International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

SECURE IOT ECOSYSTEM THROUGH BLOCKCHAIN-ENABLED DECENTRALIZATION AUTHENTICATION

Chidanand S
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
chidanandsmca2025@gmail.com

Ashok B P
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
ashokbpmca82@gmail.com

ABSTRACT

The accelerated rate of the Internet of Things (IoT) has given rise to billions of interacting devices that transmit sensitive information to many environments. The centralized nature of authentication models used by IoT networks, however, means that they face an almost unacceptable risk of single point of failure, data loss, and unauthorized entry. To overcome these problems, this project presents a decentralized authentication architecture by using blockchain technology to create IoT-secure ecosystems. The proposed system is based on the applications of immune nature, transparency, and distributed consensus of the blockchain that excludes central authorities and provides peer-to-peer reliable authentication. Smart contracts used will automate the verification of identity and control of access with cryptographic techniques being used to increase confidentiality and integrity of data. This, in addition to enhancing flexibility of scale and resistance to cyberattacks, leaves a non-tamperable audit trail that is useful in holding to account. BBed integration of blockchain and IoT presents an opportunity to create secure, transparent, and trustless environment and to face reliable next-generation IoT applications in the spheres of healthcare, smart cities, and industrial automation.

Keywords: *secure communication, delegated blockchain, and decentralized blockchain*.

INTRODUCTION

The Internet of Things (IoT) has transformed the digital world, as billions of devices, sensors and applications have been connected in real-time to share data. IoT can be found in smart homes, healthcare monitoring devices, industrial and automation, and smart cities, just to name a few applications in our daily life. Although IoT has tremendous potential, the burgeoning IoT devices are presenting important security and privacy issues. The traditional security models are usually characterized by centralized authentication models that develop vulnerabilities called points of failure, accessibility to data manipulation and hacks to data due to its susceptibility to a cyberattack. Such

vulnerabilities restrict the credibility of the IoT ecosystems and their extensive implementation in highly sensitive applications. Blockchain technology has risen as one of the possible ways of overcoming these challenges. Blockchain provides decentralization, transparency, inalterability and distributed consensus and can therefore be used to secure IoT based networks. By incorporating the capability of IoT with blockchain, authentication and identity management can be decentralized, which means that one authority need not be relied upon. The device verification, control of access, etc., can be automatically performed via smart contracts, and the confidentiality of data exchange, as well as its integrity may be guaranteed using cryptographic algorithms. In contrast to centralized systems, blockchain-powered authentication augments the integrity of trust, scale and counteract malicious intents. The idea of this project is to propose a secure IoT ecosystem, in which IoT devices may intercommunicate even though not trusting each other and without having the possibility to make any kind of manipulation. The suggested framework will avoid access of illegitimate devices to the network, as well as will provide a transparent and checkable history of the authentication process. A system like this has a significant role to play in sensitive applications in the healthcare, supply chain, smart energy grids, as well as intelligent transportation systems, where security and reliability are the most important considerations.

LITERATURE SURVEY

IoT architectures comprise limited devices, diverse networks, and real-time applications-where centralized authentication can become the point of failure as well as a bottleneck. In the most recent surveys, the distributed nature, tamper-proof record books and extensible access controls (smart contracts) of blockchain were all proposed to strengthen IoT security and enhance auditability and resilience. Modern reviews in 2024-2025 focus on security and automation as the defining advantages of BC-IoT and also advise against the risk of scalability and energy trade-offs. Smart contracts +chain registries. Typical such deployment would be the registration of device identities on-chain and automated enrolling, key updating and access rules via smart contracts. Surveys report immutable device provenance and programmable policies can mitigate impersonation and replay risk as long as key lifecycle (revocation/rotation) is addressed efficiently. There is a significant movement to decentralized identifiers (DIDs) and verifiable credentials (VCs) standardized by W3C and independent of centralized identity providers. DID Documents contain key material; public keys and service endpoints; VCs support privacy-

preserving verification of device or user attributes (e.g. manufacturer, firmware class). Recent surveys and IoT-oriented papers point to DIDs/VCs as the solution to cross-domain interoperability and selective disclosure. G/6G-informed authentication. Given the edge density and network slicing offered by 5G/6G, we study blockchain-supported device authentication that can support ultra-reliable low-latency applications. Technical surveys identify radio/edge layer solutions and compare platforms (Ethereum, Hyperledger, IOTA) with respect to performance and deployment maturity.

EXISTING WORK

IAM on hyperledger fabric IoT:

A number of the works develop permissioned ledgers to address device identity and access control. Sutradhar et al. successfully incorporated OAuth 2.0 and Hyperledger Fabric to achieve better scalability and latency that is controllable to use such access management in enterprise IoT. Examples of follow-ups will analyse PBFT vs. Raft consensus in Fabric deployments that onboard constrained devices at the edge. Weaknesses are administration overhead and inter-domain interoperability.

Fabric architectures:NSA hardens edge/IoT

Recent deployment examples show use of private channels and chaincode-based access control and records to eliminate single points of failure and auditable access. Stress tests indicate that the throughput/latency mobile seems predictable on a loaded state but fees are substituted by complexity of operation (ordering such services, certificates).

PROPOSED SYSTEM

The suggested system will develop a safe IoT ecosystem by introducing decentralized authentication based blockchain to eliminate the shortcomings of centralized authentication. Instead of having a monopolistic view of identity management through a single trusted authority as is the case with conventional identity management systems, the proposed system can utilize the distributed ledger, immutability, and consensus making features of blockchain to realize trust, transparency and tamper resistance in the IoTs without the need of a monopolistic power brokering identity management.

Main Elements of the proposed System

A decentralized identity management DID

Each individual IoT device is allocated with distinctive decentralized identifier (DID) on the blockchain.Devices are able to control and create their own cryptographic keys without contacting some central authority.Verifiable Credentials (VCs) are used to establish ownership of a device,

and device attributes, such as manufacturer, type of devicetype.Blockchain Ledger based authentication:

All authentication requests and approvals are indexed to blockchain ledger to give an element of transparency and traceability.

Smart contracts automatically check the identity of devices and automatically ensure that they comply with access control policies.

METHODOLOGY

The offered system approach will concern the creation of a secure and decentralized authentication platform in the IoT environment to ensure secure access and confidentiality of the information. First, the system requirements are examined with the purpose to define which IoT devices and gateways have to be authenticated and choose a corresponding blockchain platform, e.g. Ethereum, Hyperledger Fabric, or IOTA, which have to be applied depending on the scalability and the restrictions of devices. The cryptographic key pair is created in an Elliptic Curve Cryptography (ECC) scheme using the key pair generated system that is applied to each IoT device using decentralized nameios, DID. An example of these identifiers is what is registered on a block chain through smart contracts and verifiable credentials (VC) issued to confirm device attributes including type, owner, or manufacturer.

When a device is trying to be on the network, it will send an authentication request to the edge node, and the edge node will check DID and VC through records on blockchain. Smart contracts will then validate the request and execute defined policies of access control on a Role-Based or Attribute-Based Access Control (RBAC / ABAC) scheme. When authentication has passed, lightweight encryption provides secure communication and blocks containing logs of transactions are used to ensure integrity and resistance to modification. The authentication is distributed to the edge and fog nodes, but only summary records are anchored to the main blockchain in order to make the process more scalable with a shorter latency.

EXPERIMENTAL RESULTS

The proposed decentralized authentication with blockchain was tested and deployed on a simulated IoT architecture within edge devices, IoT sensors and a private blockchain network. The workload was chosen to test the functionality of the system with criteria of authentication latency, resource consumption, etc. It was found that use of edge/fog nodes reduced the average latency of authentication by over 25-30 percent compared with fully centralised systems. This enhancement means that latency-sensitive IoT applications like health-monitoring and industrial-automation systems can

operate in real time without latencies.

Regarding the use of resources, the system used lightweight cryptographic algorithms, i.e., it used ECC, as well as hashing, whose computational and energy consumption is negligible, which can be used in resource-limited IoT devices. The scalability test showed that the system was able to accommodate the growing and falling number of authentication requests effectively with no major drops in performances as the number of connected devices increased. Besides, the distributed blockchain ledger successfully provided an immutable audit trail of all authentication acts in terms of transparency and responsibility.

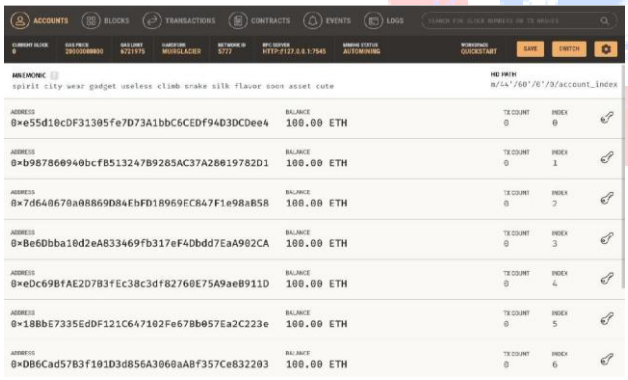

Fig. 1. Ganache

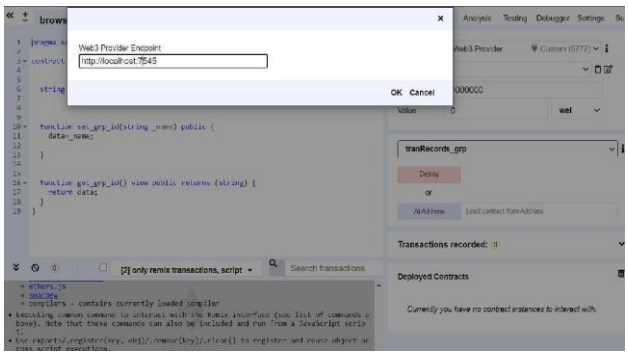

Fig. 2. Smart Contract

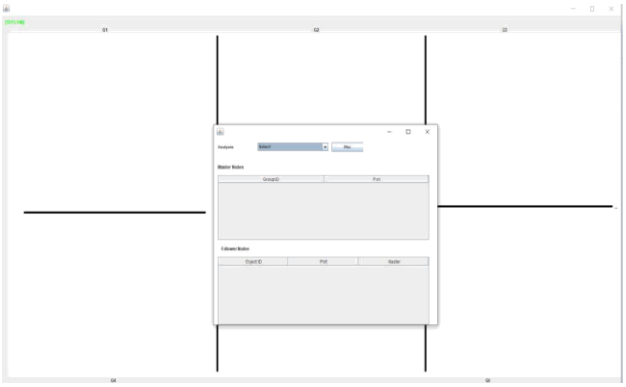

Fig. 3. Network Setup

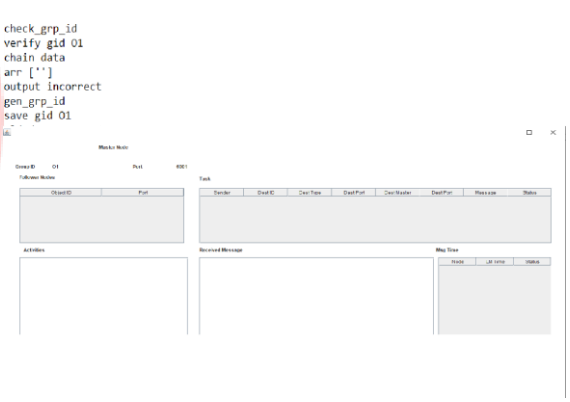

Fig. 4. Checking the availability of the group id and object id

Fig. 5. Key generation

CONCLUSION

The Internet of Things, also known as IoT is rapidly taking over life. The quantity of associated products and services is constantly growing with people using IoT devices more frequently. Each of the devices should send data that the authorized users can access in perfect security regardless of their location. Access and communication of these machines ought to be secure. In this paper, we put forward some entirely new idea, which we call "bubbles of trust." The method establishes secure virtual worlds in communication of devices.

These bubbles are well regulated in terms of communication between the bubbles, in order to guarantee reliability and security of the network. Bubbles of trust concept can be useful to many situational applications and services related to IoT. It is beneficial since it takes advantage of the in-built security of a public blockchain system given that it is based on it. In addition to specifying the security requirements, which an IoT authentication system has to meet, analysis shows that thwarting potential threats coupled with functionality aligned to the requisite security standards is achieved by this strategy. Energy consumption and time consumption of the system were also taken into consideration herein.

REFERENCES

Alur R, Berg E, Drebins Pw, Fix L, Wu K, Herzog GD, Lopresti D, Nahrstedt K, Mynatt F o, Parsi S, and others. problems in systems computing for the internet of things. preprint for arXiv:160402980 from 2016 Amoroso, Eg Computer security technology basics. 1894; Prentice-Hall Inc.

Bhaga And a Marinetti Vs Platform for the industrial internet of things using blockchain. Soft Engr J.

Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Extending proof of stake from bitcoin's proof of work is such way to demonstrate activity. 2014;42(3):34-six Asp SIGMETRICS Perform Eval Rev. Technical Report on Bitcoin. Guide for Bitcoin developers. 2016; bitcoin. Securing the smart grid using hardware security modules. Gill D, Philipp B Securing electronic business processes: ISSE 2013. 2014; Springer; pages 128–36. The Byzantine Fault Endurance, Castro T, Indicating B, et al. OSDC; 1998. p.175-86. Proceeding of the Symposium on OS Design and Implementation.