**CYBER SECURITY ASSIGNMENT 2**

**REPORT**

Name: P Samiksha

Date: 04.10.2025

GitHub Repository: <https://github.com/samikshaa0604/cybersecurityassignment2>

**ABSTRACT**

Blockchain technology has gained immense recognition as a decentralized, tamper-proof system for ensuring secure digital transactions. While it strengthens the fundamental pillars of cybersecurity—confidentiality, integrity, and availability—it is not immune to threats. Issues such as private key theft, low throughput of Proof-of-Work (PoW), smart contract vulnerabilities, and data privacy concerns in IoT and cloud environments remain critical gaps. This project addresses these challenges by developing executable improvements using Python, including a Multi-Signature Wallet simulation, a smart contract static vulnerability scanner, a comparative analysis of PoW and Proof-of-Stake (PoS), and a Zero-Knowledge Proof (ZKP) demonstration. These solutions highlight how blockchain security can be enhanced through practical methods that balance efficiency, scalability, and resilience.

**METHODOLOGY**

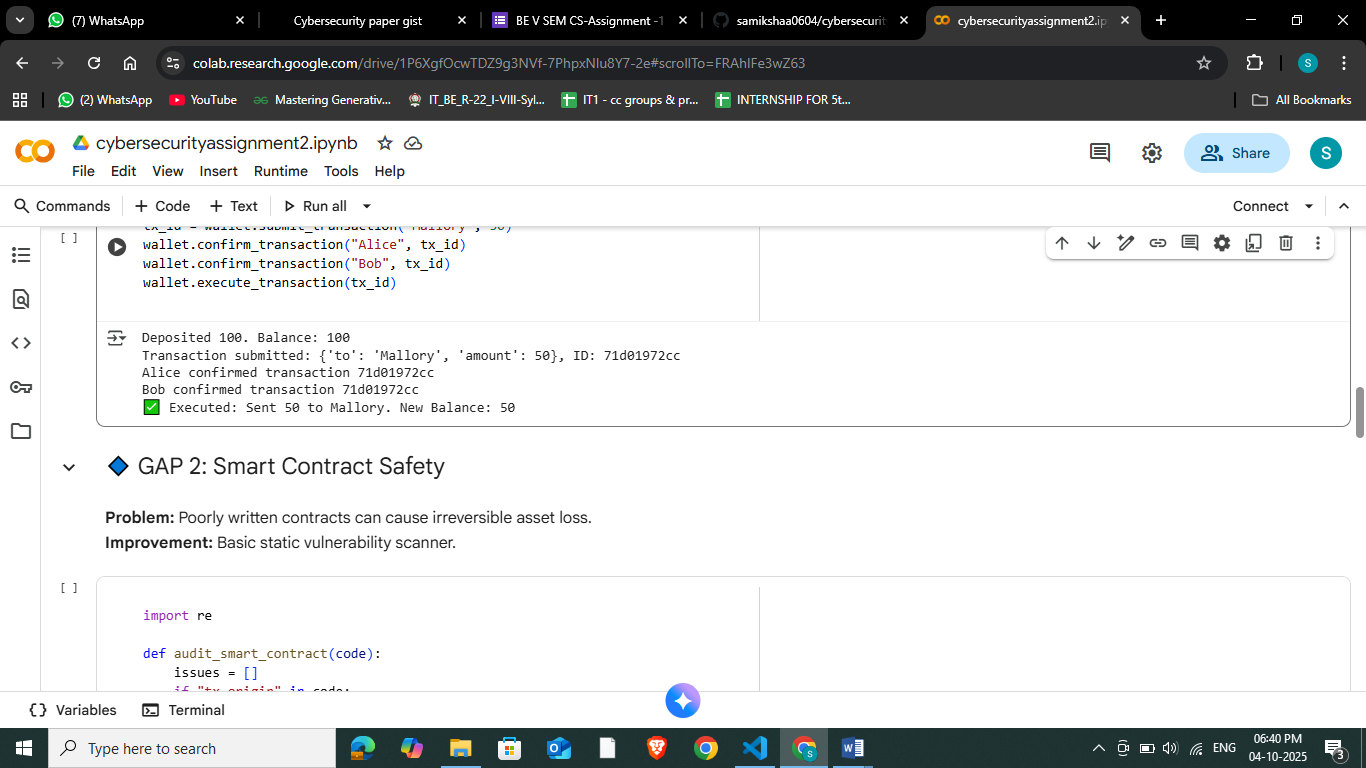
Research Gaps Filled

1. **Wallet Security Gap**
   * *Gap:* Single private key compromise leads to permanent asset loss.
   * *Improvement:* Implemented a Multi-Signature Wallet simulation requiring multiple approvals for transactions, reducing single-point failure risks.
2. **Smart Contract Safety Gap**
   * *Gap:* Poorly written contracts may contain undetected vulnerabilities.
   * *Improvement:* Developed a Static Smart Contract Analyzer in Python to detect insecure coding patterns (e.g., tx.origin, delegatecall, unchecked call.value).
3. **Consensus Performance Gap**
   * *Gap:* Proof-of-Work consumes excessive energy and limits scalability.
   * *Improvement:* Simulated and compared PoW vs PoS consensus, showcasing the efficiency and sustainability of PoS.
4. **Data Privacy Gap in IoT/Cloud**
   * *Gap:* Sensitive data shared across networks risks exposure.
   * *Improvement:* Demonstrated a Zero-Knowledge Proof (ZKP) mechanism to verify knowledge without revealing the underlying secret.

**RESULTS**

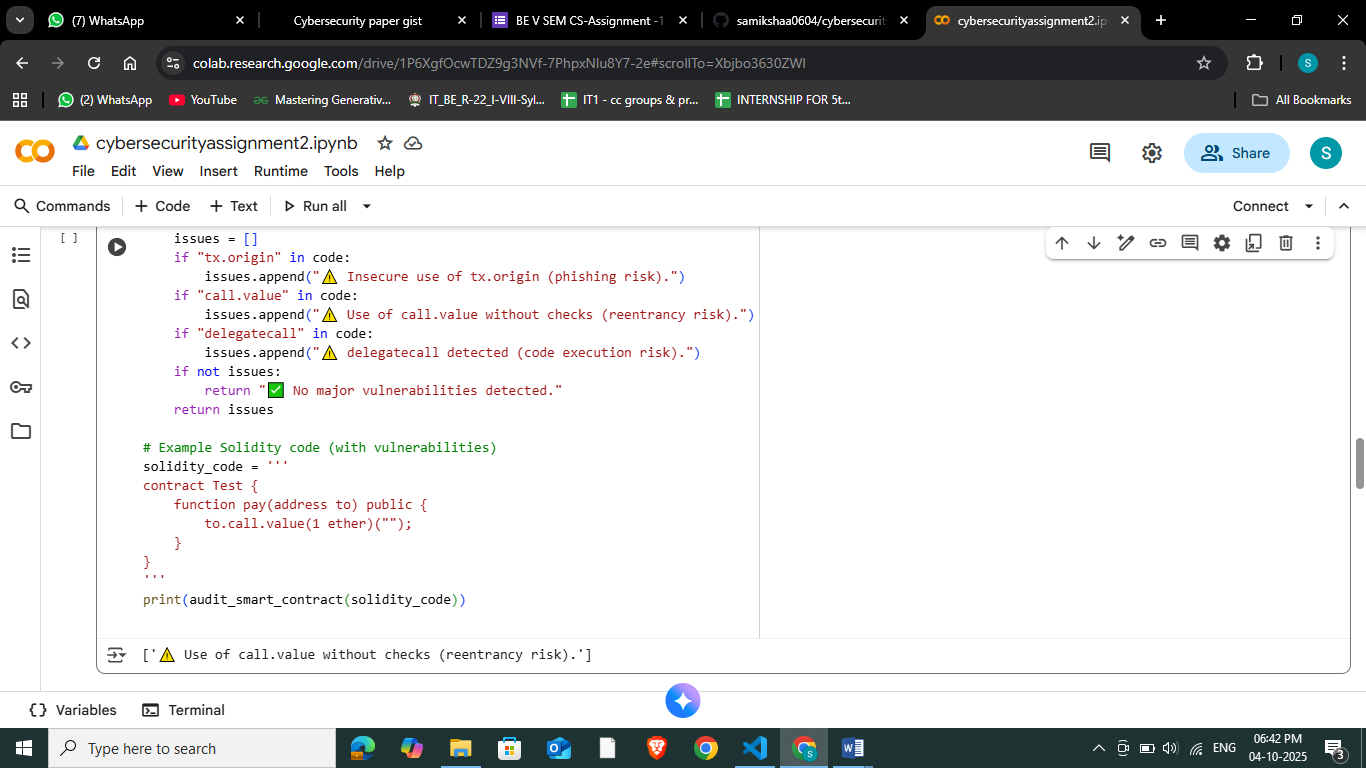
## **GAP 1: Wallet Security**

**Problem:** Single private key theft = permanent asset loss.  
**Improvement:** Multi-Signature Wallet (Multisig).



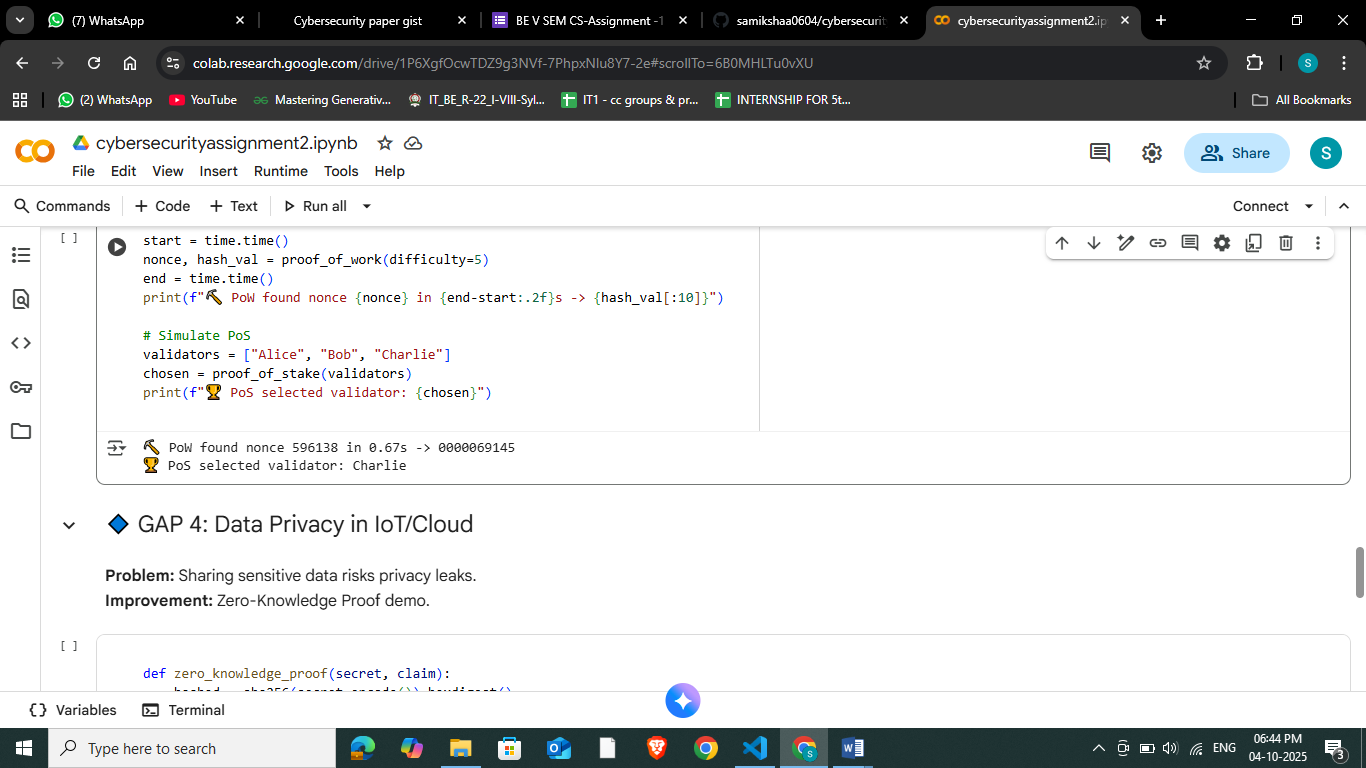
## **GAP 2: Smart Contract Safety**

**Problem:** Poorly written contracts can cause irreversible asset loss.  
**Improvement:** Basic static vulnerability scanner.



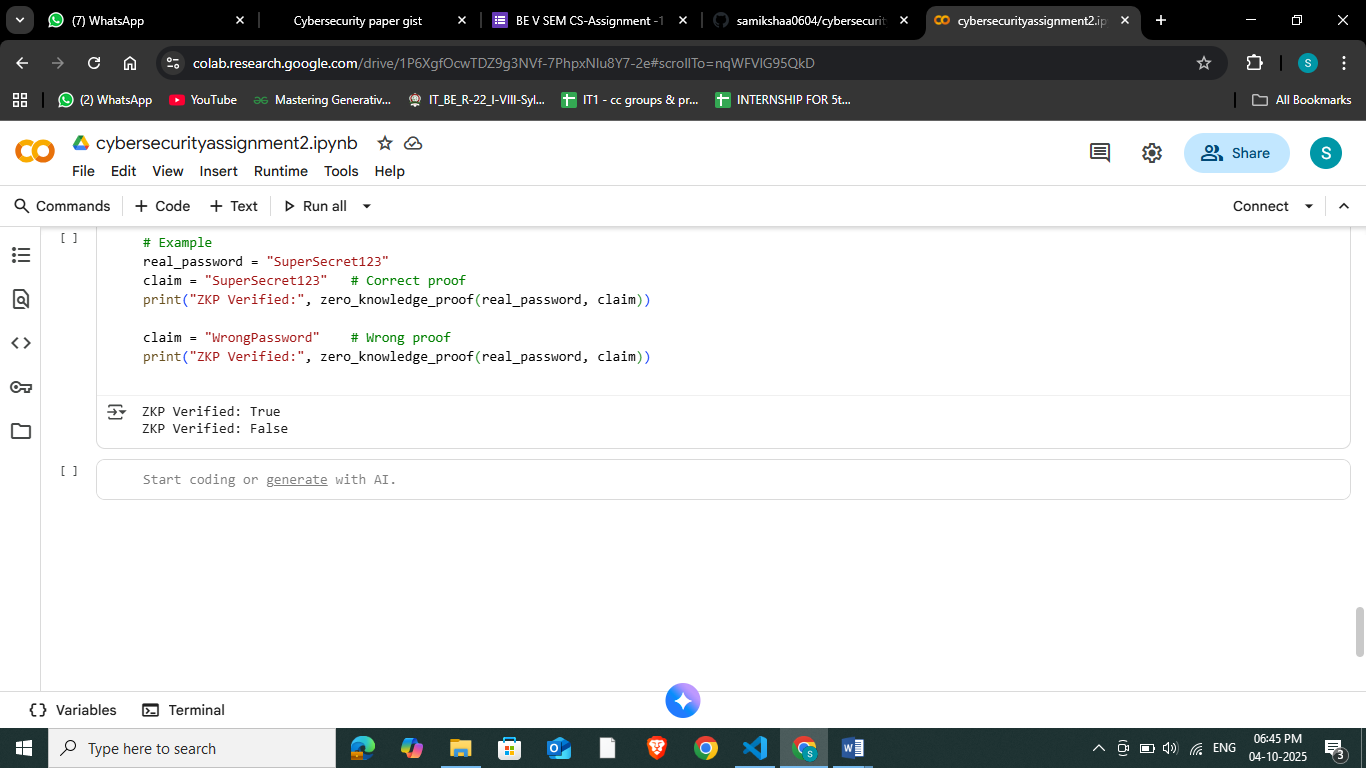
## **GAP 3: Consensus Performance**

**Problem:** Proof-of-Work is slow and energy-hungry.  
**Improvement:** Compare PoW vs PoS simulation.



## **GAP 4: Data Privacy in IoT/Cloud**

**Problem:** Sharing sensitive data risks privacy leaks.  
**Improvement:** Zero-Knowledge Proof demo.



**CONCLUSION**

This project demonstrates that while blockchain offers inherent resilience against tampering and unauthorized modifications, its security is not absolute. By identifying critical gaps—such as vulnerability to private key compromise, inefficiencies in PoW, risks from poorly written smart contracts, and privacy challenges in IoT/cloud applications—we showed how executable improvements can significantly strengthen blockchain systems.The implemented solutions—multi-signature wallets, smart contract auditing tools, PoS consensus simulation, and zero-knowledge proofs—offer both conceptual clarity and practical application. These measures make blockchain-based systems more secure, scalable, and trustworthy for real-world adoption.