RESEARCH ARTICLE OPEN ACCESS

Biolock: Biosecure Single Sign on Cold Storage Architecture with Blockchain-Based Predicament Recovery

Guide:Dr.P.Arivazhagi

M.Athithyan[1],R.Abinesh[2],R.K.Sharan[3],S.Vasanth[4]

Department of Electronics and Communication Engineering,Arasu Engineering College, Kumbakonam,Tamilnadu

Email:mathivananathithyan@gmail.com

Abstract:

The secure management of cold-stored digital assets is critically vulnerable when access control depends on a single key individual. Existing systems rely on passwords, hardware wallets, recovery phrases, or basic multi-signature mechanisms, all of which suffer from significant limitations such as single points of failure, credential loss, and vulnerability to phishing attacks. To address these challenges, this paper proposes BioLock, a Biosecure Single Sign-On (SSO)Cold Storage System integrated with Blockchain technology. The architecture utilizes multi-modal biometric authentication, specifically leveraging Electroencephalogram (EEG) signals with liveness detection, to establish a secure and non-transferable SSO identity. Biometric data privacy is ensured through cryptographic hashing and secure enclaves. Digital assets remain in true offline cold storage, accessible only via time-bound, policy-controlled hardware interfaces. Furthermore, a blockchain-based predicament recovery mechanism guarantees reliable access restoration during system failures, incapacitation,or security breaches.

I.INTRODUCTION

In the modern digital era, the protection of sensitive data and secure authentication mechanisms have become critical challenges due to the increasing frequency of cyberattacks, identity theft incidents, and unauthorized access attempts. Organizations and individuals increasingly rely on online platforms for financial transactions, data storage, communication, and critical services. However, traditional password based systems are becoming inadequate for protecting sensitive data in today's complex digital environment. BIOLOCK is a biosecure single sign-on (SSO) system designed to provide highly secure access control for cold storage environments. It integrates biometric authentication with blockchain technology to ensure tamper-proof identity verification and data integrity. The system enhances security while simplifying user access through a single authentication process. Additionally, managing multiple logins across storage units reduces operational efficiency and increases human error. Existing biometric systems often don't provide secure offline storage or tamper-proof audit logs, making legal or emergency recovery impossible in the absence of a digital will. To address these limitations, advanced security frameworks that combine biometric authentication, blockchain technology, and secure storage architectures are emerging as reliable solutions.

LITERATURE SURVEY

Extensive research has been conducted in the do main of biometric authentication, blockchain, and se cure storage systems. Below is a comprehensive review of the foundational and recent literature that inspired this architecture:

A. EEG-Based Biometrics and Machine Learning

Shams et al. (2022) surveyed machine learning techniques for EEG-based biometric authentication. They analyzed various feature extraction methods and classification algorithms used for identifying individ uals through brainwave signals, concluding that EEG biometrics provide strong protection against spoofing attacks.

B. Deep Learning in EEG Identification

Alsumari et al. (2023) proposed a deep learning model using convolutional neural networks (CNN) for user identification based on EEG signals. Their study demonstrated that EEG authentication provides higher security compared to traditional biometrics like finger prints because brain signals are virtually impossible to replicate. Furthermore, Bin Liu et al. (2025) achieved a 92.6% accuracy using deep convolutional recurrent neural networks (CNN-LSTM) for real-time brain signal authentication.

C. Event-Related Potentials in Authentication

Al-Nafjan et al. (2025) investigated EEG signals generated by different Event-Related Potentials (ERPs) for biometric authentication, proving that specific brain responses can effectively create highly secure environments. Abo Alzahab et al. (2022) further analyzed how 2 auditory stimuli influence EEG systems, showing a 9% improvement in authentication accuracy when auditory stimuli are applied.

D. Multimodal and Hybrid Systems

Rahman et al. (2021) proposed a hybrid biometric system combining EEG signals with keystroke dynamics. Using Random Forest and Extreme Gradient Boosting, they achieved an authentication accuracy above 99%. Venkataswamy et al. (2024) applied Support Vector Machine (SVM) models to classify users based on EEG signals, achieving 92.9% accuracy.

E. Blockchain and Cold Storage Security

S. Nakamoto (2008) laid the foundation for decentralized ledgers, which has since evolved into robust security frameworks. Li et al. (2020) discussed secure cold wallet designs utilizing blockchain and biometric authentication, highlighting the necessity of keeping private keys in offline, tamper-resistant environments. Conti et al. (2018) surveyed the privacy issues of centralized systems, emphasizing the need for distributed predicament recovery architectures.

III. IDENTIFICATION OF PROBLEM AND EXISTING SYSTEM

Traditional cold storage access systems rely on single-factor authentication and centralized credential management, making them vulnerable to unauthorized access, credential loss, and system failure. Managing multiple logins across storage units reduces operational efficiency and increases human error.

A. Existing System Architecture

In the existing system, multiple health and safety parameters such as body temperature, pulse rate, and user condition are continuously monitored using sensors including DHT11, pulse sensor, ACS712, and MQ2 gas sensor. These sensor values are collected and temporarily stored in an information storage unit and processed by an Arduino microcontroller. The system continuously checks whether the monitored parameters exceed predefined normal threshold limits. When any abnormal condition is detected, the Arduino automatically retrieves the user's pre-stored personal and medical information and transmits it to a predefined consultation or emergency contact number using the GSM module. Simultaneously, the sensor readings and alert information are uploaded to the cloud server, enabling remote access by clients such as doctors or caretakers for real-time monitoring.t

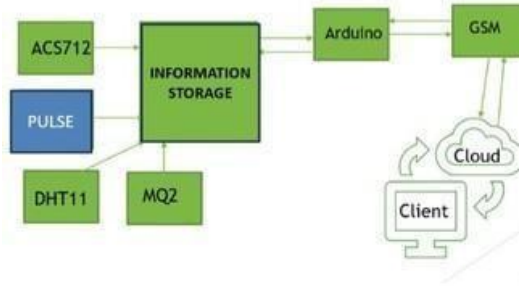

Fig 1.Block diagram of Existing System

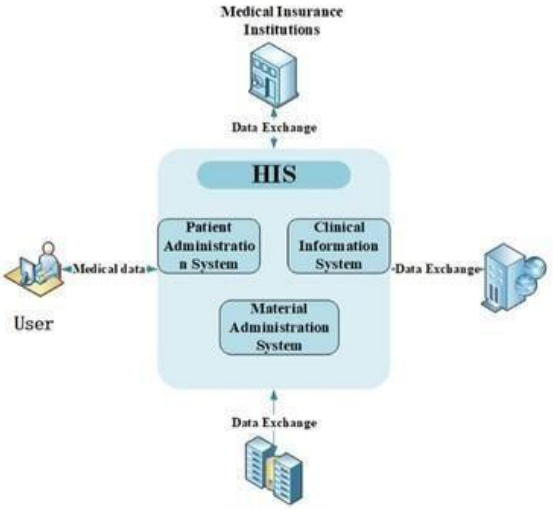

Fig 2.Circuit diagram of Existing System

B. Disadvantages of the Existing System

- **Password Reliance:** Most cold storage systems rely on passwords, which can be easily lost or forgotten, risking permanent asset loss, with no provision for asset succession.
- **Single Point of Failure:** Hardware wallets keep assets offline but fail if the sole custodian is unavailable.

- **Vulnerable recovery phrases**:Recovery phrases can be stolen,damaged or mishandled.
- **Inefficient Multi-Signature**: Multi-signature setups fail if key holders are incapacitated.
- **Lack of Offline Security**: Existing biometrics often don't provide secure true offline storage.

IV. PROPOSED ARCHITECTURE: BIOLOCK

The primary objective of BioLock is to design a highly secure, tamper-resistant authentication and data protection framework that integrates biometric based single sign-on (SSO) with cold storage security mechanisms and blockchain technology.

A. Methodology

1) **Blockchain-Based Secure Ledger**: A permis sioned blockchain network stores authentication logs, access records, and integrity proofs.

2) **Cold Storage Security Architecture:** Protec tion against online attacks, malware, and unau thorized remote access.

3) **Biometric-BasedSSO:**Multi-modal modalities (EEG, fingerprint, facial) are used for authentication.

4) **Predicament Recovery Mechanism:** Con trolled, multi-party recovery processes with smart contracts for secure succession in case of incapacitation.

5) **Monitoring and Auditability:** All access at tempts and emergency events are recorded as immutable logs.

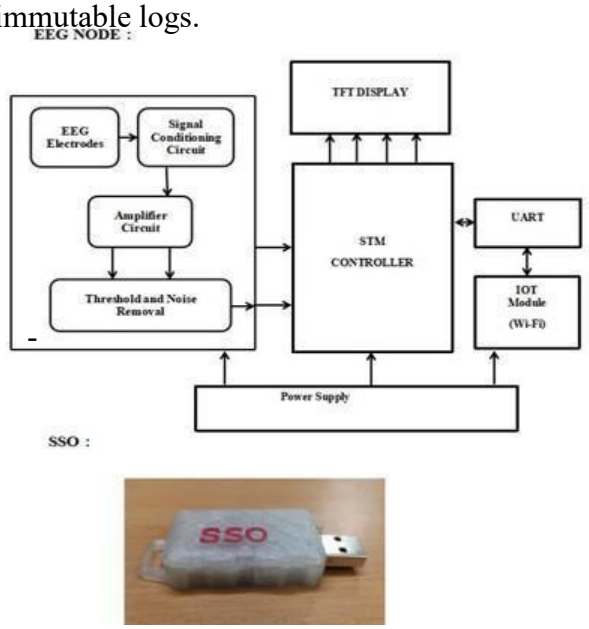

Fig 3.Block diagram of Proposed system

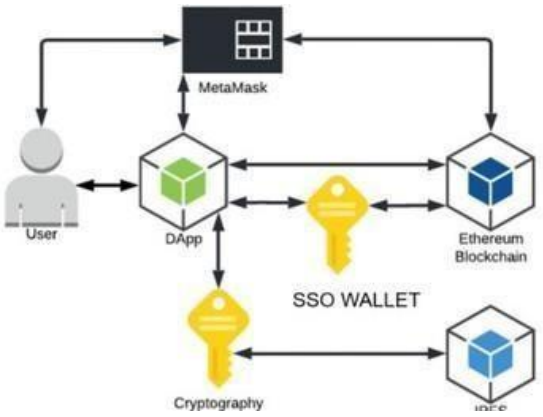

Fig 4.Circuit diagram of Proposed system

V. HARDWARE COMPONENTS

The proposed architecture integrates specialized hardware to ensure offline security and real-time processing.

A.STM32 Microcontroller Board

The core processing unit is an ARM Cortex M3/M4 based microcontroller (e.g., STM32F103C8 / STM32F4 series). It operates at 3.3V with a clock speed of 72MHz. It houses 64−125KB of Flash and 20−128KB SRAM. It acts as the central control unit, processing the incoming EEG signals, executing the system logic, and managing communication with the IoT module, TFT display, and cold storage.

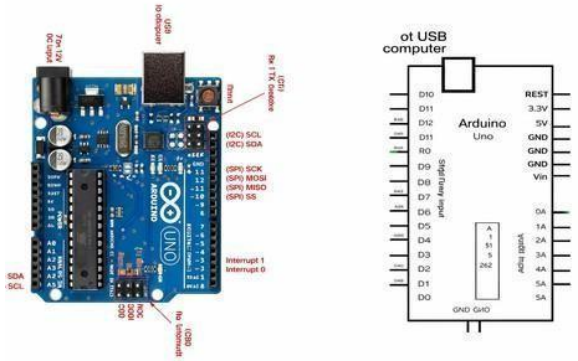

Fig.5 STM32 Microcontroller Board

B. EEG Sensor Module Examples include NeuroSky MindWave or Open BCI EEG modules. Operating at 3.3V − 5V, these sensors capture brain electrical signals in the microvolt (µV) range. They typically interface via UART, SPI, or Bluetooth. These modules capture raw brainwave signals used for identity verification and mental-state liveness detection.

C. Cold Storage Device

Utilizing Secure Flash Memory or External EEP ROM, this non-volatile memory (typically 8GB − 64GB) interfaces via SPI, I2C, or USB. It stores encrypted biometric templates and keeps sensitive credentials entirely offline to prevent network-based cyberattacks.

D. IoT Communication Module (ESP8266)

The ESP8266 or ESP32 serves as the IoT gateway. Operating at 3.3V with a clock speed of 80MHz, it handles Wi-Fi connectivity and communicates over MQTT/HTTP/HTTPS protocols. Its primary function is securely transmitting authentication logs, access attempts, and predicament alerts to the cloud and blockchain nodes.

E. TFT Display & Emergency Unlock Hardware

A 2.4″ − 2.8″ TFT LCD (240 × 320 pixels) dis plays system status and authentication prompts. The Emergency Unlock Hardware utilizes a solenoid lock or relay module (5V/12V) activated via programmed override during biometric failure or verified emergency recovery scenarios.

VI. WORKING AND SYSTEM FLOW

The system operates in a sequential pipeline from signal acquisition to authentication and logging

1) **EEG Signal Acquisition**:

Electrodes placed on the scalp detect electrical activity produced by neurons. These signals have minute amplitudes in the range of microvolts (1μV − 100μV).

2) **Signal Conditioning and Amplification:** Raw EEG signals contain noise (power lin enoise,muscleartifacts).A signal conditioning circuit filters the signal(Band pass filter range:0.5Hz−40Hz).Aninstrumentation amplifier then increases the signal gain by a factorof1000−10000 to make it readable by the ADCof theSTM32.

3) Threshold Detection & Authentication: The STM32 analyzes signal characteristics against storedbencrypted templates. If valid, the SSO token is activated.

4) Blockchain Logging & SSO Access:

Upon successful authentication, the ESP8266 transmits a cryptographic hash of the access event to the permissioned blockchain, ensuring an immutable audit log. The user
is granted unified access to all connected cold-storage

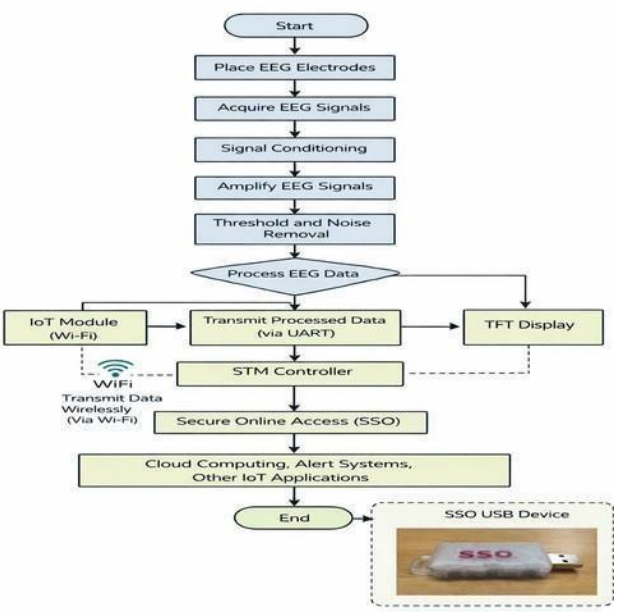

Fig.6 System Operational Flowchart

VII. SYSTEM ADVANTAGES & APPLICATIONS

A. Advantages

The proposed BioLock architecture offers significant improvements over conventional systems:

- **High Security Authentication**: Eliminates password dependency using non-transferable EEGpatterns.
- **Tamper-proof Data Handling:** Blockchain integration ensures logs cannot be altered.
- **Emergency Access Capability**: Smart contracts allow for secure, multi-party predicament recovery (digital wills).
- **True Cold Storage**: Cryptographic keys remain isolated from the network.

B. Applications

•Cryptocurrency cold storage security.
•High-security enterprise and military access control.
•Healthcare data protection databases.
•Digital asset succession planning.

VIII. CONCLUSION

The BioLock system demonstrates a robust and secure authentication framework by integrating EEG-based biometric identification with an STM32 microcontroller,cold storage architecture,and IoT connectivity.By storing sensitive biometric credentials offline and enabling controlled cloud and blockchain interaction,the system significantly reduces the risk of cyber threats while maintaining real-time monitoring and accessibility.

Unlike traditional password-based methods, EEG biometrics utilize unique brain signal patterns that are extremely difficult to replicate. The inclusion of emergency unlock hardware and blockchain-based predicament recovery ensures reliability during critical situations, enhancing system resilience. Overall, the proposed solution offers a scalable, lowpower, and tamper-resistant security model highly suitable for next-generation biometric security systems.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash Sys tem,” 2008.
[2] M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly Media, 2015.
[3] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.
[4] R. Rivest, A. Shamir, and L. Adleman, “A Method for Ob taining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
[5] H. Halpin and M. Piekarska, Digital Identity Management: Technologies and Systems, Artech House, 2010.