The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.06 Issue 05 2026
PAGE NO. 49-52
DOI 10.37547/ajast/Volume06Issue05-08

A Practical Blockchain-Based Authentication Approach for Secure IoT Systems Using Spatial Verification

Seidullayev M.K.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Received: 25 March 2026; **Accepted:** 24 April 2026; **Published:** 11 May 2026

Abstract: With the rapid growth of the Internet of Things (IoT), ensuring secure communication between devices has become one of the most critical challenges in modern networks. Many existing solutions focus only on identity-based authentication, which is often insufficient against more advanced attacks such as spoofing or location-based intrusions. In this work, a new authentication model is proposed that combines blockchain technology, spatial verification through angular distance, and lightweight hybrid cryptography.
The idea behind this approach is simple but effective: instead of trusting a device only based on its identity, the system also verifies where the device is located. At the same time, blockchain is used to store authentication records in a secure and tamper-resistant way, while smart contracts automate the decision-making process. Simulation results show that the proposed method performs reliably even as the number of devices increases, while keeping computational and energy costs relatively low. This makes it suitable for real-world IoT environments.

Keywords: Internet of Things (IoT), Blockchain Security, IoT Authentication, Spatial Verification, Angular Distance Authentication, Lightweight Cryptography, Smart Contracts, Merkle Tree, Elliptic Curve Cryptography (ECC) and ASCON Encryption.

INTRODUCTION

IoT technologies are becoming a fundamental part of modern life, from smart homes to industrial automation. However, as the number of connected devices increases, so does the attack surface. Many IoT devices are limited in terms of processing power and energy, which makes it difficult to apply traditional security mechanisms directly.

One of the most common problems in IoT systems is authentication. In many cases, devices are authenticated only based on their identifiers. This creates a serious vulnerability, because an attacker can imitate a legitimate device by stealing or forging its ID.

To overcome this issue, researchers have started to explore blockchain-based solutions. Blockchain provides transparency, immutability, and decentralization, which are highly desirable properties for secure systems. However, relying only on blockchain is not enough.

In this work, we take a different approach. Instead of focusing only on identity, we introduce an additional verification layer based on the physical location of the device. This is achieved using an angular distance method. By combining this with blockchain and lightweight cryptography, we aim to build a system that is both secure and practical.

2. Key Concepts Behind the Proposed System

2.1 Spatial Verification Using Angular Distance

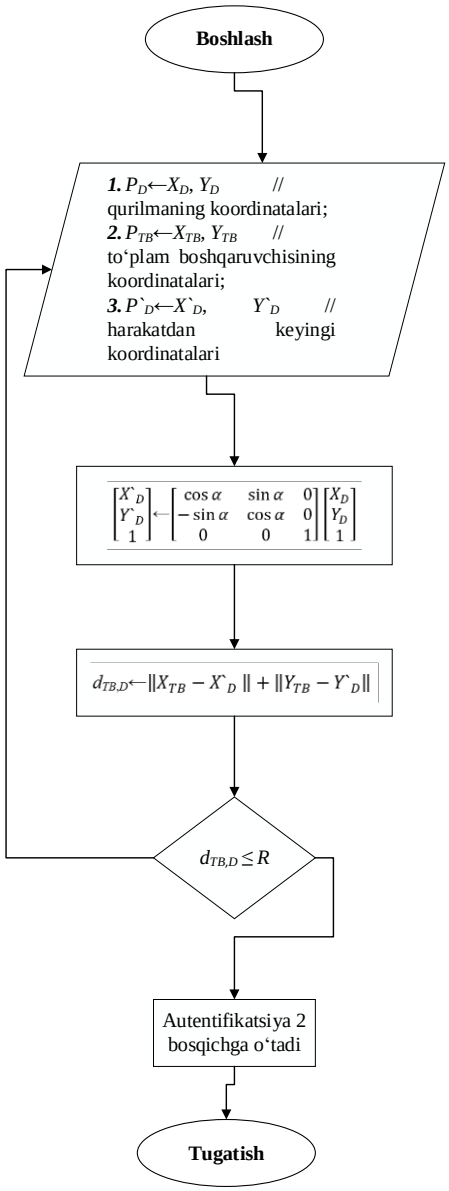
One of the main ideas in this work is to verify not only who the device is, but also where it is. This is important because many attacks involve devices trying to connect from unauthorized locations.

To handle this, we use a concept called angular distance. In simple terms, it measures how far a device is from the cluster controller based on its

coordinates. If a device is outside the allowed region, it will not be accepted into the system.

When a device moves, its position can be recalculated using a rotation model. After that, the distance between the device and the controller is computed. If this distance is within a predefined threshold, the device is considered valid.

As described in the original system design , this approach helps detect devices that try to fake their location, which is something traditional authentication methods cannot handle.



CC

2.2 Blockchain and Merkle Tree Usage

Blockchain is used in this system as a secure storage layer. Every authentication event is recorded as a transaction, and these transactions are grouped into blocks.

To make verification efficient, a Merkle tree structure is used. Instead of checking all transactions one by one, the system only needs to verify a small set of hash values. This significantly reduces the workload, which is especially important for IoT devices.

Another advantage of blockchain is that once data is stored, it cannot be changed. This ensures that all authentication records remain trustworthy.

2.3 Smart Contracts for Automation

Smart contracts are used to automate the authentication process. They act like rules written in code: when certain conditions are met, specific actions are executed automatically.

For example:

- If a device passes identity and location checks → it is approved.
- If not → access is denied.

- cThis removes the need for manual control and reduces the possibility of human error.

2.4 Hybrid Cryptography

The system uses a combination of symmetric and asymmetric cryptography.

- Symmetric encryption (ASCON) is used for fast and efficient data encryption.
- Elliptic Curve Cryptography (ECC) is used for secure key exchange.

This combination provides both security and efficiency, which is crucial for IoT systems.

3. How the System Works

The authentication process is carried out in several steps.

First, a device generates a request using its ID, a random number, and a timestamp. This ensures that each request is unique.

Then, the cluster controller receives the request and performs several checks:

- It verifies the timestamp to prevent replay attacks,
- It calculates the angular distance to confirm the device's location,
- It checks the integrity of the message using a hash function.

If everything is valid, the controller creates a blockchain record and sends it to the blockchain server.

After that, the server verifies and distributes the record across the network.

Finally, the device receives a response and establishes a secure connection using the provided cryptographic parameters.

4. Security Discussion

The proposed method improves security in several ways.

First, identity spoofing becomes much harder because authentication is not based on ID alone. Even if an attacker copies an ID, they also need to match the physical location.

Second, replay attacks are prevented using timestamps. Old messages cannot be reused.

Third, blockchain ensures that all authentication records are protected against modification.

Finally, the use of ECC and ASCON ensures that communication remains secure without placing too much burden on the device.

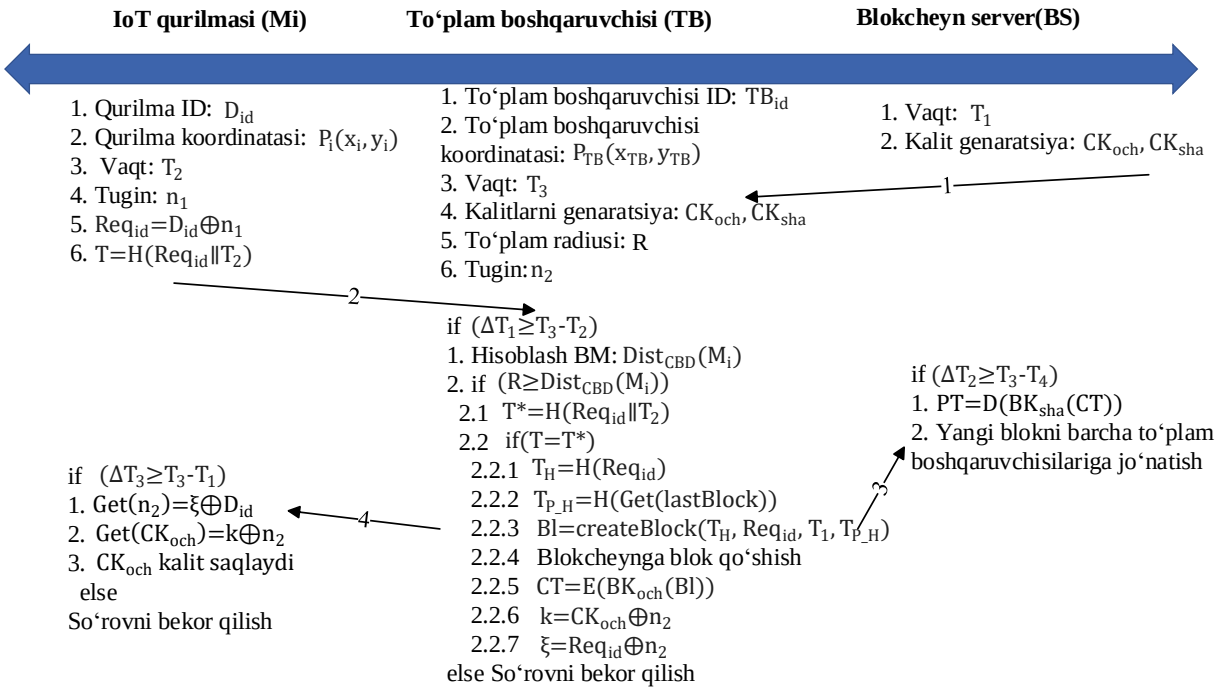
5. Performance Considerations

The system was tested in a simulation environment where multiple IoT devices were connected.

The results show that:

- The authentication process is reliable,
- Malicious devices are successfully detected,
- The system remains stable even as the number of devices increases,
- Energy consumption stays relatively low.

These results indicate that the proposed approach is practical and can be applied in real IoT systems.



Conclusion

In this paper, a new IoT authentication model was presented that combines spatial verification, blockchain, and hybrid cryptography. Unlike traditional approaches, the proposed method considers both identity and location, which significantly improves security.

At the same time, the system is designed to be lightweight and efficient, making it suitable for real-world applications.

Future work may include testing the system in real hardware environments and further optimizing its performance.

References

1. Kevin Ashton, “That ‘Internet of Things’ Thing,” RFID Journal, 2009.
2. Gartner, “Internet of Things Technologies and Market Analysis,” 2020.
3. Cisco, “Internet of Things Global Report,” 2021.
4. oneM2M, “Global IoT Standards Initiative Report,” 2022.
5. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
6. Ralph C. Merkle, “Protocols for Public Key Cryptosystems,” IEEE Symposium on Security and Privacy, 1980.
7. Vitalik Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” 2014.
8. NIST, “Lightweight Cryptography Standardization Process,” 2023.
9. Dobraunig, C., Eichlseder, M., and Mendel, F., “Ascon v1.2: Submission to the CAESAR Competition,” 2016.
10. Hankerson, D., Vanstone, S., and Menezes, A., Guide to Elliptic Curve Cryptography, Springer, 2004.
11. Dorri, A., Kanhere, S. S., and Jurdak, R., “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, 2017.
12. Christidis, K., and Devetsikiotis, M., “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, 2016.
13. Singh, S., Sharma, P. K., Moon, S. Y., and Park, J. H., “Advanced Lightweight Encryption Algorithms for IoT Devices,” Future Generation Computer Systems, 2019.
14. Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F., “Internet of Things Security: A Survey,” Journal of Network and Computer Applications, 2017.
15. Internet of Things va blokcheyn asosidagi xavfsizlik tizimlari bo‘yicha zamonaviy ilmiy sharhlar, Springer, 2025.