PIP2001 Capstone Project
Review

PROJECT TITLE : AN EFFECTIVE PRIVACY PRESERVING BLOCKCHAIN ASSISTED SECURITY PROTOCOL

Batch Number:2021-25

Roll Number	Student Name
20211CEI0166	Thrisha Reddy P
20211CEI0157	Hruthika S N
20211CEI0141	Chandana G S

Under the Supervision of,

Dr./Mr./Ms./Prof. Joe Arun Raja
Professor / Associate Professor / Assistant Professor
School of Computer Science and Engineering
Presidency University

Name of the Program: Computer Engineering (Artificial Intelligence and Machine Learning)
Name of the HoD: Dr.Gopal Krishna Shyam
Name of the Program Project Coordinator: Joe Arun Raja
Name of the School Project Coordinators: Dr. Sampath A K / Dr. Abdul Khadar A / Mr. Md Ziaur Rahman

Content

- Problem Statement
- Github Link
- Analysis of Problem Statement
- Timeline of the Project(Gant Chart)
- References

Problem Statement Number:

- Organization: Presidency University
- Category (Hardware / Software / Both) : Software
- Problem Description:The proposed system combines Elliptic Curve Cryptography (ECC) with a blockchain-assisted infrastructure, enabling fast and secure communication between legitimate users without relying on traditional certificate authorities. The use of ECC enhances computational efficiency, making it suitable for the resource-constrained environment of IoT devices that support Digital Twins.
- Difficulty Level: Complex

Github Link

Github Link:

https://github.com/Thrisha1206/An-effective-privacy-preserving-blockchain-assisted-security-protocol.git

Problem Statement

- The implementation of Digital Twin (DT) technology in cloud-assisted environments faces significant challenges related to secure data sharing, integrity verification, and privacy preservation.
- As data generated from physical assets is transmitted to cloud servers for simulation and analysis, the risk of sensitive information being intercepted or tampered with by adversaries becomes a major concern.
- Existing authentication mechanisms often fail to provide essential security features such as user anonymity, mutual authentication, and protection against identity and password guessing attacks.
- Traditional cryptographic systems suffer from complex certificate management and key escrow issues, making them unsuitable for secure DT environments.
- To address these challenges, there is a need for a robust and efficient authentication protocol that ensures secure communication, data integrity, and privacy preservation in cloud-assisted DT environments.
- The solution must withstand various security threats, including impersonation attacks, and facilitate secure data sharing between data owners, users, and cloud servers.
- This problem can be resolved by leveraging blockchain technology to verify data integrity through hash values and elliptic curve cryptography (ECC) for efficient, certificate-less authentication.

Analysis of Problem Statement

Functional Requirements

- The proposed system for the privacy-preserving blockchain-assisted security protocol in Digital Twin (DT) environments must fulfill several core functionalities.
- Firstly, it should implement certificateless authentication to ensure that users can securely authenticate without the need for traditional certificate management, using partial private keys generated by a trusted third party and personal secrets.
- The system must integrate blockchain technology to record and verify data integrity, storing hash values of DT data and maintaining a tamper-proof log of transactions.
- It should also facilitate secure communication among users by utilizing Elliptic Curve Cryptography (ECC) to ensure that authentication processes are both efficient and resistant to common security threats such as impersonation and password guessing.

Analysis of Problem Statement (contd...)

Software and Hardware Requirements:

H/W System Configuration:-

- ➢ Processor - Pentium –IV
- ➢ RAM - 4 GB (min)
- ➢ Hard Disk - 20 GB

Software Requirements:

- Operating System - Windows XP
- Coding Language - Java/J2EE(JSP,Servlet)
- Front End - J2EE
- Back End - MySQL

Analysis of Problem Statement (contd...)

- This project aims to design and implement a privacy-preserving authentication protocol for Digital Twin (DT) environments, leveraging the security of blockchain technology and the efficiency of certificateless cryptography.
- Digital Twins are real-time virtual replicas of physical systems used in various industries like manufacturing, healthcare, and IoT.
- securely sharing and verifying the data exchanged between users, devices, and cloud services remains a significant challenge.
- To address these challenges, this project proposes a secure framework that uses blockchain to store hash values of the data generated by DTs.
- The blockchain ensures that the data remains tamper-proof and verifiable by all participants in the network.
- The certificateless cryptography scheme is employed to solve issues related to traditional cryptosystems, such as complex certificate management and key escrow problems.
- This ensures that the authentication process is efficient ad resistant to various security attacks, such as impersonation and password guessing.

Timeline of the Project (Gantt Chart)

Phase 1

- Firstly, we review and cryptanalysis the scheme proposed by Son et al. [7] and identify that the scheme is susceptible to impersonation attacks, password guessing attacks, anonymity, and untraced ability attacks. Besides, it does not support mutual authentication and session key agreement.

Phase 2

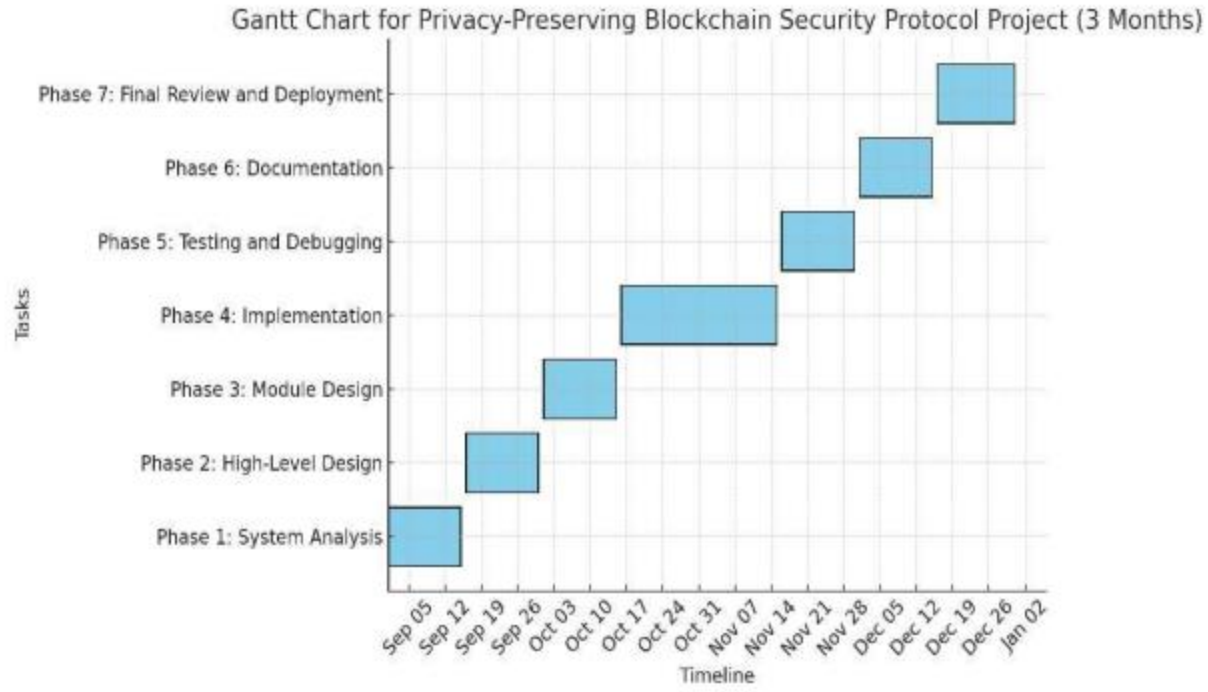
- We design a ‘‘secure three-factor privacy-preserving authentication scheme for the DT environment’’ by utilizing block chain technology and ‘‘elliptic curve cryptography (ECC)’’ to realize secure communication among legitimate users and conquer security flaws.

Phase 3

- The suggested framework’s informal analysis ensures that the protocol is resilient to various security assaults. Using the ROR model [17] and BAN logic [18], we also demonstrate that the proposed scheme can assure ‘‘mutual authentication’’ and ‘‘session key security’’.

- The computational and communication efficiency of the work is demonstrated by analyzing the presented work with the pre-existing authentication schemes.

Gant Chart


Gantt Chart for Privacy-Preserving Blockchain Security Protocol Project (3 Months)
Tasks
Phase 7: Final Review and Deployment
Phase 6: Documentation
Phase 5: Testing and Debugging
Phase 4: Implementation
Phase 3: Module Design
Phase 2: High-Level Design
Phase 1: System Analysis
Sep 05
Sep 12
Sep 19
Sep 26
Oct 03
Oct 10
Oct 17
Oct 24
Oct 31
Nov 07
Nov 14
Nov 21
Nov 28
Dec 05
Dec 12
Dec 19
Dec 26
Jan 02
Timeline

References (IEEE Paper format)

- [1] M. Grieves and J. Vickers, ‘‘Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems,’’ in *Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches*. Cham, Switzerland: Springer, 2017, pp. 85–113.
- [2] B. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino,‘‘Materials, structures, mechanical systems, and manufacturingroadmap,’’ NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.
- [3] H. Laaki, Y. Miche, and K. Tammi, ‘‘Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,’’ *IEEE Access*, vol. 7, pp. 20325–20336, 2019.
- [4] H. Wang and J. Zhang, ‘‘Blockchain based data integrity verification for large-scale IoT data,’’ *IEEE Access*, vol. 7, pp. 164996–165006,2019.
- [5] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ‘‘Blockchain data-based cloud data integrity protection mechanism,’’ *Future Gener. Comput. Syst.*, vol. 102, pp. 902–911, Jan. 2020.
- [6] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, ‘‘Blockchain based data integrity service framework for IoT data,’’ in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.
- [7] 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.

- [8] "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.
- [9] "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.
- [10] "Blockchain based data integrity verification for large-scale IoT data," by H. Wang and J. Zhang IEEE Access, 7 (2019), 164996–165001.
- [11] 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.
- [12] "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.
- [13] 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.
- [14] "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.
- [15] 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.


Thank
You!