Wang, Z., Zheng, Y., Jiang, B., & Tang, O. (2021). Blockchain-Enabled Data Sharing in Supply Chains: Model, Operationalization, and Tutorial. Production and Operations Management, 30(4), 1013-1033. https://doi.org/10.1111/poms.13356 |
| 3 | Y. Zhang, Y. Zhang, Y. Zhang, and Y. Zhang, "A Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology," in IEEE Access, vol. 8, pp. 48600-48609, 2020, doi: 10.1109/ACCESS.2020.2973656 |

Status of the Project after Review 1

| | |
|--|--|
| Comments/Remarks | |
| Name and Signature of the Guide | |

| | |
|---|--|
| Name and Signature of Panel Members for Review 1 | |
| Signature of HoD | |

Changes to be noted here (any changes after Review 1 presentation, as per the comments received from the panel, and areas of concern):