AN EFFECTIVE PRIVACY PRESERVING BLOCKCHAIN ASSISTED SECURITY PROTOCOL

A PROJECT REPORT

Submitted by,

THRISHA REDDY P	**20211CEI0166**
HRUTHIKA S N	**20211CEI0157**
CHANDANA G S	**20211CEI0141**

Under the guidance of,

Dr. JOE ARUN RAJA

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER ENGINEERING (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

DECEMBER 2024

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Project report **“AN EFFECTIVE PRIVACY PRESERVING BLOCKCHAIN ASSISTED SECURITY PROTOCOL”** being submitted by “THRISHA REDDY P, CHANDANA G S, HRUTHIKA S N” bearing roll number “20211CEI0166, 20211CEI0141, 20211CEI0157” in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Engineering (Artificial Intelligence and Machine Learning) is a bonafide work carried out under my supervision.

Dr. Joe Arun Raja
Associate Professor
School of CSE&IS
Presidency University

Dr. Gopal Krishna Shyam
HoD
School of CSE&IS
Presidency University

Dr. L. SHAKKEERA
Associate Dean
School of CSE
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-VC School of Engineering
Dean -School of CSE&IS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **AN EFFECTIVE PRIVACY PRESERVING BLOCKCHAIN ASSISTED SECURITY PROTOCOL** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Engineering (Artificial Intelligence and Machine Learning)**, is a record of our own investigations carried under the guidance of **Dr. Joe Arun Raja, Associate Professor, School of Computer Science Engineering & Information Science, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

Student Name	Roll Number	Signature
Thrisha Reddy P	20211CEI0166	
Hruthika S N	20211CEI0157	
Chandana G S	20211CEI014	

ABSTRACT

This project presents a state-of-the-art privacy-preserving blockchain-assisted security protocol tailored for cloud-based Digital Twin (DT) environments. Digital Twin technology revolutionizes simulation, real-time monitoring, and optimization across industries, but its adoption hinges on secure data sharing and integrity verification. The proposed solution integrates blockchain technology with certificateless cryptography to address critical challenges in secure communication, data integrity, and user privacy.

The system leverages blockchain for tamper-proof data exchange and decentralized verification, avoiding reliance on central authorities. Certificateless cryptography also simplifies key management and eliminates weaknesses such as key escrow and identity impersonation. ECC is used for computational efficiency, and the implementation makes it suitable for resource-constrained environments such as IoT and healthcare.

Therefore, this protocol creates a robust anti-replay able and man-in-the-middle type of attack and also ensures user anonymity in accordance with data-protection regulations: it is designed based on scalable and very efficient architecture that makes it transformational for secure operation for Digital Twin applications, opening up to further development toward manufacturing, smart healthcare, smart cities, or other industries based on the new paradigm.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC, School of Engineering and Dean, School of Computer Science Engineering & Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Deans **Dr. Shakkeera L and Dr. Mydhili Nair,** School of Computer Science Engineering & Information Science, Presidency University, and Dr. "Gopal Krishna Shyam", Head of the Department, School of Computer Science Engineering & Information Science, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. Joe Arun Raja, Associate Professor** and Reviewer **Ms. Yogeetha, Assistant Professor**, School of Computer Science Engineering & Information Science, Presidency University for her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the PIP2001 Capstone Project Coordinators **Dr. Sampath A K, Dr. Abdul Khadar and Mr. Md Zia Ur Rahman,** department Project Coordinators Ms. Sudha P and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Thrisha Reddy P
Hruthika S N
Chandana G S

LIST OF FIGURES

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO THE PROJECT

A Digital Twin is a precise, live digital replica of the functionalities of a physical system. To conduct simulations in the virtual world, a clone of the physical item is created in the DT environment. In 2002, Grieves and Vickers originally introduced the notion of using a clone to do simulations in a virtual environment. The National Aeronautics and Space Administration (NASA) called this technology a DT in 2010. The Industrial Internet of Things (IIOT) and Industry 4.0 paradigms may now be benefited from thanks to the development of the DT concept. The goal is to enable automated connection setup and auto-discovery by providing access to all control interface descriptions and data sources relevant to processes or products via a single interface. By examining the DTs of the included components, developers and engineers may identify, create, and build the necessary interfaces, integrations, and communication linkages without having to have expertise of each component. In the future, it might not be necessary for an engineer to intervene on behalf of the devices for them to locate and interact with one another. This type of auto-discovery and auto established connectivity, with the help of DTs, may someday make IOT more scalable for applications that are today unthinkable. The industrial, construction, healthcare, and space industries are just a few of the many sectors where DT technology is being researched.

The application area of DT technology has lately expanded to include IOT and mobile devices. For example, in an automobile setting, autonomous driving is possible, while in a hospital setting, accurate and thorough remote medical care is possible. Because cloud computing offers so many benefits, it is the most practical way to install DT services. Because it offers on-demand services, computational power, widespread network connectivity, and other features, it fits well with the design of the upcoming information technology age.

In situations where data is generated from physical assets and sent to a cloud server, data owners in cloud assisted DT environments simulate data transfer in a virtualized environment and share the simulation outcomes with the owner. In addition, the user has request-based access to the data. However, there are a number of challenges in using DT technology. The most difficult task is figuring out how to securely transmit real-time and simulation data. If the adversary obtains the sensitive information that the data owner transmitted, there will be grave privacy consequences. It appears that the following points— illustrated below—are essential for the implementation of the DT environment: The need to provide a safe channel for effectively exchanging the sent information is great. A process for verifying the sent data is necessary; in other words, data integrity must be verified. It is important to ensure security requirements including untrace ability, anonymity, and secrecy.

In order to fulfil the above-described security requirements, we require a private and secure authentication system that makes use of block chain technology. Block chain allows the person using the data or the data owner to confirm the data's integrity. Users can use a Merkle hash tree to easily verify the requested data. By using a cloud server to store the DT data and a block chain to keep the data hash values, the system presented in this study allows users to confirm the accuracy of the data they have received. Moreover, the user-server shared data log transactions are posted to the block chain. The literature introduces a number of authentication systems, however most of them are vulnerable to different types of security attacks. For example, a large number of two-factor based protocols are unable to support user anonymity and forward secrecy; many are also vulnerable to identity and password guessing attacks. Comparably, only a tiny percentage can be verified using the ROR Model and BAN logic, and some are vulnerable to user and server impersonation attacks. Furthermore, identity-based and conventional public cryptosystems are used in the design of the majority of authentication processes. These cryptosystems do, however, have certain weaknesses. The intricate certificate administration, storage, and key escrow problems are the weaknesses in the paradigms developed utilizing the public cryptosystem and the identity-based cryptosystem, respectively.

Numerous certificate-less paradigms have been put up to address these weaknesses since certificate-less cryptosystems provide the greatest answer to the problems. According to this paradigm, the user calculates the private key by using the partial private key, and a third party is responsible for calculating the users' partial private keys.

By using elliptic curve cryptography, the system's computing performance is increased. As a result, we have implemented the block chain-based certificate less authentication technique for the DT environment.

1.1.1 STATEMENT OF THE PROBLEM

There are many security risks involved in moving data from that physical assets to cloud servers. Adversaries may intercept sensitive data as it is being transmitted, including user data, performance metrics, and operational parameters. The problem of preserving secrecy and integrity increases as these data sets get larger and more interconnected. Unauthorized access may result in severe financial losses, interruptions to business operations, and reputational harm. Integrity Verification Integrity of data is crucial for DT applications. Decision-making processes may be impacted if the data that is transferred to the cloud is manipulated, as this could lead to inaccurate outcomes in the studies and simulations that follow. Ensuring data integrity throughout transmission and storage is crucial to guaranteeing stakeholders can rely on the information they are given.

Privacy Preservation Privacy issues arise because sensitive data is shared between users, cloud service providers, data owners, and other parties in cloud environments. Inadequate privacy protection measures may cause personal data to be disclosed without authorization, upsetting the law and undermining user confidence. methods in use today. An abundance of these systems suffers with: 1. User Anonymity: It's critical to preserve user identities while enabling essential interactions. 2. Mutual Authentication: Preventing impersonation attacks requires that the user the server be able to authenticate each other. 3. Protection Against Identity and Password Guessing Attacks: Many of the popular attack vectors that take use of weak passwords or compromised identities are not well-defended against in existing systems. The Need for a New Security Framework An inventive authentication strategy that ensures safe communication, data integrity, and privacy preservation in cloud-assisted DT contexts is desperately needed to meet these complex issues.

This system should allow for safe data sharing between stakeholders and be resistant to a variety of security risks, including impersonation attacks.

Data Integrity through Hash Values Using blockchain technology can be crucial to maintaining data integrity. Any data transported to the cloud can be represented as a distinct hash value by using hash algorithms. A blockchain can be used to record every transaction or piece of data, producing a permanent and unchangeable log. The hash value of the data can be calculated and recorded on blockchain when it is transferred from a physical asset to the cloud. By recalculating the hash and comparing it to the recorded value, this allows any party to confirm the accuracy of the data. Without a certificate Elliptic Curve Cryptography for Authentication Elliptic Curve Cryptography provides a very effective and safe substitute for conventional public key infrastructures in authentication. ECC that requires smaller key sizes to achieve the equivalent security levels compared to other cryptographic methods, which reduces computational overhead and enhances performance—an essential consideration in cloud environments. A certificate-less authentication protocol can be designed using ECC, enabling secure user authentication without the complexities of managing certificates. In such a system, users could authenticate themselves by generating unique keys derived from their identities, which can be shared with the cloud server. This approach alleviates the issues associated with key escrow and certificate management.

Proposed Authentication Protocol

Step 1: Registration During the initial registration phase, users generate a unique key pair (public and private keys) based on their identity. This key pair is then securely stored and registered with the cloud server without the need for certificates.

Step 2: Authentication Request When a user wants to exchange data or access their Digital Twin, they send an authentication request to the cloud server. The communication is digitally signed using user's the private key, and this request also includes their public key.

Step 3: Mutual Authentication The cloud server using the user's public key to confirm signature after obtaining request. The server the creates a challenge and delivers it back to user if the verification is successful.

After using their private key to sign this challenge, the user sends it back to the server.

Step4: Verification of Data Integrity Following user authentication, the cloud server compares the shared data's hash value to the value recorded on blockchain to confirm that data's integrity. The server can be sure that no tampering has occurred with the data if the values match.

Step 5: Sharing Secure Data When data integrity and mutual authentication are verified, users and the cloud server can safely share data. This encrypted channel guarantees

1.1.2 BRIEF DESCRIPTION OF THE PROJECT

The introduction of Digital Twin (DT) technology has completely changed how several industries handle simulation, real-time monitoring, and optimization of physical systems. By acting as a virtual duplicate of a real asset, a digital twin helps businesses forecast maintenance requirements, assess performance, and improve operational effectiveness. However, the safe sharing of data between users, devices, and cloud services is essential for the successful deployment of DTs. In order to address urgent problems of safe data exchange and integrity verification in DT settings, this project intends to design and implement the a privacy preserving authentication protocol that makes use of blockchain technology and certificateless cryptography.

The Significance of Digital Twins

Digital twins are becoming more and more common in a number of industries, such as Internet of Things (IoT), manufacturing, and healthcare. They help with production process the optimization and predictive the maintenance in the industrial industry. They provide individualized treatment regimens in the medical field by instantly assessing patient data. Digital twins allow for smart device management in the Internet of Things by continuously tracking operational parameters and performance. But as these systems become more integrated, there are more security issues pertaining to data integrity and sharing.

Data Sensitivity and Security Risks

Sensitive data, like as operational metrics, user data, and system performance indicators, are frequently transferred in DT contexts. There are serious security dangers associated with sending this data to cloud services, such as interception, unauthorized access, and data alteration. Serious repercussions from a breach could include monetary losses, business interruptions, and legal ramifications.

Inefficiencies of Traditional Authentication Mechanisms

Since current authentication methods rely on conventional Public Key Infrastructure (PKI), they frequently fail in DT contexts. The maintenance of certificates and key escrow in these systems is complicated. Furthermore, they are susceptible to a number of assaults, including password guessing and impersonation, which erodes the confidence that is necessary for safe data sharing.

The Proposed Solution

The goal of this project is to provide a safe framework that creates a privacy-preserving authentication procedure for Digital Twin environments by fusing blockchain technology with certificateless cryptography. The objectives of this solution are to improve data security, expedite the authentication procedure, and guarantee the accuracy of the data that is shared between stakeholders.

Blockchain for Data Integrity and Tamper-Proof Storage

1. The use of the blockchain technology is the fundamental component of the suggested remedy. The technology maker sure that the data is the unchangeable and verifiable by all network users by keeping hash values of the data produced by Digital Twins on a decentralized ledger. A distinct hash is assigned to each transaction or data entry in the blockchain, creating an open, unchangeable record that all stakeholders can review.
2. The hash value serves as the data's unique fingerprint. The associated hash is computed and recorded on the blockchain for each transmission of data. A distinct hash will be produced for each attempt to modify the data, making it simple for participants to confirm the accuracy of the data being transferred.
3. Due to its decentralized structure, blockchain is impervious to manipulation. Since data is stored among several nodes, it cannot be changed by a single party without the network's approval.

Implementation of the Authentication Protocol

The suggested authentication methodology is composed of multiple essential steps:
Users create a unique key pair, comprising of a public and private key, depending on their identification during the first registration step. Without the use of certificates, this key pair is safely kept and registered with the cloud service. New users or devices can be onboarded more quickly thanks to the simple and quick registration process. A user sends the authentication request to the cloud server in the order to share data or access their Digital Twin. Together with a digitally signed message created with their private key, this request also contains their public key. After that, the server confirms the signature to make sure the request is coming from an authorized user.

The cloud server creates a challenge and delivers it back to the user after successful verification. In order to answer this challenge, the user must sign it with their private key and send the signed answer back to the server. By ensuring that both parties can confirm one other's identities, this mutual authentication step guards against impersonation attempts. After authentication, the cloud server checks hash value to ensure the integrity of the data being transferred. Secure data sharing can begin after mutual authentication and data integrity have been confirmed. During this stage, authorized users can securely communicate while ensuring that their messages are shielded from prying eyes and manipulators. Through integration of certificateless cryptography and blockchain the technology, the suggested solution offers a strong security framework that can withstand a range of assaults, such as password guessing and impersonation.

The authentication procedure is more effective when ECC is used and certificate management complications are removed, which makes it appropriate for the dynamic and resource-constrained situations found in most Internet of Things devices. Because blockchain technology is decentralized, it can simply grow as additional users and devices are added while retaining security and integrity without requiring major infrastructure upgrades. By guaranteeing user anonymity and safeguarding sensitive data, the protocol builds confidence between network users and promotes a wider usage of digital twin technology.
While there are many potential advantages to the cross-industry integration of Digital Twin technology, there are also substantial security problems. In order to properly solve these issues, this project provides a privacy-preserving authentication protocol that makes use of

certificateless cryptography and blockchain technology. In DT contexts, the suggested method improves data integrity, guarantees secure communication, and cultivates stakeholder confidence. Putting strong security measures in place will be essential for enabling Digital Twins to reach their full potential and spurring innovation across industries as businesses continue to investigate their possibilities.

1.1.3 SOFTWARE AND HARDWARE SPECIFICATIONS

Hardware configuration:

➢ Pentium IV processor

➢ RAM of up to 4 GB (minimum)

➢ Hard drive of up to 20 GB

➢ Keyboard: Standard Windows keyboard

➢ Mouse: Two or three button mouse

➢ SVGA monitor

Software prerequisites:

➢ Windows XP as the operating system

➢ Front end: J2EE; Coding language: Java/J2EE (JSP, Servlet)

➢ MySQL at the back end

1.2 FUNCTIONAL AND NON -FUNCTIONAL REQUIREMENTS

➢ **Functional Requirements**

1. **User Registration**: Users must be able the to register with Key Generation Center (KGC) and generate a partial private key through the system. By assuring that users can start the cryptographic process without depending on conventional certificate-based techniques, this procedure creates a safe foundation for user authentication.

2. **User Authentication**: Users will need to combine their own secret information with the partial private key to authenticate themselves. By using two keys, the entire private key is protected even if the partial key is compromised, improving user security.

3. **Data Integrity**: All communications sent over the network should be guaranteed to

maintain their integrity by the system. To ensure that data has not been changed during transmission, methods like hash functions should be used. This is essential for preserving communication trust.

4. **Decentralized Verification**: The authentication procedure must allow for the decentralized verification of user identities and transactions using blockchain technology. As a result, there is less dependence on a single point of failure, increasing user confidence and system resilience.

5. **Session Management**: In order to enable secure session initiation and termination, the system must efficiently handle user sessions. This involves guarding against session hijacking and making sure user communications are private and secure.

6. **Key Management**: Cryptographic keys must be managed by users, who must be allowed to create, save, and remove them as needed. This feature is necessary to keep control over one's personal security credentials and to adjust to evolving security needs.

7. **Replay Protection**: The system has to incorporate safeguards against replay attacks, such the use of nonce values or timestamps. By preventing the fraudulent reuse of previously sent messages, these techniques help protect user sessions.

8. **Access Control**: Enforcing access control policies is necessary to guarantee that resources can only be accessed by authorized users. This keeps malevolent individuals from gaining illegal access and safeguards vital data and functionality.

9. **Secure Communication**: To maintain secrecy, all correspondence between users and the KGC or other parties needs to be encrypted. Maintaining user confidence requires safeguarding user information from interception or eavesdropping.

10. **Audit Logging**: For security monitoring, the system needs to keep track of all significant actions and authentication attempts. This logging feature facilitates regulatory compliance and allows for the identification of possible security breaches.

➢ Non-Functional Requirements

1. **Scalability:** To manage a big number of users and devices, the system needs to be built with efficient scaling in mind. This is especially crucial in settings where the number of users and devices might grow quickly, such as the Digital Twin and the Internet of Things. Scalability guarantees that as demand increases, system performance stays at its best.

2. **Performance:** The authentication procedure must be quick and effective, finishing in a fair amount of time. User happiness depends on prompt response times, particularly in busy settings where delays can irritate users and reduce their participation.

3. **Reliability:** High dependability is required of the system to guarantee constant availability with less downtime. In IoT and DT contexts, reliability is especially important for key applications and maintaining user trust and operational continuity.

4. **Usability**: Users should be able to easily navigate the registration and authentication processes thanks to a simple and user-friendly user interface. Good usability reduces the learning curve that comes with implementing new security policies and boosts user engagement.

5. **Interoperability:** To enable smooth integration with a range of apps and services, the system needs to be compatible with current protocols and technologies. Widespread adoption depends on this interoperability, which guarantees that customers can gain from improved security without requiring significant changes.

6. **Security:** The system must guard against known vulnerabilities by adhering to industry-standard security procedures. To preserve user trust and defend sensitive data from unwanted attacks, a strong security system is necessary.

7. **Maintainability:** It should be possible for developers to quickly address emerging dangers or introduce enhancements by using an architecture that is straightforward to update and maintain. Maintainability is essential to guaranteeing the security and long term health of a system.

8. **Privacy:** By protecting login credentials and personal information during the authentication process, the authentication protocol must guarantee user privacy. Protections against privacy boost users' trust in the system and promote wider adoption.

9. **Resource Efficiency:** When running on devices with limited resources, the system should minimize power consumption and computational overhead. This is especially important for Internet of Things devices, since they frequently have low processing and battery life.

10. **Compliance:** The system needs to abide by all applicable legal and regulatory requirements for cybersecurity and data protection. Respecting these rules promotes confidence among users and stakeholders in addition to ensuring legal compliance.

CHAPTER 2

LITERATURE SURVEY

Wang, H., X. Chen, Y. Dai, Zheng, Xie, & S. Zheng in 2017 [1] presented an overview of blockchain technology: Architecture, consensus, and future trends." IEEE International Congress on the Big Data, Big Data Congress, 2017. Zheng and colleagues conducted a comprehensive examination of blockchain technology and emphasized its applications in the cloud and IoT security. Blockchain ensures data integrity and immutability by maintaining tamper-proof transaction logs. However, scaling concerns are also brought up in this study, especially in large-scale IoT setups. The authors argue that while blockchain enhances data security, it is not meant to handle private user interactions or sensitive data, leaving room for more sophisticated privacy-preserving methods.

Yang, X., Huang, X., Wong, D. S., and Liu, Z. 2014 [2] presented an Certificateless two-party authenticated key agreement protocols. 2287–2295 in IEEE Transactions on Computers, 63(10).Liu et al. investigated certificateless cryptography as a potential remedy for identity-based cryptography (IBC) and classical public key infrastructure (PKI)'s key escrow issue. They provide a two-party authenticated key agreement technique that does away with certificate administration and improves computational performance. Though the protocol allays some privacy worries, it is not immune to some sophisticated assaults that are widespread in decentralized cloud environments, like impersonation and password guessing.

Moon, S. Y., Park, J. H., Chen, Y. P., and Sharma, V. 2020 [3] presented an Efficient privacy-preserving authentication scheme in blockchain-based healthcare IoT systems." 20(6), Sensors, 1–21.A blockchain-based authentication system was put up by Sharma et al. to safeguard IoT devices in medical settings. The plan guarantees data integrity and safe sharing between reliable entities by utilizing smart contracts and a public ledger. The authors do concede that although blockchain technology increases security, its use may still reveal user identification or other metadata, so privacy-preserving features like anonymity and unlikability are still necessary.

N. Koblitz. "Elliptic curve cryptosystems. 1987 [4] presented a Mathematics of Computation, 203-209.Elliptic curve cryptography (ECC), first proposed by Koblitz in his groundbreaking work, has grown to be a crucial tool for creating effective cryptographic protocols. Compared to conventional RSA-based systems, ECC provides higher security with smaller key sizes, which makes it appropriate for cloud and IoT contexts. Blockchain and ECC have been used in recent work, such as Jiang et al.'s (2019), to improve the computational efficiency of privacy-preserving authentication systems.

Kim, Y., Yoo, K., and Son, Y. 2021 [5] presented a Privacy-preserving three-factor authentication scheme for cloud-assisted IoT applications." 178, 102933, Journal of Network and the Computer Applications. Son et al. created a three-factor authentication the scheme specifically designed to protect privacy in Digital Twin contexts and optimized for cloud assisted Internet of Things applications. The approach increases security by using mutual verification and multi-factor authentication; nonetheless, flaws in anonymity and resistance to impersonation attacks were found in the study. For large-scale DT applications, the protocol's efficiency and scalability are further restricted by its dependence on conventional cryptosystems.He, D., Kumar, N., and Chilamkurti, N. 2017 [6] presented A private-protected, secure three-factor user authentication mechanism for wireless sensor networks." 2131-2139 in IEEE Transactions on Industrial Informatics, 12(6). He and colleagues examined the various authentication algorithms that are already in use and their drawbacks in relation to wireless sensor networks (WSNs). Their research demonstrated how most protocols are unable to offer forward secrecy, mutual authentication, or defense against brute force and impersonation assaults. While the three-factor technique improved security, their plan, like others, had difficulty becoming efficient and scalable without compromising privacy.

Weber, I., Xu, X., and Staples, M. 2019. [7] presented an Architecture for blockchain applications. Springer. In their discussion of blockchain's application to safe data sharing settings, Xu et al. focused on the technology's utility for data integrity verification. A visible and unchangeable record of transactions is made possible by the combination of blockchain technology with cloud computing; nonetheless, the authors contend that maintaining privacy is still a difficult task.

They suggest employing privacy-preserving methods to provide secure verification without jeopardizing user data, such as Merkle trees and zero-knowledge proofs. Enhancement and cryptanalysis of the three-factor user authentication system for smart grid applications. The flaws in the current three-factor authentication techniques used in smart grid environments are addressed in this research. The authors thoroughly cryptanalyze these schemes to find any vulnerabilities or possible dangers. They suggest an upgraded authentication technique that preserves usability while boosting security. Their conclusions imply that the suggested plan provides a strong substitute for protecting smart grid assets while reducing the dangers related to unwanted access.

Wazid, M., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. 2017. [8] presented an Safe three-factor user identification system for smart grids powered by renewable energy sources. This study introduces a brand-new three-factor user authentication system created especially for smart grid applications including renewable energy. The authors conclude that their method improves the overall integrity of smart grid operations while also securing user identification.

Shuai, M., Yu, N., Wang, H., & Xiong, L. (2019). [9] presented an anonymous authentication system with verifiable security for smart homes. The authors present an anonymous authentication system that balances strong security and user privacy for smart homes. The program uses cutting-edge cryptography to provide users with anonymity, which is essential for reducing privacy issues.

Chen, Y., Martinez, J., Castillejo, P., & López, L. 2019. [10] presented a bilinear map pairing based smart grid authentication system. This study suggests an authentication system for smart grid the communications security that is based on the bilinear map pairing.

The authors explain the underlying mathematical ideas in depth and show how their approach improves data transmission efficiency and security. The analysis of the suggested method shows that it can prevent standard attacks and enable smooth communication between smart grid components. According to the study's findings, the Pauth scheme represents a major advancement in the development of safe and dependable smart grid communication protocols.

CHAPTER 3
RESEARCH GAPS OF EXISTING METHODS

3.1 EXISTING SYSTEM

Grieves established the Digital Twin as the applied paradigm that underpins Product Lifecycle Management (PLM) with authority in 2002. NASA has been honing the idea since the 1960s, and in 2010 it was recognized with the title "digital twin." We start by summarizing some research that might provide light on the DT environment. Aheleroff et al. suggest a DT reference architecture for use in industrial settings. They integrated a DT as a server and focused on creating the industry 4.0 DT reference architectural paradigm. Lai et al. have suggested a safe and privacy-preserving approach for DT-based traffic control. The protocol uses a group signature with time-bound keys technique to offer data source authentication with effective member revocation and privacy protection throughout the data uploading phase. This provides assurance that data may be stored safely on cloud service providers after synchronization with its twin. To enable flexibility and successful data sharing, an additional attribute-based access control technique is added at the data sharing phase. Liu et al. have developed a cloud-based paradigm that uses DT technology to provide healthcare services. Their primary objective is to use digital twin technology into healthcare for senior citizens. As per their protocol, health data is generated by medical devices such as RFID cards, wristbands, and portable electrocardiograms, and is then collected on computers or mobile phones. The collected data are then sent to a remote cloud server using wireless networks, such as Ethernet, Wi-Fi, and mobile networks. Liu et al. employ a DT to construct a conceptual model for cloud based healthcare systems. Additionally, a lot of efforts have been made to combine DT with blockchain technology. Liu et al. have created a secure communication architecture based on blockchain technology to meet the management requirements of the Internet of Vehicles (IoV) driven by 6G DTs. When obtaining data, these systems are able to identify potential risks to vehicle nodes. Access control will become more accurate and efficient with the use of the blockchain. Huang et al. introduced a blockchain-based data management system for product digital twins.

Digital twin data may be shared, stored, accessed, and authenticated safely and quickly with the use of the blockchain. Blockchain is used by Sasikumar et al.'s protocol to combine DT with a distributed network for Industrial Internet of Things (IIoT) applications. This paper proposes a Proof of Authority (PoA) trust mechanism based on blockchain technology to provide high-quality IIoT services including data privacy and security. In a similar vein, Wang et al. proposed a blockchain-based sustainable DT management architecture for an Internet of Things that facilitates decentralized networks and effective data transfer.

Grover and colleagues brought to light the security flaws in the protocol created by Wazid and colleagues. Additionally, they suggested an improved procedure for smart grid situations, which the ProVerif tool was used to analyze. For smart homes, Kaur and Kumar developed a two-factor user authentication system. They demonstrated how their plan was more effective and outlined the Shuai et al. scheme's security flaws. Similarly, Wu et al. sheds light on the security holes in Chen et al.'s study. By contrasting their procedure with analogous previous protocols, they were able to demonstrate its superiority even further. Khatoon et al. in telecare medical information systems (TMIS). created a system for key agreement between servers and clients. They demonstrated how their protocol might more effectively guarantee a number of security features. Nevertheless, their technique is vulnerable to known session specific temporary information attack and provides no mechanism for data verification. Additionally, Sengupta et al. created an authentication framework using bilinear pairing and ECC for cyber-physical systems. Later cryptanalysis, however, revealed that this system was unable to reliably maintain user anonymity. While none of these processes deal with DT environments, they were all created for settings similar to DT. Two-factor-based protocols are unable to support forward secrecy and user anonymity features in an existing system.

Many are unable to resist password guessing and identity theft. Comparably, only a tiny percentage can be verified using the ROR Model and BAN logic, and some are vulnerable to user and server impersonation attacks. Furthermore, identity-based and conventional public cryptosystems are used in the design of the majority of authentication processes. These cryptosystems do, however, have certain weaknesses. The intricate certificate administration, storage, and key escrow problems are the weaknesses in the paradigms developed utilizing the public cryptosystem and the identity-based cryptosystem, respectively.

CHAPTER 4
PROPOSED MOTHODOLOGY

4.1 Proposed System

Certificateless cryptosystems provide a robust solution to the challenges associated with traditional cryptographic systems, such as certificate the management in Public Key Infrastructure (PKI) and key escrow issues in the Identity-Based Cryptography (IBC). In PKI, the use of certificates requires complex management, renewal, and validation processes, which become burdensome in large-scale environments like the Digital Twin (DT) or the Internet of Things (IoT). On the other hand, IBC, while eliminating the need for certificates, introduces a key escrow problem where a trusted authority has access to users' private keys, creating potential security risks.

To overcome these limitations, certificateless cryptography eliminates the need for certificates while also mitigating the key escrow issue. The responsibility for generating the complete private key lies with the user, who combines the partial private key with their own secret information. This dual process significantly reduces the risk of key compromise, as the KGC does not the have access to the user's full private key. This enhances security while simplifying key management.

To further enhance the performance of the certificateless system, Elliptic Curve Cryptography (ECC) is employed. ECC is known for its high level of security with smaller key sizes, leading to improved computational efficiency. ECC provides the same level of security as traditional cryptosystems like RSA but with much lower computational overhead, making it highly suitable for resource-constrained environments such as IoT devices and DT systems.

Given these advantages, the certificateless authentication scheme has been adopted for the DT environment in this work, leveraging blockchain technology. By incorporating blockchain, data integrity, transparency, and immutability are ensured, while the certificateless cryptosystem enables secure, efficient, and scalable user authentication.

Blockchain also adds an additional layer of security by enabling decentralized verification of transactions and data, further ensuring the integrity and privacy of communications in DT environments.

This combination of certificateless cryptography and blockchain results in a highly secure, efficient, and the privacy-preserving the authentication protocol for modern decentralized systems.

4.2 ADVANTAGES OF PROPOSED SYSTEM

- Through an open channel, transmitted communications can be replayed, inserted, eavesdropped on, modified, and deleted by a hostile attacker.
- "Power-analysis attacks" can be used by an adversary to get the secret credentials from a mobile device or smart card that has been stolen.
- The attacker may intercept or alter the smart device during the registration step. As a result, a malicious party can launch additional security attacks after obtaining the secret credentials from the device's memory.
- An adversary may be a malevolent insider or a registered user, or the opposite may occur.
- The adversary is able to execute offline password guessing and identity theft attacks concurrently. As a result, the adversary is able to simultaneously identify the authentic user’s identity and password.

4.3 FEASIBILITY STUDY

Finding that the system request is doable is a significant result of the preliminary research. Only if it is doable with the time and resources available will this be viable. The many scenarios that need to be examined include Practicality of Operation Operational feasibility The analysis of the system's potential that has to be developed. Operationally, this approach relieves the administrator of all his stress and assists him in efficiently monitoring the project's advancement. There is no doubt that this type of automation will save the time and energy that were previously used for manual labor. The analysis demonstrates the operational viability of the system. Economic Feasibility An evaluation of the financial case for a computer-based project is known as economic feasibility or cost-benefit analysis. The hardware project had a cheap cost since hardware was installed from the start and served several tasks.

Any number of workers connected to the organization's local area network (LAN) can utilize this tool at any time because it is network based.

The organization's current resources will be used to construct the virtual private network. Therefore, the proposal is financially viable. Technical Feasibility Technical feasibility, according to Roger S. Pressman, is the evaluation of the organization's technical resources. The company requires IBM compatible computers that are linked to the Intranet and Internet using a graphical web browser. The system is designed to operate in a platform-neutral environment. The system is developed using Java Server Pages, JavaScript, HTML, SQL Server, and WebLogic Server. The technical viability analysis has been completed. The system can be created using the current facilities and is technically possible.

CHAPTER 5
OBJECTIVES

The Privacy-Preserving Blockchain Security Protocol for Cloud-Based Digital Twin (DT) project delivers significant advancements in the fields of cybersecurity, data integrity, and operational efficiency. These outcomes reflect the project's objectives and its application in various industries, particularly in resource-constrained environments like IoT, manufacturing, and healthcare. Below is an extensive discussion of the project's key outcomes:

1. Enhanced Data Security

One of the primary outcomes of the project is the establishment of a highly secure communication framework for cloud-assisted Digital Twin environments. By leveraging certificateless cryptography and blockchain technology, the project provides robust protection against common cybersecurity threats such as:

- Eavesdropping and tampering during data transmission.
- Replay attacks, which involve the unauthorized reuse of valid data packets.
- Impersonation attacks, where malicious entities attempt to mimic legitimate users.

The project's multi-layered approach to authentication, encryption, and verification ensures that data exchanged between physical assets, cloud servers, and users remains secure and untampered.

2. Privacy Preservation

The project addresses growing privacy concerns by implementing privacy-preserving mechanisms, including certificateless cryptography. These mechanisms ensure:

- User anonymity, which protects individuals' identities during interactions.
- Untrace ability, making it difficult for adversaries to link transactions to specific users.
- Confidentiality, ensuring sensitive data is only accessible to authorized entities.

This robust privacy-preservation framework not only enhances user trust but also complies with stringent data protection regulations.

3. Strong Authentication Framework

The integration of a three-factor authentication framework results in a highly secure method of verifying user identity. This framework combines:

- A password (knowledge factor).
- A device or smart card (possession factor).
- Biometric data (inherence factor).

The project effectively mitigates risks such as password guessing, brute force attacks, and stolen credentials. It ensures that even if one factor is compromised, the remaining factors provide additional layers of defense.

4. Data Integrity and Transparency

The use of blockchain technology for recording data transactions achieves a significant outcome in ensuring data integrity. By storing hash values on a decentralized ledger, the system provides an immutable record of data exchanges. This allows all stakeholders to verify the authenticity of data by comparing hash values without requiring centralized trust.

Key benefits include:

- Protection against data manipulation.
- A transparent system for tracking changes and updates in real-time.
- Enhanced confidence in data accuracy and reliability.

5. Elimination of Certificate Management Complexity

Traditional Public Key Infrastructure (PKI) and Identity-Based Cryptography (IBC) are often hindered by challenges like certificate management and key escrow issues. The project overcomes these limitations through certificateless cryptography, which eliminates the need for certificate issuance, renewal, and revocation.

This approach simplifies:

- User onboarding processes.
- Key management tasks for administrators.
- Integration with existing systems.

By decentralizing key generation, users retain control over their private keys, which reduces vulnerabilities associated with centralized key authorities.

6. Improved Computational Efficiency

The project integrates Elliptic Curve Cryptography (ECC), which provides high levels of security with smaller key sizes compared to traditional cryptographic algorithms like RSA. The advantages of ECC include:

- Reduced computational overhead, making it ideal for resource-constrained environments such as IoT.
- Faster encryption and decryption processes.
- Lower energy consumption, which is critical for battery-operated devices.

This outcome ensures the scalability and sustainability of the security framework, even as the number of connected devices grows.

7. Decentralized Verification and Trust

The decentralized nature of blockchain ensures that no single entity controls the verification process, enhancing trust among stakeholders. By distributing data across multiple nodes, the system:

- Prevents unauthorized alterations or deletions.
- Ensures resilience against system failures or malicious actors.
- Facilitates transparent and secure collaboration between multiple parties.

Decentralized verification strengthens stakeholder confidence in the system’s reliability, making it suitable for critical applications in industries like healthcare and manufacturing.

8. Scalability and Flexibility

The project demonstrates significant improvements in scalability, ensuring the framework can handle large volumes of users and devices without compromising performance. This scalability is achieved through:

- Efficient key management, which reduces the complexity of onboarding new users or devices.
- The adoption of lightweight cryptographic algorithms, enabling smooth operations in environments with limited processing power.
- The ability to integrate with various industries and applications, such as predictive maintenance in manufacturing and remote monitoring in healthcare.
- The flexibility of the system allows it to adapt to changing requirements and scale seamlessly as organizational needs grow.

9. Support for Multi-Industry Applications

The project's outcomes extend beyond technical advancements, offering practical benefits across multiple industries:

- Healthcare: Secure remote patient monitoring, accurate diagnostics, and personalized treatment plans.
- Manufacturing: Enhanced production process optimization, real-time performance tracking, and predictive maintenance.
- Internet of Things (IoT): Reliable device authentication, secure data sharing, and operational transparency.
- Smart Cities: Efficient traffic management, energy optimization, and infrastructure monitoring.

These applications highlight the versatility of the project and its potential to drive innovation in diverse domains.

10. Enhanced User Trust and Adoption

By addressing critical concerns such as security, privacy, and usability, the project builds confidence among users and stakeholders. Key factors contributing to this outcome include:

- A user-friendly interface that simplifies the authentication process.
- Transparent operations facilitated by blockchain technology.
- Robust privacy measures that protect sensitive data.

This trust is crucial for encouraging the adoption of Digital Twin technology across industries, paving the way for widespread integration and innovation.

11. Robustness Against Cybersecurity Threats

The project delivers a system capable of withstanding a wide range of cybersecurity threats, including:

- Replay attacks, where attackers attempt to reuse valid data packets.
- Man-in-the-middle attacks, which involve intercepting and altering communications between users and servers.
- Offline password guessing attacks, where attackers use computational power to guess credentials.

The project's comprehensive threat model and countermeasures ensure a secure operating environment for users and devices.

12. Regulatory Compliance

The system aligns with industry standards and regulatory requirements for data protection and cybersecurity. Compliance with frameworks such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) ensures the solution is viable for use in highly regulated industries like healthcare and finance.

13. Encouraging Innovation

The successful implementation of this project fosters an environment for future innovation by addressing foundational security and operational challenges in Digital Twin environments. It provides a framework for exploring advanced applications, such as:

- Predictive analytics for maintenance and operations.
- Real-time simulations for decision-making.
- Integration with emerging technologies like 5G and artificial intelligence.

14. Cost Efficiency and Economic Viability

The project achieves cost savings by reducing the complexity of certificate management and minimizing computational overhead. The use of ECC further reduces hardware requirements, making the solution economically viable for large-scale deployments.

15. Future Scope for Optimization

The project's design and implementation provide a strong foundation for future enhancements. Potential areas of improvement include:

- Message compression: Reducing the size of data transmitted during authentication to improve efficiency.
- Asynchronous communication: Allowing non-blocking interactions to manage traffic loads more effectively.
- Batch authentication: Enabling simultaneous verification of multiple users or devices to enhance system throughput.
- Adaptive algorithms: Dynamically adjusting computational requirements based on network conditions and device capabilities.

The outcomes of this project demonstrate its effectiveness in addressing the complex challenges of securing cloud-assisted Digital Twin environments. By combining privacy-preserving cryptographic methods with blockchain technology, the project achieves significant advancements in data security, privacy, scalability, and operational efficiency. These outcomes position the system as a critical enabler for the adoption and growth of Digital Twin technology across industries, driving innovation and improving the efficiency of modern interconnected systems.

CHAPTER 6
SYSTEM DESIGN & IMPLEMENTATION

Building large software or hardware systems requires an organized process called system design and development, which makes sure the systems fulfill functional, performance, and reliability specifications. This is a high-level summary of the procedure.

6.1 HIGH LEVEL DESIGN

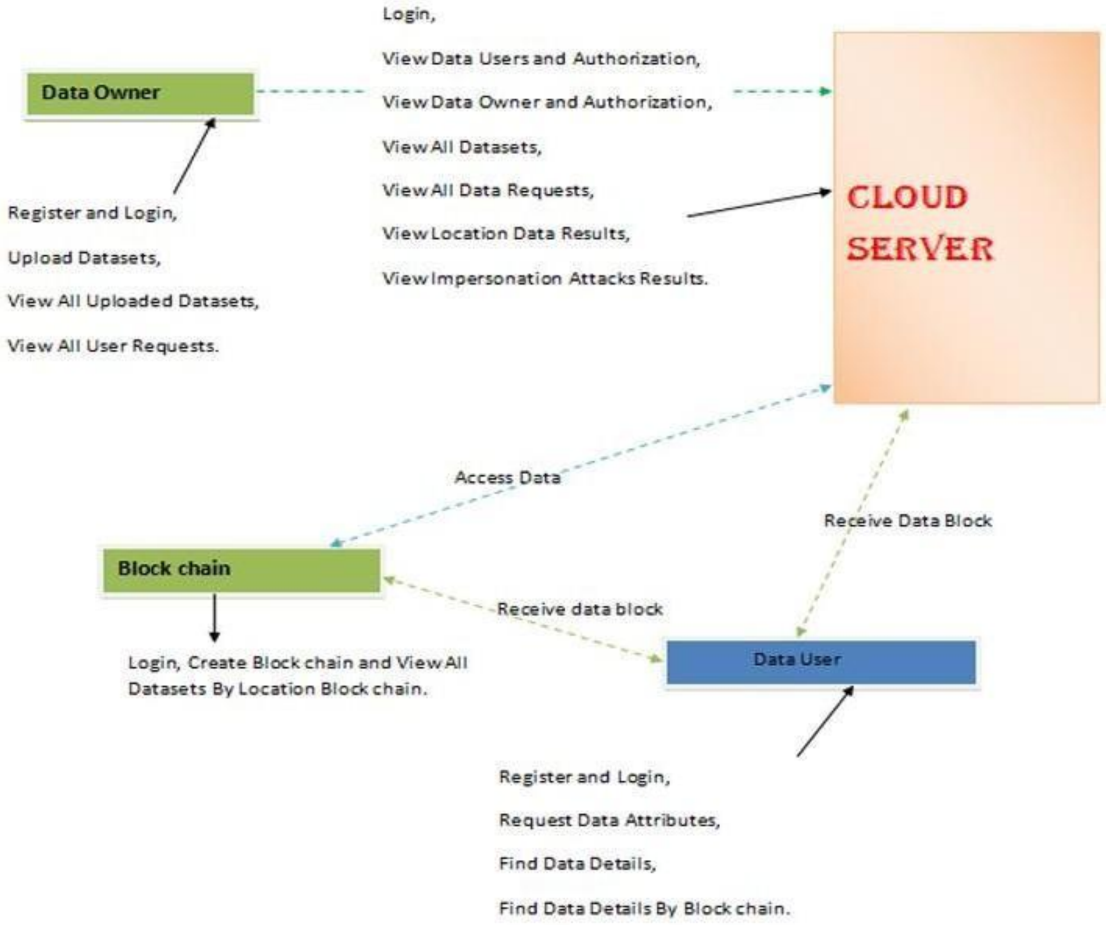

Login,
View Data Users and Authorization,
View Data Owner and Authorization,
View All Datasets,
View All Data Requests,
View Location Data Results,
View Impersonation Attacks Results.
Data Owner
Register and Login,
Upload Datasets,
View All Uploaded Datasets,
View All User Requests.
CLOUD SERVER
Access Data
Receive Data Block
Block chain
Receive data block
Login, Create Block chain and View All Datasets By Location Block chain.
Data User
Register and Login,
Request Data Attributes,
Find Data Details,
Find Data Details By Block chain.

Fig 6.1 High Level Design

6.2 DATAFLOW DIAGRAM

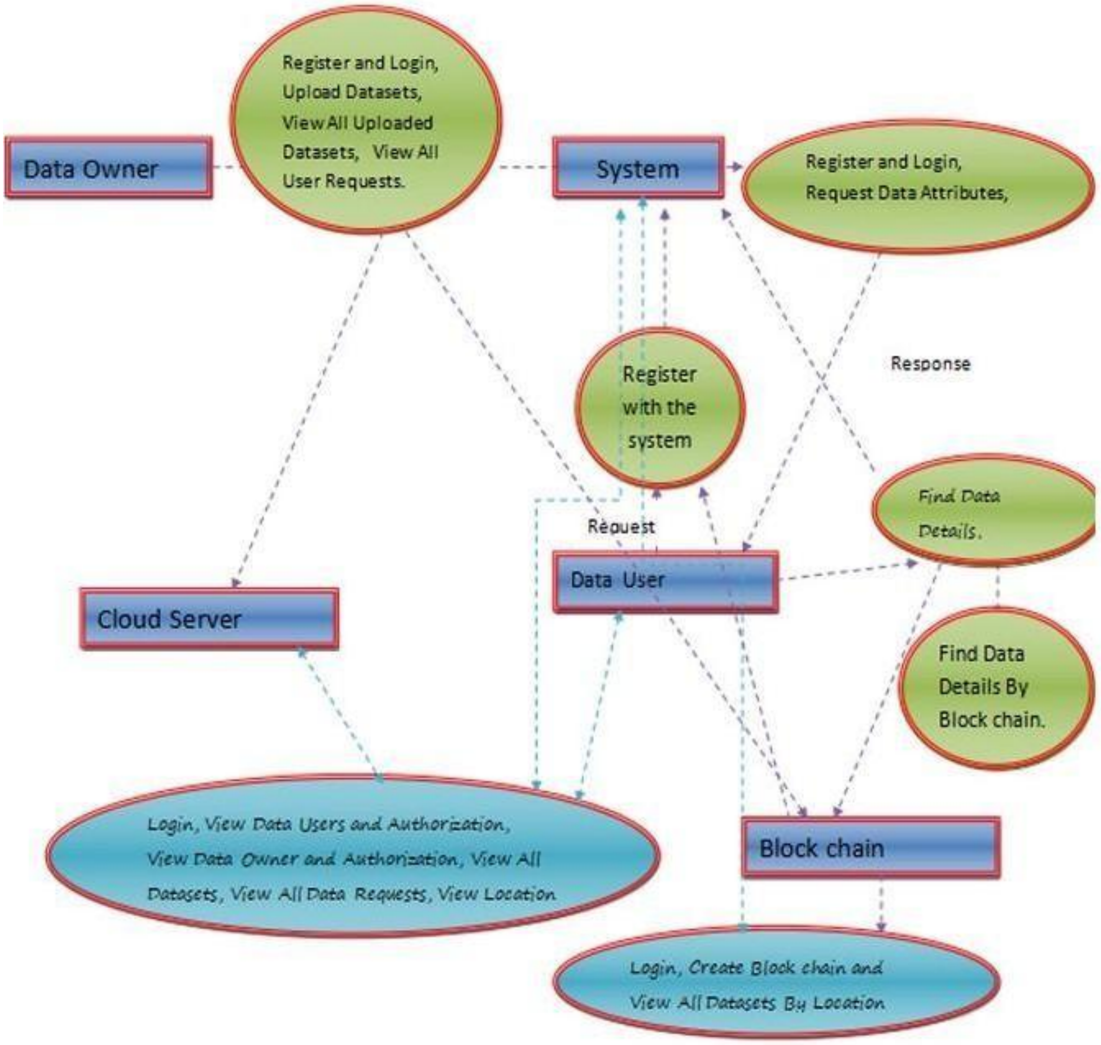

Data Owner
Register and Login, Upload Datasets, View All Uploaded Datasets, View All User Requests.
System
Register and Login, Request Data Attributes,
Register with the system
Response
Find Data Details.
Request
Data User
Cloud Server
Find Data Details By Block chain.
Login, View Data Users and Authorization, View Data Owner and Authorization, View All Datasets, View All Data Requests, View Location
Block chain
Login, Create Block chain and View All Datasets By Location

Fig 6.2 Data Flow Diagram

A data flow diagram is the visual representation of how data moves through a system (DFD). Because it makes data storage, external entities, and data flow between processes simpler to perceive.

6.3 USE CASE DIAGRAM

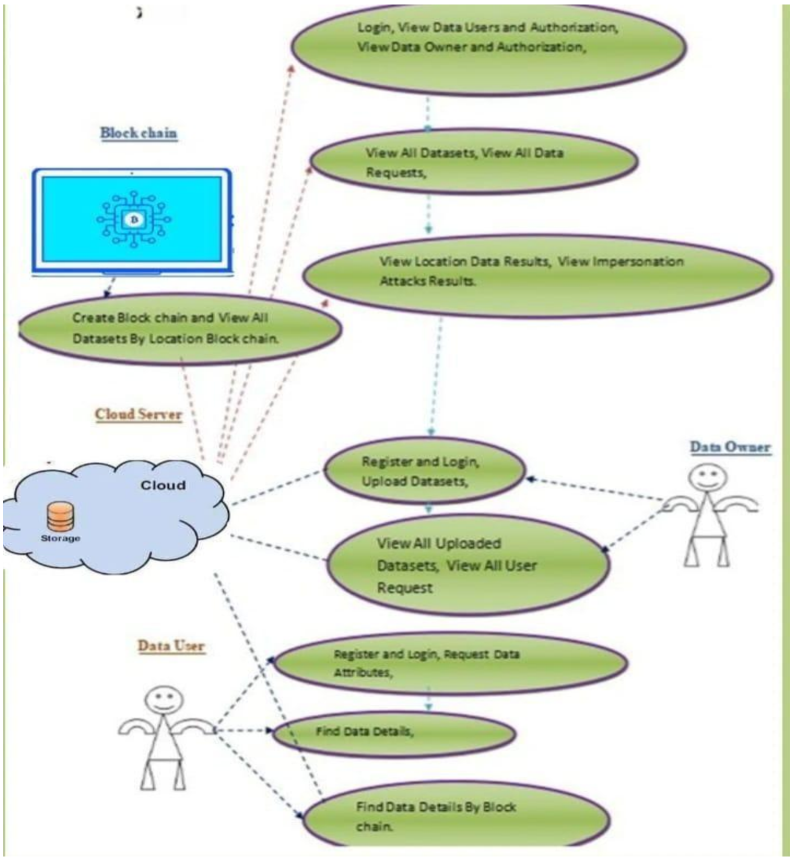

Login, View Data Users and Authorization, View Data Owner and Authorization,
Block chain
View All Datasets, View All Data Requests,
View Location Data Results, View Impersonation Attacks Results.
Create Block chain and View All Datasets By Location Block chain.
Cloud Server
Data Owner
Register and Login, Upload Datasets,
Cloud
Storage
View All Uploaded Datasets, View All User Request
Data User
Register and Login, Request Data Attributes,
Find Data Details,
Find Data Details By Block chain.

Fig 6.3 Use Case Diagram

Use case diagram of the interaction between the four entities: Blockchain, Cloud Server, Data Owner, and Data User in a data-sharing system.

•Blockchain: It manages authentication, datasets, data requests, location-based data results, and impersonation detection. It also supports the creation and viewing of datasets by location.

•Cloud Server: It serves as a center for user registration and login, uploading datasets, and allows data owners to view the uploaded datasets and user requests.

•Data Owner: Registers, uploads datasets, and handles user access requests.

•Data User: Registers, requests data attributes, and retrieves data via the blockchain.

6.4 SEQUENCE DIAGRAM

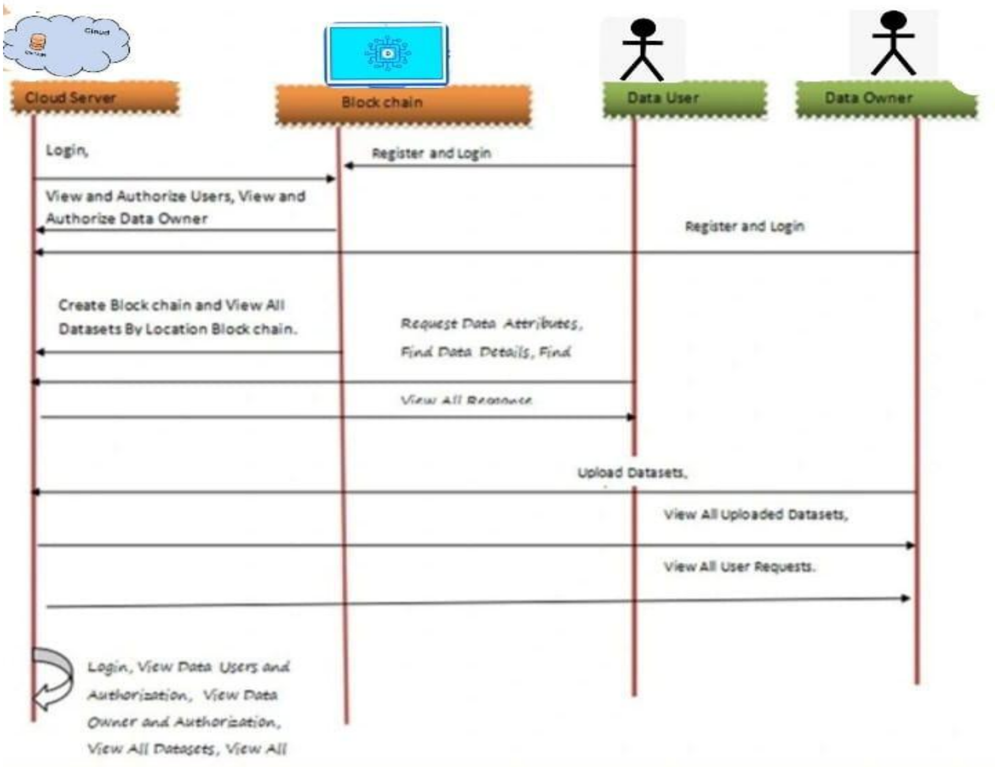

Cloud
Cloud Server
Block chain
Data User
Data Owner
Login,
Register and Login
View and Authorize Users, View and Authorize Data Owner
Register and Login
Create Block chain and View All Datasets By Location Block chain.
Request Data Attributes, Find Data Details, Find
View All Response
Upload Datasets,
View All Uploaded Datasets,
View All User Requests.
Login, View Data Users and Authorization, View Data Owner and Authorization, View All Datasets, View All

Fig 6.4 Sequence Diagram

This is a sequence diagram that shows interactions between Cloud Server, Blockchain, Data User, and Data Owner in a data-sharing system.

- Cloud Server:

Handles login, user authorization, and dataset access, Creates and manages blockchain datasets.

- Blockchain:

Supports data attribute requests, retrieving data details, and responding to user queries.

- Data User:

Registers, logs in, and requests data attributes or details.

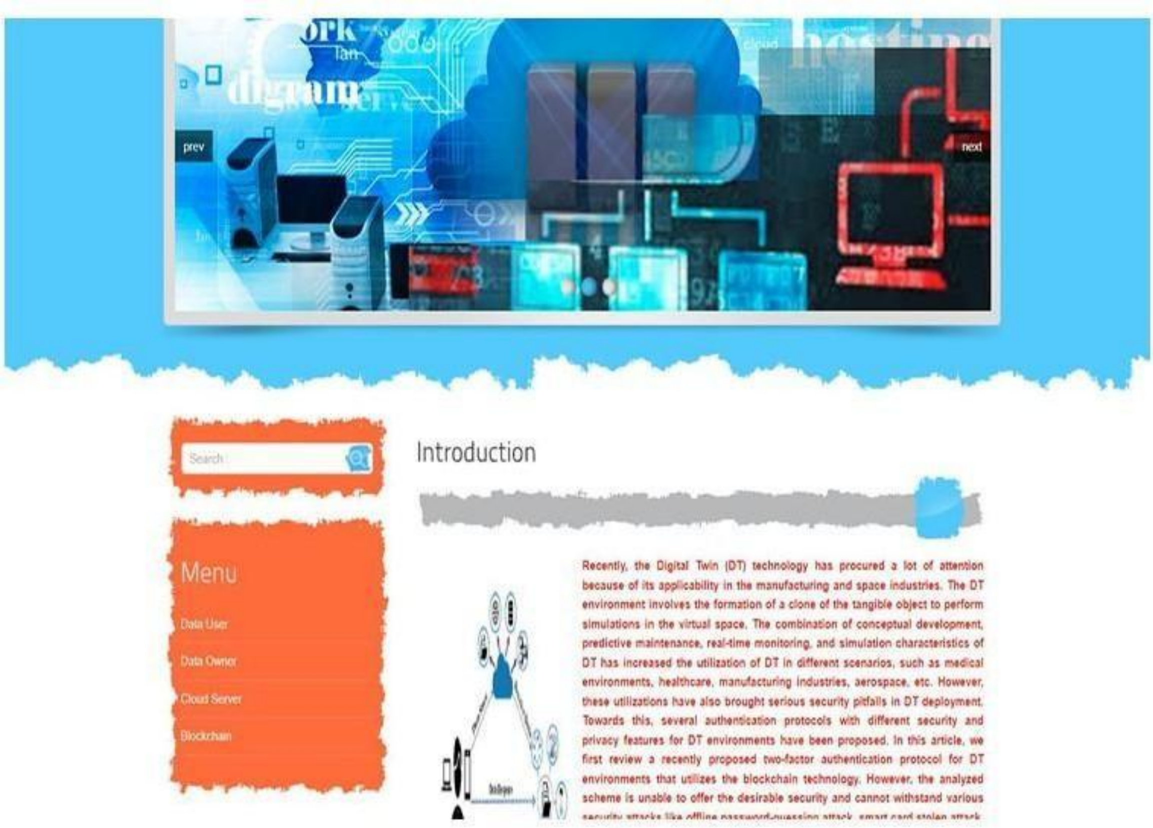
- Data Owner:

Registers and uploads datasets, view uploaded datasets and handles user requests.

This diagram illustrates step-by-step operations and responsibilities spread over entities while sharing data efficiently and securely.

6.5 INPUT /OUTPUT INTERFACE DESIGN

6.5.1 HOME PAGE

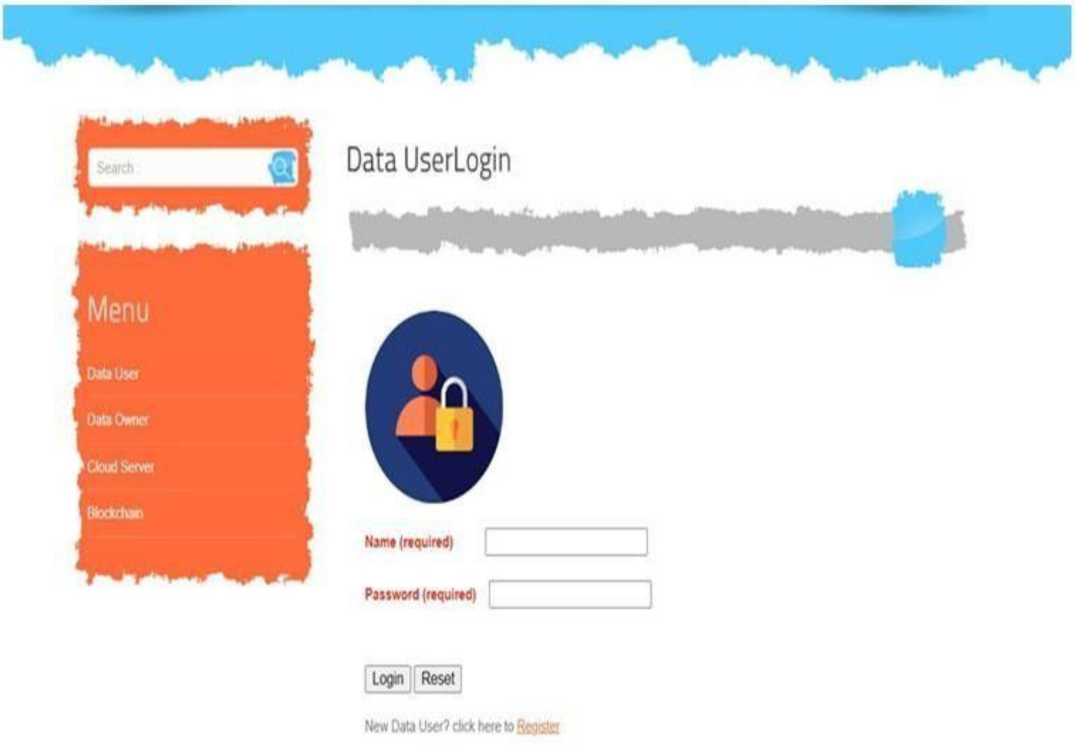


Recently, the Digital Twin (DT) technology has procured a lot of attention because of its applicability in the manufacturing and space industries. The DT environment involves the formation of a clone of the tangible object to perform simulations in the virtual space. The combination of conceptual development, predictive maintenance, real-time monitoring, and simulation characteristics of DT has increased the utilization of DT in different scenarios, such as medical environments, healthcare, manufacturing industries, aerospace, etc. However, these utilizations have also brought serious security pitfalls in DT deployment. Towards this, several authentication protocols with different security and privacy features for DT environments have been proposed. In this article, we first review a recently proposed two-factor authentication protocol for DT environments that utilizes the blockchain technology. However, the analyzed scheme is unable to offer the desirable security and cannot withstand various security attacks like offline password-guessing attack, smart card stolen attack,

Fig 6.5.1 Home Page

This interface is the introductory page of a system focused on Digital Twin (DT) technology

6.5.2 DATA USER LOGIN



Data UserLogin

Name (required)

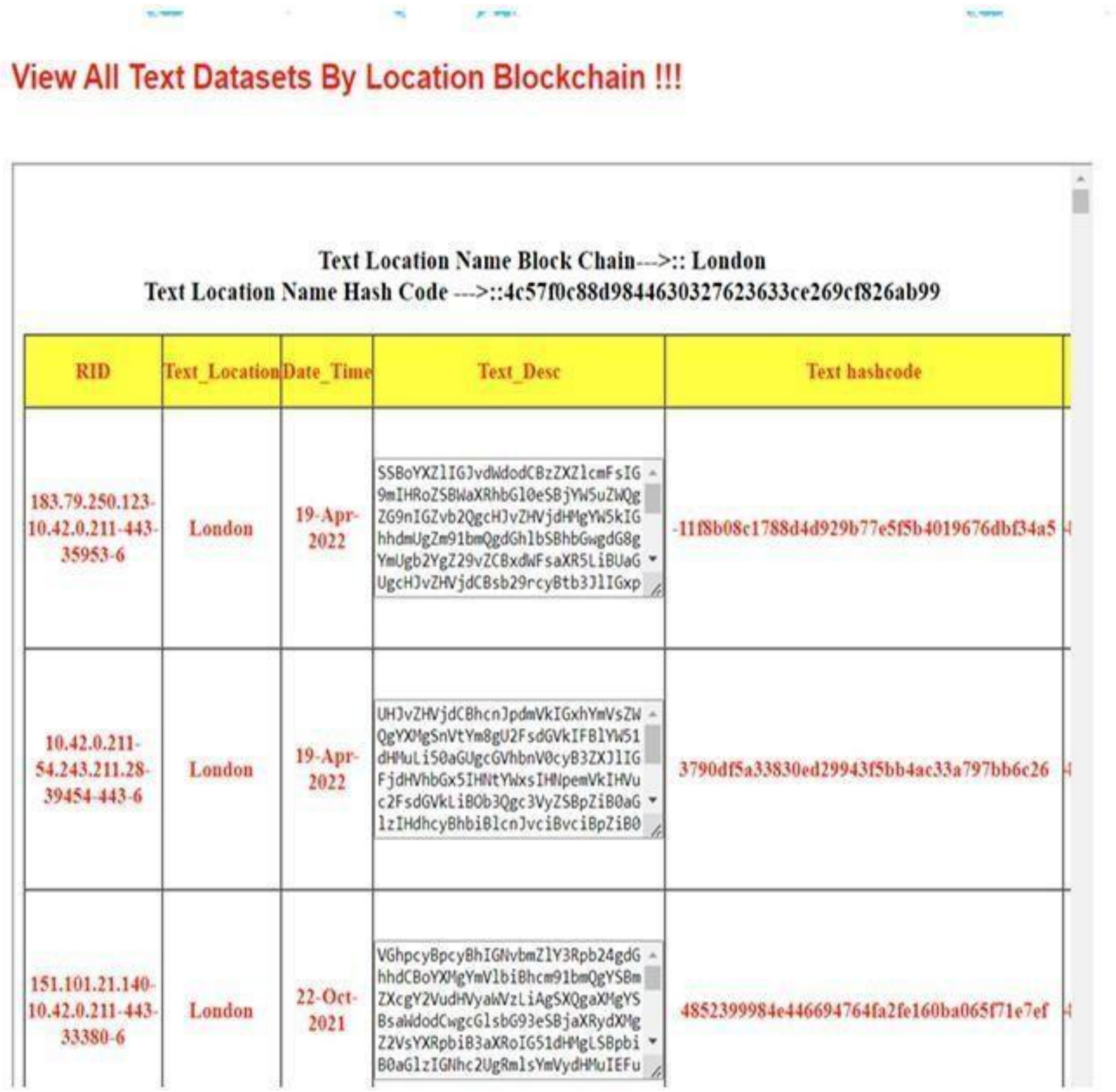
Password (required)

New Data User? click here to Register

Fig 6.5.2 Data User Login

This interface is the data user login ,through which users can login by entering credentials.

6.5.3 DATASET VIEW BY LOCATION



View All Text Datasets By Location Blockchain !!!

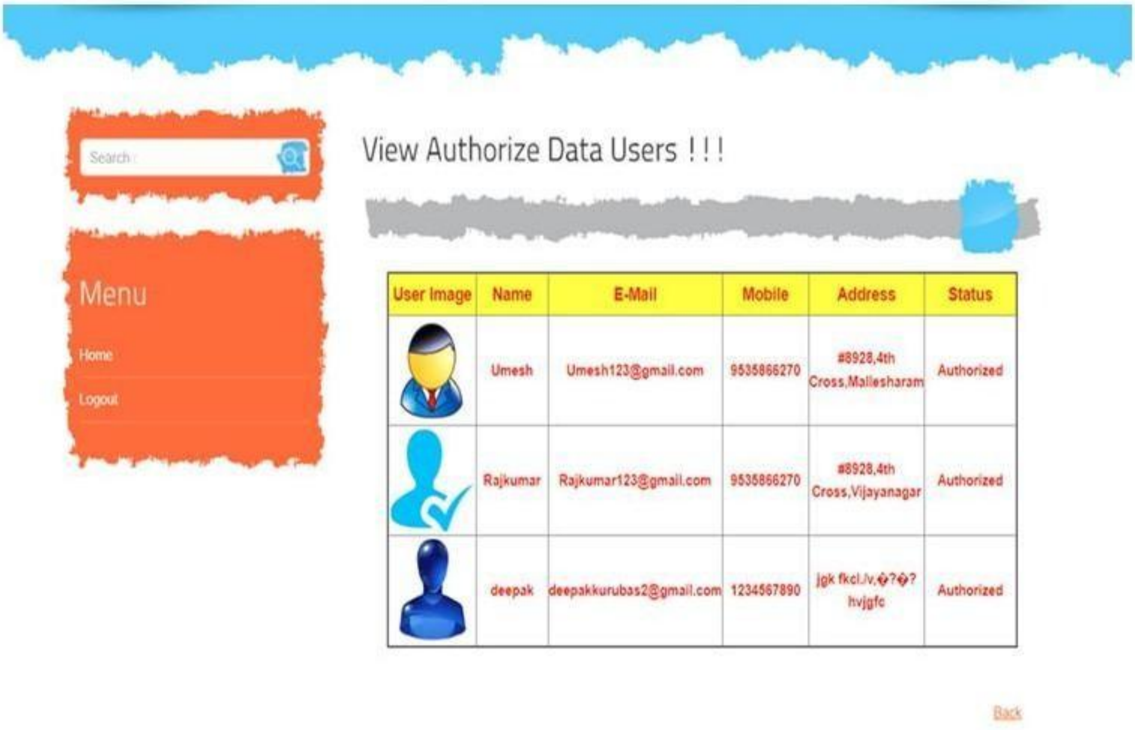
Text Location Name Block Chain--->:: London
Text Location Name Hash Code --->::4c57f0c88d9844630327623633ce269cf826ab99

RID	Text_Location	Date_Time	Text_Desc	Text hashcode
183.79.250.123-10.42.0.211-443-35953-6	London	19-Apr-2022	SSBoYXZlIGJvdWdodCBzZXZlcmFsIG 9mIHRoZSBWaXRhbGl0eSBjYW5uZWQg ZG9nIGZvb2QgcHJvZHVjdHMgYW5kIG hhdmUgZm91bmQgdGhlbSBhbGwgdG8g YmUgb2YgZ29vZCBxdWFsaXR5LiBUaG UgcHJvZHVjdCBsb29rcyBtb3JlIGxp	-11f8b08c1788d4d929b77e5f5b4019676dbf34a5
10.42.0.211-54.243.211.28-39454-443-6	London	19-Apr-2022	UHJvZHVjdCBhcnJpdmVkIGxhYmVsZW QgYXMgSnVtYm8gU2FsdGVkIFBlYW51 dHMuLi50aGUgcGVhbnV0cyB3ZXJlIG FjdHVhbGx5IHNtYWxsIHNpemVkIHVu c2FsdGVkLiBOb3Qgc3VyZSBpZiB0aG lzIHdhcyBhbiBlcnJvciBvciBpZiB0	3790df5a33830ed29943f5bb4ac33a797bb6c26
151.101.21.140-10.42.0.211-443-33380-6	London	22-Oct-2021	VGhpcyBpcyBhIGNvbmZlY3Rpb24gdG hhdCBoYXMgYmVlbiBhcm91bmQgYSBm ZXcgY2VudHVyaWVzLiAgSXQgaXMgYS BsaWdodCwgcGlsbG93eSBjaXRydXMg Z2VsYXRpbiB3aXRoIG51dHMgLSBpbi B0aGlzIGNhc2UgRmlsYmVydHMuIEFu	4852399984e446694764fa2fe160ba065f71e7ef

Fig 6.5.3 Data set view by location

This interface displays a table of text datasets stored on a blockchain, organized by location.

6.5.4 AUTHORIZED USERS



View Authorize Data Users ! ! !

User Image	Name	E-Mail	Mobile	Address	Status
	Umesh	Umesh123@gmail.com	9535866270	#8928,4th Cross,Mallesharam	Authorized
	Rajkumar	Rajkumar123@gmail.com	9535866270	#8928,4th Cross,Vijayanagar	Authorized
	deepak	deepakkurubas2@gmail.com	1234567890	jgk fkcl./v,�?�? hvjgfc	Authorized

Fig 6.5.4 Authorized Users

This interface displays a dashboard for viewing authorized data users in a data-sharing system.

6.6 MODULE DESCRIPTION

1. Owner of Data

He enters his or her login credentials in this module. Following their login, the data owner can upload datasets, see all uploaded datasets, and view all user requests, among other actions.

2. User of Data

He enters his or her login credentials in this module. The user may do many tasks after logging in, including requesting data attributes, finding data details, and finding data details by block chain.

3. Block chain

The block chain in this module may do the following functions: Create Block chain, View All Datasets by Location Block chain, and Login.

4. Cloud Server

In addition to acting as a server for data storage, the cloud server may perform the following functions: view data users and authorization, view data owners and authorization, View Location Data Results, View All Datasets, View All Data Requests, and View Results of Impersonation Attacks.

CHAPTER-7

TIMELINE FOR EXECUTION OF PROJECT (GANTT CHART)

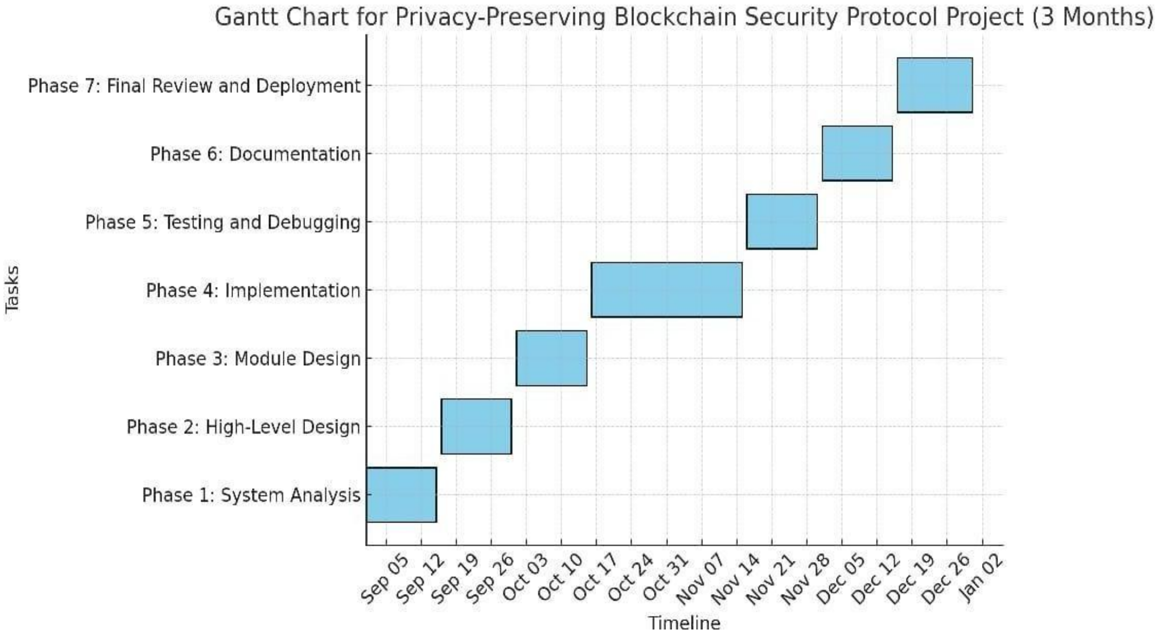


Fig 7.1 Gantt Chart

The Gantt chart outlines the "Privacy-Preserving Blockchain Security Protocol Project" timeline over three months, divided into seven phases:

1. System Analysis (Sep 5 - Sep 18): Assessing system requirements.
2. High-Level Design (Sep 19 - Oct 2): Developing the overall architecture and planning components.
3. Module Design (Oct 3 - Oct 16): Creating detailed designs for each module.
4. Implementation (Oct 17 - Nov 13): Coding and developing the security protocol.
5. Testing and Debugging (Nov 14 - Dec 4): Ensuring functionality and fixing issues.
6. Documentation (Dec 5 - Dec 18): Preparing technical and functional documentation.
7. Final Review and Deployment (Dec 19 - Jan 2): Finalizing and deploying the protocol.

CHAPTER 8
OUTCOMES

The Privacy-Preserving Blockchain Security Protocol for Cloud-Based Digital Twin (DT) project delivers significant advancements in the fields of cybersecurity, data integrity, and operational efficiency. These outcomes reflect the project's objectives and its application in various industries, particularly in resource-constrained environments like IoT, manufacturing, and healthcare. Below is an extensive discussion of the project's key outcomes:

1. Enhanced Data Security

One of the primary outcomes of the project is the establishment of a highly secure communication framework for cloud-assisted Digital Twin environments. By leveraging certificateless cryptography and blockchain technology, the project provides robust protection against common cybersecurity threats such as:

- Eavesdropping and tampering during data transmission.
- Replay attacks, which involve the unauthorized reuse of valid data packets.
- Impersonation attacks, where malicious entities attempt to mimic legitimate users.

The project's multi-layered approach to authentication, encryption, and verification ensures that data exchanged between physical assets, cloud servers, and users remains secure and untampered.

2. Privacy Preservation

The project addresses growing privacy concerns by implementing privacy-preserving mechanisms, including certificateless cryptography. These mechanisms ensure:

- User anonymity, which protects individuals’ identities during interactions.
- Untrace ability, making it difficult for adversaries to link transactions to specific users.
- Confidentiality, ensuring sensitive data is only accessible to authorized entities.

This robust privacy-preservation framework not only enhances user trust but also complies with stringent data protection regulations.

3. Strong Authentication Framework

The integration of a three-factor authentication framework results in a highly secure method of verifying user identity. This framework combines:

- A password (knowledge factor).
- A device or smart card (possession factor).
- Biometric data (inherence factor).

The project effectively mitigates risks such as password guessing, brute force attacks, and stolen credentials. It ensures that even if one factor is compromised, the remaining factors provide additional layers of defense.

4. Data Integrity and Transparency

The use of blockchain technology for recording data transactions achieves a significant outcome in ensuring data integrity. By storing hash values on a decentralized ledger, the system provides an immutable record of data exchanges. This allows all stakeholders to verify the authenticity of data by comparing hash values without requiring centralized trust.

Key benefits include:

- Protection against data manipulation.
- A transparent system for tracking changes and updates in real-time.
- Enhanced confidence in data accuracy and reliability.

5. Elimination of Certificate Management Complexity

Traditional Public Key Infrastructure (PKI) and Identity-Based Cryptography (IBC) are often hindered by challenges like certificate management and key escrow issues. The project overcomes these limitations through *certificateless cryptography*, which eliminates the need for certificate issuance, renewal, and revocation.

This approach simplifies:

- User onboarding processes.
- Key management tasks for administrators.
- Integration with existing systems.

By decentralizing key generation, users retain control over their private keys, which reduces vulnerabilities associated with centralized key authorities.

6. Improved Computational Efficiency

The project integrates Elliptic Curve Cryptography (ECC), which provides high levels of security with smaller key sizes compared to traditional cryptographic algorithms like RSA. The advantages of ECC include:

- Reduced computational overhead, making it ideal for resource-constrained environments such as IoT.
- Faster encryption and decryption processes.
- Lower energy consumption, which is critical for battery-operated devices.

This outcome ensures the scalability and sustainability of the security framework, even as the number of connected devices grows.

7. Decentralized Verification and Trust

The decentralized nature of blockchain ensures that no single entity controls the verification process, enhancing trust among stakeholders. By distributing data across multiple nodes, the system:

- Prevents unauthorized alterations or deletions.
- Ensures resilience against system failures or malicious actors.
- Facilitates transparent and secure collaboration between multiple parties.

Decentralized verification strengthens stakeholder confidence in the system's reliability, making it suitable for critical applications in industries like healthcare and manufacturing.

8. Scalability and Flexibility

The project demonstrates significant improvements in scalability, ensuring the framework can handle large volumes of users and devices without compromising performance. This scalability is achieved through:

- Efficient key management, which reduces the complexity of onboarding new users or devices.
- The adoption of lightweight cryptographic algorithms, enabling smooth operations in environments with limited processing power.
- The ability to integrate with various industries and applications, such as predictive maintenance in manufacturing and remote monitoring in healthcare. The flexibility of the system allows it to adapt to changing requirements and scale seamlessly as organizational needs grow.

9. Support for Multi-Industry Applications

The project's outcomes extend beyond technical advancements, offering practical benefits across multiple industries:

- Healthcare: Secure remote patient monitoring, accurate diagnostics, and personalized treatment plans.
- Manufacturing: Enhanced production process optimization, real-time performance tracking, and predictive maintenance.
- Internet of Things (IoT): Reliable device authentication, secure data sharing, and operational transparency.
- Smart Cities: Efficient traffic management, energy optimization, and infrastructure monitoring.
- These applications highlight the versatility of the project and its potential to drive innovation in diverse domains.

10. Enhanced User Trust and Adoption

By addressing critical concerns such as security, privacy, and usability, the project builds confidence among users and stakeholders. Key factors contributing to this outcome include:

- A user-friendly interface that simplifies the authentication process.
- Transparent operations facilitated by blockchain technology.
- Robust privacy measures that protect sensitive data.

This trust is crucial for encouraging the adoption of Digital Twin technology across industries, paving the way for widespread integration and innovation.

11. Robustness Against Cybersecurity Threats

The project delivers a system capable of withstanding a wide range of cybersecurity threats, including:

- Replay attacks, where attackers attempt to reuse valid data packets.
- Man-in-the-middle attacks, which involve intercepting and altering communications between users and servers.
- Offline password guessing attacks, where attackers use computational power to guess credentials.

The project's comprehensive threat model and countermeasures ensure a secure operating environment for users and devices.

12. Regulatory Compliance

The system aligns with industry standards and regulatory requirements for data protection and cybersecurity. Compliance with frameworks such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) ensures the solution is viable for use in highly regulated industries like healthcare and finance.

13. Encouraging Innovation

The successful implementation of this project fosters an environment for future innovation by addressing foundational security and operational challenges in Digital Twin environments.
It provides a framework for exploring advanced applications, such as:

- Predictive analytics for maintenance and operations.
- Real-time simulations for decision-making.
- Integration with emerging technologies like 5G and artificial intelligence.

14. Cost Efficiency and Economic Viability

The project achieves cost savings by reducing the complexity of certificate management and minimizing computational overhead. The use of ECC further reduces hardware requirements, making the solution economically viable for large-scale deployments.

15. Future Scope for Optimization

The project's design and implementation provide a strong foundation for future enhancements. Potential areas of improvement include:

- Message compression: Reducing the size of data transmitted during authentication to improve efficiency.
- Asynchronous communication: Allowing non-blocking interactions to manage traffic loads more effectively.
- Batch authentication: Enabling simultaneous verification of multiple users or devices to enhance system throughput.
- Adaptive algorithms: Dynamically adjusting computational requirements based on network conditions and device capabilities.

CHAPTER 9

RESULTS AND DISCUSSIONS

1. Enhanced Security Framework

- **Results:**

The project successfully implemented a robust security framework combining blockchain technology and certificateless cryptography. This framework ensures:

- Protection against common security threats, such as eavesdropping, tampering, replay attacks, and impersonation.

- Secure data transmission between physical systems, cloud servers, and users.

- **Discussion:**

Traditional Public Key Infrastructure (PKI) systems often face challenges such as certificate management complexities and key escrow vulnerabilities. By employing certificateless cryptography, the project eliminates these issues, enabling users to independently generate private keys. This decentralization reduces the risks associated with centralized control over cryptographic credentials.

The inclusion of elliptic curve cryptography (ECC) further strengthens the security framework, offering high levels of protection with minimal computational overhead. These advancements position the system as a viable solution for resource-constrained environments like IoT and DT applications.

2. Data Integrity and Immutability

- **Results:**

The integration of blockchain technology ensures data integrity by recording hash values for all data transactions on a decentralized ledger. Key outcomes include:

- An immutable record of data exchanges, preventing tampering and unauthorized modifications.

- Simplified verification processes, allowing stakeholders to confirm the authenticity of data by comparing hash values.

- **Discussion:**

Data integrity is critical for the reliability of simulations and decision-making in DT environments.

The use of blockchain technology creates a transparent system where all data changes are logged and verifiable. This eliminates the reliance on centralized authorities for data verification, reducing the risk of single points of failure.

By employing a Merkle hash tree, the system enables efficient and scalable verification, ensuring that even large datasets can be validated with minimal computational effort.

3. Privacy Preservation

- **Results:**

The project achieved significant advancements in preserving user privacy through:

- Certificateless cryptography, ensuring anonymity and untrace ability.

- Strong encryption protocols that protect sensitive data during transmission and storage.

- **Discussion:**

Privacy is a major concern in cloud-based systems, especially when dealing with sensitive data like operational metrics and user identities. The project addresses these concerns by implementing privacy-preserving techniques that ensure data confidentiality while allowing secure interactions.

This approach not only builds user trust but also ensures compliance with regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). By balancing security and privacy, the project sets a new standard for secure data sharing in DT environments.

4. Efficient Authentication Mechanism

- **Results:**

The implementation of a three-factor authentication framework delivers:

- Enhanced security through the combination of knowledge (password), possession (device), and inherence (biometric) factors.

- Resistance to attacks such as password guessing, brute force, and impersonation.

- **Discussion:**

Traditional authentication methods often rely on single or two-factor mechanisms, which are vulnerable to various attacks. The project’s three-factor authentication approach provides an additional layer of security, making it significantly more difficult for attackers to compromise the system.

By leveraging certificateless cryptography, the system eliminates the need for certificates, reducing administrative overhead while maintaining high levels of security. This framework is particularly beneficial for applications in healthcare, manufacturing, and IoT, where secure authentication is critical.

5. Scalability and Performance Optimization

- **Results:**

The project demonstrates excellent scalability and performance, with key achievements including:

- Reduced computational overhead through the use of ECC, which requires smaller key sizes compared to traditional algorithms.
- Efficient data processing and transmission, ensuring smooth operations even in resource-constrained environments.

- **Discussion:**

Scalability is a critical factor in DT systems, which often involve large numbers of connected devices and users. The project's lightweight cryptographic algorithms enable the system to handle high transaction volumes without compromising performance.

The use of asynchronous communication and batch authentication further enhances scalability by reducing the frequency of interactions and optimizing network traffic. These features make the system well-suited for dynamic environments, such as IoT and smart cities, where scalability and efficiency are essential.

6. Decentralized Verification and Trust

- **Results:**

Blockchain technology enables decentralized verification of data transactions, ensuring:

- Transparency and accountability through tamper-proof records.
- Reduced reliance on centralized authorities, enhancing system resilience.

- **Discussion:**

Decentralized verification eliminates the risks associated with centralized systems, such as single points of failure and susceptibility to targeted attacks.

By distributing data across multiple nodes, the system ensures that no single entity can alter or manipulate records without detection.

This approach fosters trust among stakeholders, making the system suitable for collaborative applications where transparency is crucial. For example, in healthcare, decentralized verification can improve data sharing between hospitals, laboratories, and patients while maintaining confidentiality.

7. Multi-Industry Applicability

➢ **Results:**

The project demonstrates versatility, with potential applications across various industries:

- Healthcare: Secure remote monitoring, real-time diagnostics, and personalized treatment plans.

-Manufacturing: Predictive maintenance, production process optimization, and real-time performance monitoring.

-Smart Cities: Efficient traffic management, energy optimization, and infrastructure monitoring.

- IoT: Reliable device authentication, secure data sharing, and operational transparency.

➢ **Discussion:**

By addressing industry-specific challenges and requirements, the project's outcomes extend beyond technical advancements to offer practical benefits. For instance, in healthcare, the system ensures the confidentiality and integrity of patient data, enabling accurate diagnoses and treatment planning.

In manufacturing, the system supports predictive maintenance by securely transmitting real-time performance data, reducing downtime and optimizing operational efficiency. These applications highlight the system's potential to drive innovation across sectors.

8. User Trust and Adoption

➢ **Results:**

The project builds user trust through:

- A user-friendly interface that simplifies registration and authentication.
- Transparent operations enabled by blockchain technology.
- Robust privacy and security measures that protect sensitive data.

➢ **Discussion:**

Trust is a key factor for the adoption of any security framework. The project addresses user concerns by providing a secure, reliable, and easy-to-use system.

The transparency offered by blockchain technology allows users to verify the integrity of their data, fostering confidence in the system.

By protecting sensitive information and ensuring compliance with regulatory requirements, the project creates a secure environment that encourages widespread adoption of DT technology.

9. Robustness Against Cybersecurity Threats

- **Results:**

The system demonstrates resilience against various cybersecurity threats, including:

- Replay attacks.
- Man-in-the-middle attacks.
- Offline password guessing and brute force attacks.
- Impersonation and identity theft.

- **Discussion:**

The project’s comprehensive threat model and mitigation strategies ensure a secure operating environment. By combining blockchain technology with advanced cryptographic methods, the system protects against both traditional and emerging threats.

This robustness is particularly important in critical applications, such as healthcare and manufacturing, where security breaches can have severe consequences.

10. Compliance with Regulatory Standards

- **Results:**

The system aligns with regulatory frameworks such as GDPR and HIPAA, ensuring:

- Secure handling of sensitive data.
- Adherence to legal requirements for data protection and privacy.

- **Discussion:**

Compliance with regulatory standards is essential for the deployment of DT systems in regulated industries. By meeting these requirements, the project ensures its viability for applications in healthcare, finance, and other sectors where data security and privacy are critical.

The Privacy-Preserving Blockchain Security Protocol for Cloud-Based Digital Twin project delivers significant results that address key challenges in security, privacy, and scalability.

By combining blockchain technology with certificateless cryptography, the system ensures secure data transmission, integrity, and authentication while maintaining user privacy.

These results demonstrate the system’s potential for multi-industry applications, fostering innovation and improving operational efficiency. The project sets a new standard for secure and scalable DT implementations, paving the way for broader adoption and integration into modern interconnected systems.

CHAPTER 10
CONCLUSION

Thus, as the world moves forward with innovations, especially in smart environments, the urgency of establishing extensive user authentication models cannot be overemphasized. In this context, as exposed earlier in our study, we analyzed certain design flaws and weaknesses concerning the authentication scheme presented. Despite the creativity of the above mentioned scheme, the study realized that it was vulnerable to different cryptographic attacks such as; user impersonation attacks Key Session State Tracking and Intercept Attacks (KSSTIA) and offline password guessing attacks.

A danger is associated with unauthorized user impersonation that enables HI to be accessed by other unauthorized users under the guise of other HI users. Further, with the aid of state tracking, KSSTIA enables the attacker to take control of the active session compromising the confidentiality of the communication. Offline password guessing attacks take advantage of vulnerabilities in password, making it possible for the attacker to guess the credentials of a user without him or her knowing. These foregoing vulnerabilities accentuate the need to find better and safer ways of authenticating users. To counter these threats, we the have introduced an improved privacy-preserving three-factor-based the authentication framework using blockchain for DT environment. They assert that through blockchain, one is able to decentralize, make the authentication processes clear and thus cannot be altered in any way, which are qualities that when implemented helps in increasing security.

The proposed framework integrates three factors of authentication: an element which only the user is supposed to know (for example a password), an element the user is supposed to possess (for example a smart device), an element representing the user in some way (for example biometric data). This lays down multiple barriers to impersonation attacks thus lessening the possibility of an attacker gaining access to the higher tiers. The blockchain component remains as an extra layer of security, where the authentication transactions are to be recorded on the distributed ledger.

Every time the user tries the account, proof is provided in the blockchain as an audit trail. Besides using it the monitoring and reporting of any unauthorized access, this feature enables the quick handling of any threats to the security of the organization.

We provided an informative and parallel analysis of Security risk management and showed that our scheme has low take risk rate and could provide high level of protection against modern types of attacks., to validate the robustness of our framework, we performed the formal analysis using the ROR Model and the BAN logic.

6.1 SCOPE FOR FUTURE ENHANCEMENT

Over the last few decades, smart environment such as Digital Twin (DT) has emerged raising the need for better authentication technologies and techniques. In light of the various vulnerabilities and threats, the proposed blockchain-based three-factor authentication framework does present potential solutions for each of them Nevertheless, there is still much that can be improved to guarantee the framework’s continued efficacy and robustness in an ever-changing environment.

• **Message Compression**: It will always be helpful to employ message compression algorithms so as to cut down the total amount of data that passes through the authentication process. As with most anything that involves Net two-way communication, the less the payload size, the faster the message and the least utilization of bandwidth.

• **Asynchronous Communication:** Leveraging asynchronous communication protocols can help manage traffic loads. Instead of requiring immediate responses, allowing devices to authenticate in a non-blocking manner can enhance user experience and system responsiveness.

• **Batch Authentication**: Implementing batch authentication for multiple users or devices can reduce the frequency of communication required. By processing several authentication requests together, we can cut down on network traffic and improve overall efficiency.

2. Improved Computational Efficiency: The computational demands of the authentication framework are critical, especially for devices with limited processing power. Future enhancements should focus on optimizing the algorithms used for authentication.

Potential Approaches:

• **Algorithm Optimization**: Reviewing and refining the cryptographic algorithms used in the authentication process can lead to more efficient computations. Utilizing lightweight cryptography designed specifically for constrained environments can significantly lower the processing overhead.

• **Parallel Processing**: One can incorporate parallelism processing to tap into multi-faced core processors present on current generation devices to divide the computational load to improve the overall computational speed.

• **Adaptive Algorithms**: It is possible to design algorithms that will have the computational load optimized in accordance with the current network conditions and the capabilities of the devices to guarantee high efficiency of the selected types of authentications independent of the circumstance.

REFERENCES

[1] Digital twin: Mitigating emergent behavior that is unanticipated and unwanted in complex systems, by M. Grieves and J. Vickers, Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches. Springer, Cham, Switzerland, 2017, pp. 85–113.

[2] "Materials, structures, mechanical systems, and manufacturing road map," by B. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino NASA Technical Report TA-12, Washington, DC, USA, 2012.

[3] "Prototyping a digital twin for real-time remote control over mobile networks: Application of remote surgery," by H. Laaki, Y. Miche, and K. Tammi IEEE Access, 7 (2019), 20325–20336.

[4] "Blockchain based data integrity verification for large-scale IoT data," by H. Wang and J. Zhang IEEE Access, 7 (2019), 164996–165001.

[5] Blockchain data-based cloud data integrity protection system, P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, Future Gener. Comput. Syst., vol. 102, pp. 902–911, Jan. 2020.

[6] "Blockchain based data integrity service framework for IoT data," B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, Proc. IEEE Int. Conf. Web Services (ICWS), Jun. 2017, pp. 468 475.

[7] On the design of a privacy-preserving communication strategy for cloud-based digital twin settings using blockchain, S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park IEEE Access, volume 10, 2022, pages 75365–75375.

[8] "An enhanced pairing-based authentication scheme for smart grid communications," by T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan J. Natural Environment

[9] "Privacy preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, IEEE Access, vol. 7, pp. 47962–47971, 2019.

[10] A safe and improved two factor authentication approach employing elliptic curve and bilinear pairing for cyber physical systems, A. Sengupta, A. Singh, P. Kumar, and T. Dhar, Multimedia Tools Appl., vol. 16, pp. 1–24, Jul. 2022.

[11] In December 2020, H. S. Grover and D. Kumar published a paper in the Journal of Reliable Intelliability and Environment, titled "Cryptanalysis and improvement of a three factor user authentication scheme for smart grid environment," which covered 249–260.

[12] "Secure three factor user authentication scheme for renewable-energy-based smart grid environment," by M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues Dec. 2017, 3144–3153; IEEE Trans.

[13] Ind. Informat., vol. 13, no. 6. In J. Inf. Secur. Appl., vol. 58, May 2021, Art. no. 102787, D. Kaur and D. Kumar discuss "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home."

[14] Anonymous authentication technique for smart home environment with provable security, M. Shuai, N. Yu, H. Wang, and L. Xiong, Comput.Secur., vol. 86, pp. 132–146, Sep. 2019.

[15] "A bilinear map pairing based authentication scheme for smart grid communications: PAuth," by Y. Chen, J. Martinez, P. Castillejo, and L. López IEEE Access, 7 (2019), 22633–22643.

[16] "Cryptanalysis of Khatoon et al.'s ECC-based authentication protocol for healthcare systems," by M. Nikooghadam and H. Amintoosi arXiv:1906.08424, 2019.

[17] Password-based authenticated key exchange in the three-party setting: M. Abdalla, P.-A. Fouque, and D. Pointcheval, Proc. Int.

[18] A logic of authentication, by M. Burrows, M. Abadi, and R. Needham, ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, Feb. 1990.

[19] "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system," by A. K. Das and B. Bruhadeshwar 2013, vol. 37, no. 5, p. 9969, J. Med. Syst.

[20] Secur. Commun. Netw., vol. 8, no. 9, pp. 1752–1771, 2015. S. Chatterjee and A. K. Das, "An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks,"

[21] "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card," by D. Mishra, A. K. Das, and S. Mukhopadhyay, was published in Peer-Peer Network Applications in January 2016 (vol. 9, no. 1, pp. 171–192).

[22] "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, and Y. Park, IEEE Internet Things J., vol. 7, no. 4, pp. 3184–3197, Apr. 2020.

[23] "Design and testbed experiments of user authentication and key establishment mechanism for smart healthcare cyber physical systems," by M. Wazid, S. Thapliyal, D. P. Singh, A. K. Das, and S. Shetty Early access to IEEE Trans. Netw. Sci. Eng. (May 29, 2022) doi: 10.1109/TNSE.2022.3163201.

APPENDIX-A

PSUEDOCODE

Below is the pseudocode for implementing the Privacy-Preserving Blockchain Security Protocol for Cloud-Based Digital Twin (DT). It covers the key functionalities: registration, authentication, data integrity verification, and secure data sharing.

1. Registration Phase

Objective: Register users with unique key pairs and store information securely.

```
Procedure UserRegistration():
    Input: UserID (UID), UserPassword (PWD)
    Output: User's Public Key (PK), Private Key (SK)
    Step 1: Generate PartialPrivateKey (PPK) from Key Generation Center (KGC).
    Step 2: User combines PPK with their own secret information to generate Private Key (SK).
    Step 3: Derive Public Key (PK) from SK using elliptic curve cryptography (ECC).
    Step 4: Securely store PK and SK in the cloud server (No certificate required).
    Step 5: Return success message.
EndProcedure
```

2. Authentication Phase

Objective: Authenticate users using a three-factor method (password, possession, and biometric data).

```
Procedure UserAuthentication():
    Input: UID, PWD, DeviceToken, BiometricData
    Output: Authentication Status (Success/Failure)
    Step 1: Receive authentication request from user with UID and signed message.
    Step 2: Verify password (PWD) using stored hash.
    Step 3: Check possession factor by validating DeviceToken.
    Step 4: Validate BiometricData with stored reference data.
    Step 5: If all factors are verified, generate server-side challenge (Nonce).
    Step 6: Send Nonce to user and request signed response using Private Key (SK).
    Step 7: Verify user's signature using Public Key (PK).
    Step 8: If verified, authenticate user; else, deny access.
EndProcedure
```

3. Blockchain Data Integrity Verification

Objective: Verify the integrity of data using hash values stored on the blockchain.

```
Procedure VerifyDataIntegrity():
    Input: Data (D), BlockchainHash (BH)
    Output: Integrity Status (Valid/Invalid)
    Step 1: Compute HashValue (HV) of the received Data (D) using a cryptographic hash function.
    Step 2: Retrieve the corresponding BlockchainHash (BH) from the blockchain ledger.
    Step 3: Compare HV with BH.
        If HV == BH:
            Return "Data is Valid and Untampered."
        Else:
            Return "Data Integrity Compromised."
EndProcedure
```

4. Secure Data Sharing

Objective: Allow secure data sharing between authenticated users and the cloud server.

```
Procedure SecureDataSharing():
    Input: AuthenticatedUser (AU), DataRequest (DR)
    Output: Encrypted Data (ED)
    Step 1: Verify that AU is authenticated (Use UserAuthentication()).
    Step 2: Encrypt requested data (DR) using AU's Public Key (PK).
    Step 3: Record data sharing transaction on blockchain (Hash of DR and AU).
    Step 4: Send Encrypted Data (ED) to AU.
    Step 5: Log transaction for auditing purposes.
EndProcedure
```

5. Blockchain Record Transaction

Objective: Record transaction data securely on the blockchain.

```
Procedure RecordTransactionOnBlockchain():
    Input: TransactionData (TD)
    Output: Blockchain Transaction Status (Success/Failure)
    Step 1: Compute Hash (H) of the TransactionData (TD).
    Step 2: Add H to the blockchain as a new block.
    Step 3: Verify block addition using consensus mechanism (e.g., Proof of Authority).
    Step 4: If consensus achieved, finalize the block.
    Step 5: Return success message.
EndProcedure
```

6. Mutual Authentication Between User and Cloud Server

Objective: Establish trust between the user and the cloud server.

```
Procedure MutualAuthentication():
    Input: UserRequest (UR), CloudResponse (CR)
    Output: Mutual Authentication Status (Success/Failure)
    Step 1: User sends authentication request (UR) signed with Private Key (SK).
    Step 2: Cloud server verifies signature using User's Public Key (PK).
    Step 3: Cloud generates challenge (Nonce) and sends it to the user.
    Step 4: User signs Nonce with SK and sends response (SignedNonce) back to the server.
    Step 5: Cloud verifies SignedNonce with PK.
    Step 6: If both verifications are successful, establish trust.
EndProcedure
```

7. Audit Logging for Security Monitoring

Objective: Maintain logs of authentication attempts and data transactions.

```
Procedure AuditLogging():
    Input: EventDetails (ED), UserID (UID)
    Output: Log Entry Status (Success/Failure)
    Step 1: Create a log entry with timestamp, UID, and EventDetails.
    Step 2: Store log entry in a secure database.
    Step 3: Optionally, record log hash on blockchain for tamper-proof auditing.
    Step 4: Return success message.
EndProcedure
```

Key Considerations

1. **Security:** The pseudocode includes cryptographic measures like ECC, hash functions, and blockchain for secure data handling.

2. **Scalability:** Lightweight cryptography ensures scalability for resource-constrained environments like IoT.
3. **Privacy:** Certificateless cryptography ensures user anonymity and untrace ability.
4. **Transparency:** Blockchain integration ensures transparent and verifiable transactions.

This pseudocode provides a comprehensive framework for implementing the proposed system, covering all major functionalities discussed in the report.

APPENDIX-B

SCREENSHOTS

VIEW IMPERSONATION ATTACK

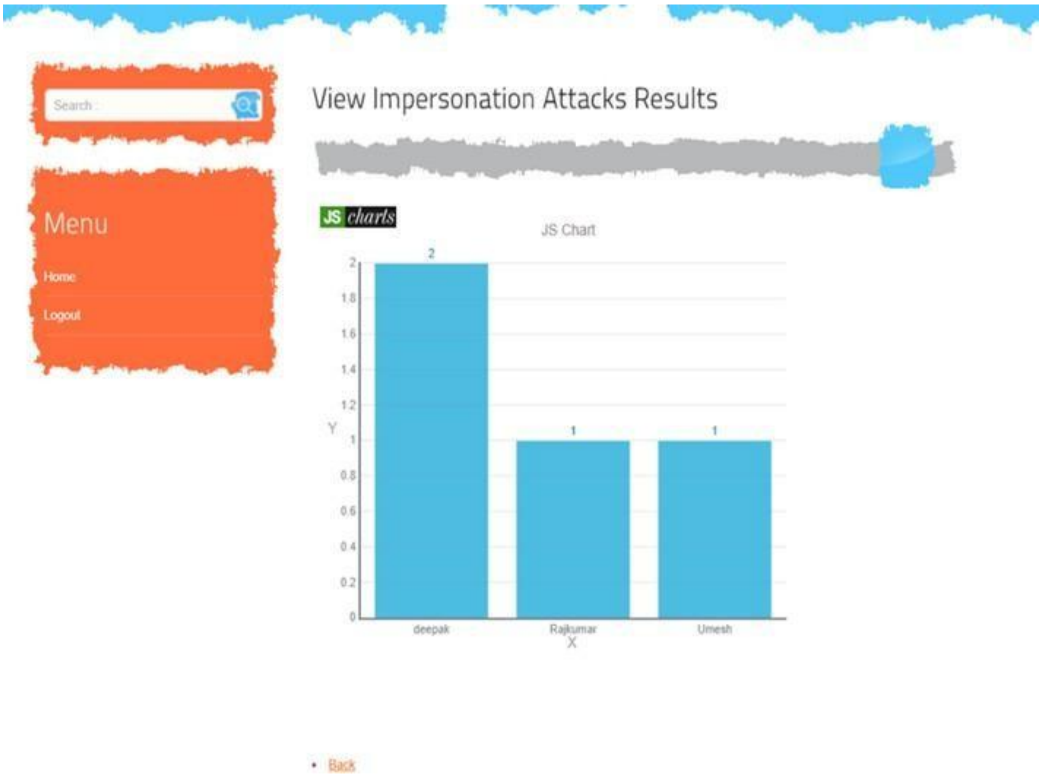


Fig. VIEW IMPERSONATION ATTACK

Figure shows the outcomes of simulated impersonation attacks. The table depicts the number of successful impersonations attempts for three users: Deepak, Rajkumar, and Umesh.
Deepak has experienced the maximum number of attacks(2), whereas Rajkumar and Umesh faced one successful impersonation each.

APPENDIX-C

ENCLOSURES