Blockchain-based Decentralized Authentication Modelling Scheme in Edge and IoT Environment

INTRODUCTION:

Authentication, one of the most crucial entry points to many information systems, is crucial to information system safety because it guarantees that the appropriate user has access to the proper system with the right identity. At the moment, there are three types of identity authentication technologies available: password-based authentication, certificate-based authentication, and biotechnology-based authentication, such as face, fingerprint, or voice recognition. Everyone is aware that the password-based authentication system keeps the user's password hash value in the database and compares the hash values of the current new passwords to the hash value of the original password that is already saved. The authentication will be accepted if they are consistent; else, it will be refused. Although using a password-based authentication mechanism is simple, there are several severe security issues, such as dictionary attacks and brute force cracking. Digital certificates are used in the authentication process with certificate-based authentication, which is considered as a very safe and dependable method, to guarantee that the identification information is not altered or deleted. By tying together the identity data and associated key of the certificate holder, a digital certificate may successfully address the issue of identity authentication in the network environment. Public-key infrastructure (PKI), which serves as the fundamental architecture of the digital certificate, offers identity establishment and authentication mechanisms in the network through the management of digital certificates. This enables users to easily use encryption, decryption, and digital signature technology in a variety of application scenarios. Biotechnology-based authentication gathers and compares user biometric data, including voiceprint, iris, face, and fingerprint, for the protection of identification information. Compared to traditional identity authentication, biometric-based identification technology offers several benefits, including privacy, portability, strong anti-counterfeiting performance, not being simple to fake or steal, and usage at any time and anyplace. The gathering of biometric data is challenging, though. Private data leaking might occur if the information is not encrypted.

ABSTRACT:

Authentication is the initial step in many information systems, however typical single-sided authentication is brittle and weak, posing a security risk of breakdown or failure brought on by external threats or insider fraud. Blockchain may be used at the edge and Internet-of-Things (IoT) environment to better support the IoT and offer decentralised high security service solutions. In order to offer a more secure, dependable, and robust fault tolerance unique solution, we suggested a blockchain-based decentralised authentication modelling scheme (called BlockAuth) in the edge and IoT environment in this paper. Each edge device is treated as a node to establish a blockchain network. For the purpose of assessing the viability, security, and performance, we created a secure registration and authentication strategy, a blockchain-based decentralised authentication protocol, the blockchain consensus, smart contracts, and an entire blockchain-based authentication platform. According to study and assessment, the suggested BlockAuth scheme offers a unique, decentralised authentication that is more secure, trustworthy, and strong in the face of faults, together with high-level security-driven configuration management. The proposed BlockAuth technique is appropriate for high-level security requirement systems in edge and IoT environments that require password-based, certificate-based, biotechnology-based, and token-based authentication.

EXISTING SYSTEM:

The primary procedure for gaining access to any online application's services, including online banking, insurance access, health record access, and many others, is authentication. All currently used online apps rely on a single, central server that stores user information. These details are checked during user authentication, however this central server is run by internal staff, who may abuse the user database or be hacked by attackers to steal user information. Existing servers can utilise encryption technologies to protect user information, but internal staff can retrieve keys and decode data by keeping track of the encryption and decryption processes.

DISADVANTAGES OF EXISTING SYSTEM:

1. may breach this server's database and take user data
2. Currently, all servers in use offer different types of authentication, including biometric authentication, authentication using a digital certificate and public and private keys, and authentication using a username and password. All of these authentication methods were handled by a single centralised server and are vulnerable to hacking or alteration by malicious users.

PROPOSED SYSTEM:

The author of this work introduces Blockchain technology to existing, safe, decentralised authentication methods in order to address this issue. Since blockchain servers don't need human administration, they establish a decentralised network where each node and IOT device shares user information. If one device goes down, user authentication may still be done using a functional IOT device. Each node in a blockchain will store data as a block or transaction and associate each block with a distinct hash code. This hash code will link all older and newer data blocks together as a chain. All nodes verify the hash codes of all blocks before storing new data blocks to determine if any blocks have been updated or not. If no blocks have been altered, the data is safe and cannot be tampered with in the Blockchain as a result of this verification. Each IOT device server will constitute a group of networks in the proposed paper, and users will be able to execute authentication from any decentralised IOT devices.

Advantages of proposed system:

1. Users of blockchain-based IOT devices are independent of a single centralised server
2. The blockchain's built-in hash verification mechanism prevents tampering with their contents.

SYSTEM ARCHITECTURE:

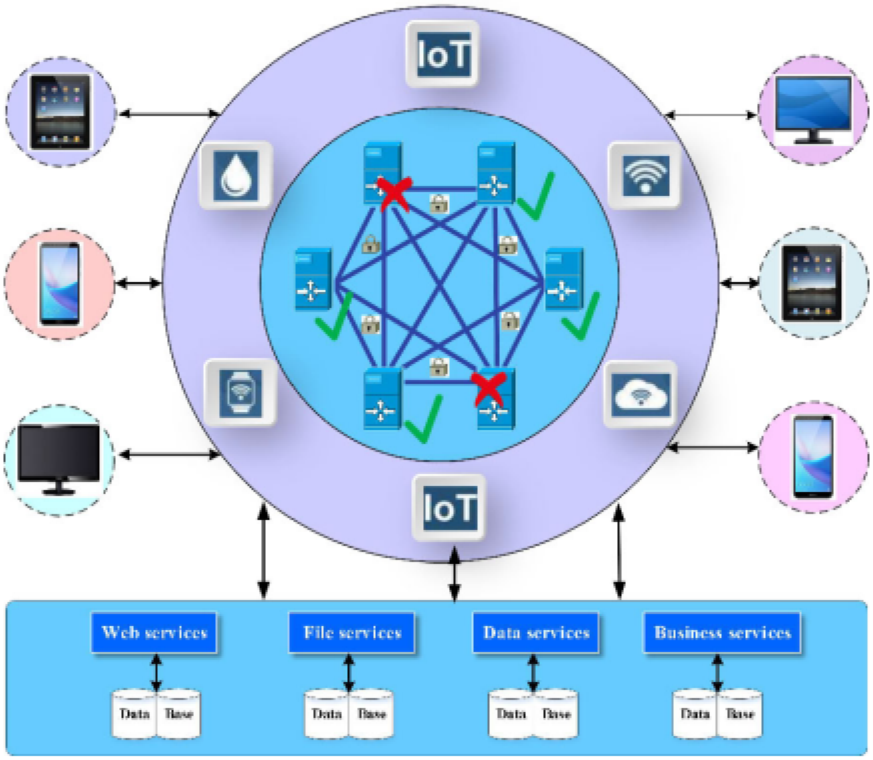

Fig.1: System architecture

REQUIREMENTS:

The following are the specifications for the hardware and software needed to implement the suggested system.

Hardware Requirements

1)Operating System : Windows Only

2)Processor : i5 and above

3)Ram : 4gb and above

4)Hard Disk : 50 GB

Software Requirement

1)Visual Studio Community Version

2)Nodejs (Version 12.3.1)

3)Python IDEL (Python 3.7)

CONCLUSION:

We put forth the BlockAuth Scheme, which may offer a more secure, dependable, robust fault tolerance decentralised innovative authentication solution with high-level security, to address the security and dependability of traditional authentication in the edge and IoT environment. According to this plan, each edge device functions as a node in the blockchain network. To test the viability, security, and performance of our secure registration and authentication strategy and blockchain-based decentralised authentication protocol, we specifically improved blockchain consensus, created smart contracts, and then implemented the entire blockchain-based authentication platform. Our scheme improves security and stability while sacrificing some degree of time complexity, and it satisfies the stringent security and fault tolerance criteria of identity authentication in edge and IoT environments, according to evaluations and comparisons with the relevant current method. Additionally, the scheme we've developed may satisfy the development needs of the global standard authentication method as well as the authentication requirements of many scenarios.