IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Smart Contract Powered IoT Software Update System Using Blockchain and CP-ABE

[1]MONGAM YELLAJI,
Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]CH KODANDA RAMU, Miracle Educational Society Group of Institutions
[3]A SRINIVASA BABU, Miracle Educational Society Group of Institutions
[1]yellajimongam123@gmail.com

ABSTRACT:

This research proposes a novel, secure, and low-cost approach to updating Internet of Things (IoT) devices using blockchain technology. Existing update mechanisms either pose a risk of attacks or have a substantial computational burden on the resource-constrained IoT devices. This system applies blockchain technology for transparency and immutability, uses Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for selective access, and utilizes IPFS for decentralized file storage. Smart contracts certify the delivery of the software and stipulate payment terms. In addition, update verification is secured using the Elliptic Curve Digital Signature Algorithm (ECDSA) to verify integrity. With blockchain technology, these systems can achieve confidentiality, decrease reliance on central systems, and improve trust for the given system. The proposed framework has been implemented and tested which demonstrated secure, efficient, and scalable results.

Keywords: CP-ABE, blockchain, ECDSA

INTRODUCTION

The Internet of Things (IoT) is a game-changer as it allows devices to collect and share data. The connected devices pose enormous security risk, especially for receiving timely updates. Existing update approaches depend on a centralized server which is a weakness on focus for these systems. This project provides a solution for a decentralized software update system based on blockchain technologies that solves the above-stated issues. Using smart contracts, CP-ABE encryption, and IPFS for decentralized storage, the update delivery system described is secure, efficient, and tamper proof. Additionally, the persisting absence of any single points of failure and the transparent audit trails the system provides is vital for compliance-driven industries such as healthcare and energy. Furthermore, not only CP-ABE and IPFS based systems strengthen IoT security, they also enhance the ease of the update mechanism, thus improving reliability, scalability, and efficiency in a wider range of IoT systems.

RELATED WORK

Within the last few years, many researchers have been trying to build frameworks that focus on improving the efficiency of secure software updates and inter-device communication for IoT systems. Zhang and Green (2014) focused on mitigating the security issues of IoT networks, in particular, the DDoS attacks and pointed out the importance of lightweight communication security algorithms to the constrained resource devices. This was the first attempt to understand the vulnerability of IoT systems to external attacks. Alsaadi and Tubaishat (2017) studied the problem of eavesdropping and node capture attacks in IoT systems and proposed stronger encryption and more distributed algorithms to address the vulnerabilities. Huh et al. (2017) created an Ethereum and smart contract-based framework for managing IoT devices via blockchain. Their work illustrated a method for securely and decentralized managing device configuration and authentication through the mechanism of storing public keys on-chain and private keys off-chain. The work of Samaniego and Deters (2016) also proposed Blockchain as a Service BaaS for IoT. Their work indicates and improves the performance and scalability of blockchains hosted in the cloud and on the edge in their ability to manage IoT data. Samaniego and Deters (2017) later on, in a different study, designed a framework for relocating software-defined IoT devices to the edge on the IoT employing blockchains for better network latencies and security. They recommended microservices architectures for easier modular, dynamic, and secure software.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author(s)	Contribution	Impact on Current Research
Zhang and Green (2014)	Proposed a lightweight DDoS prevention algorithm for IoT networks	Inspired focus on securing IoT communication and minimizing resource consumption
Alsaadi and Tubaishat (2017)	Analyzed IoT vulnerabilities like eavesdropping and node capture	Highlighted the need for advanced encryption and decentralized architectures
Huh et al. (2017)	Developed Ethereum-based IoT device management using smart contracts	Introduced blockchain-based identity and access management for secure software interactions
Samaniego and Deters (2016)	Proposed Blockchain-as-a-Service (BaaS) for managing IoT data	Demonstrated benefits of using cloud and edge-hosted blockchains for data integrity and scale
Samaniego and Deters (2017)	Shifted software-defined IoT components to the edge using blockchain	Validated blockchain's role in efficient and secure distributed IoT software deployment

PROPOSED APPROACH

The proposed system describes an IoT environment response to resource challenged environments with an infrastructure-less software update method supported by blockchains. The framework proposes integrating emerging technologies to guarantee the secure, efficient, and verifiable delivery of software. The system leverages blockchain technology as the foundational technology providing an immutable ledger capable of securely tracking records and events for updates, transactions, and audits. The use of smart contracts on platforms such as Ethereum automate user authentication, update authorization, and payment for the subsequent transactions thereby enforcing payment. In order to secure update content, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is utilized. This enables a single encryption for updates, granting access exclusively to authorized IoT devices, which in turn, reduces the computational burden on the manufacturer. In addition, update integrity is verified via ECDSA digital signatures. Due to the exorbitant storage cost using blockchain, the system leveres IPFS to store large encrypted update files off-chain. Only the IPFS hash references are stored on the blockchain which allows for retrieval while retaining decentralization.

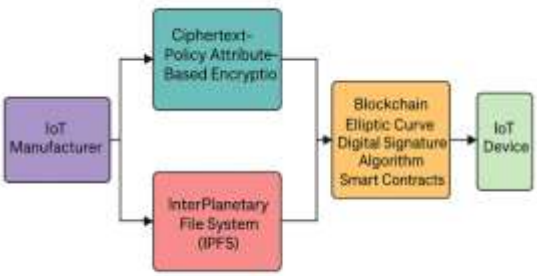


Figure 1: Proposed software updates System

METHODOLOGIES

The methodology for this project involves designing and implementing a secure, decentralized IoT software update system using blockchain, CP-ABE encryption, smart contracts, and IPFS. The development follows a modular approach, focusing on four core components: user management, update encryption and delivery, payment processing, and verification.

1. User Management

IoT manufacturers and owners register through a Django-based web application. User details—such as credentials and roles—are securely stored on the blockchain to prevent unauthorized access and modification.

2. Encryption and Upload Process

Manufacturers upload software updates, which are divided into smaller blocks for scalability. These blocks are encrypted using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), allowing only specified IoT devices (based on attributes) to decrypt the files. This reduces redundant key generation and minimizes computational strain on devices.

3. Storage via IPFS

Since blockchain is inefficient for storing large files, the encrypted blocks are stored in the InterPlanetary File System (IPFS), a decentralized storage system. The system then stores the corresponding IPFS hashes on the blockchain, ensuring data immutability and retrievability.

4. Smart Contract Integration

Smart contracts, written in Solidity, manage update verification, purchase authorization, and automatic logging of transactions. These contracts ensure that

updates are only accessible after valid payment and proper authorization. They also generate audit trails for regulatory compliance.

5. Verification and Payment

To verify the authenticity of updates, Elliptic Curve Digital Signature Algorithm (ECDSA) is used. Devices compare hash values before and after decryption to confirm integrity. Payment details are also stored immutably on-chain, ensuring transparency and traceability.

RESULTS

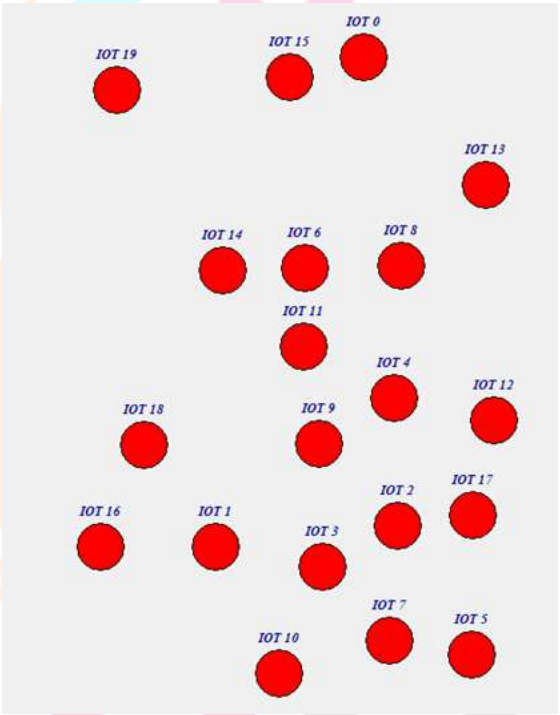
The proposed blockchain-facilitated IoT software update framework was implemented and tested in a simulated environment using Django, Web3.py, IPFS, and Ethereum smart contracts. The results demonstrate the system's effectiveness in providing secure, decentralized, and efficient software update delivery.

Upon testing, the encryption and decryption processes using CP-ABE proved significantly faster and more scalable than traditional key generation methods, especially for large numbers of IoT devices. The storage of update files in IPFS allowed for reduced blockchain memory usage while maintaining immutability and easy retrieval using unique content hashes. Smart contracts successfully managed update access and payment validation, ensuring that only authorized IoT owners could retrieve and decrypt updates.

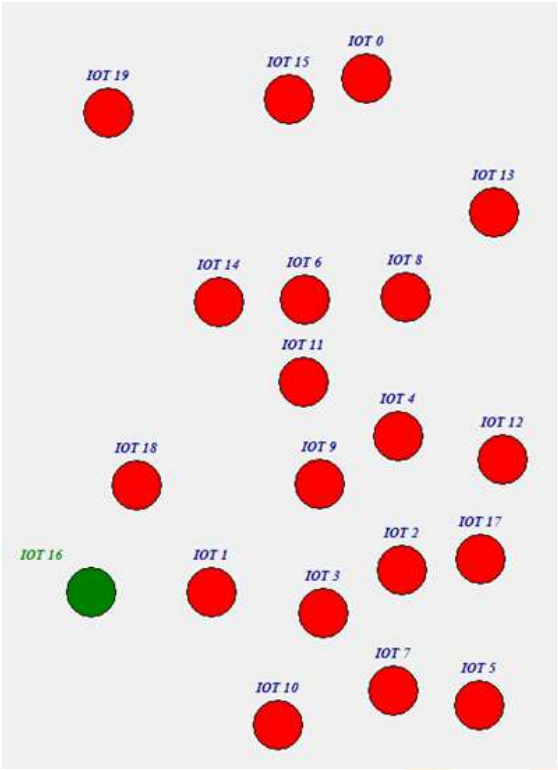
Security tests showed that the use of ECDSA hash validation effectively detected any tampering with update files. Moreover, the system withstood simulation of rollback and spoofing attacks, confirming the robustness of the blockchain's immutability and access control mechanisms.

Same file multiple blocks are generated and we can see name of file, name of blocks, encrypted content and verification code

All files and their blocks



IOT nodes and are placed at different location



The IOT for which IOT owner purchase updates will receive and changed its colour to green to indicate as its receiving updates.

DISCUSSION

The implementation and testing of the proposed framework highlight several key benefits and areas for further exploration. The integration of blockchain technology and smart contracts effectively addresses traditional issues in IoT software updates such as data tampering, fake payments, and unauthorized access. By ensuring that all transactions and update logs are stored immutably, the system enhances transparency and compliance, particularly in highly regulated sectors.

The use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) offers a practical solution for reducing the computational burden on manufacturers and devices. Unlike conventional encryption schemes that require generating separate keys for each recipient, CP-ABE enables a single encryption process for multiple authorized users. This efficiency is critical for scaling the system across large IoT networks.

Storing encrypted updates on IPFS rather than on-chain significantly cuts storage costs and avoids blockchain size limitations, while still preserving file traceability through hash references. Moreover, the verification mechanism using ECDSA proved successful in detecting file integrity breaches, ensuring only valid and unaltered updates are installed.

CONCLUSION

This project illustrates the construction of an IoT update system using blockchain, CP-ABE, IPFS, and smart contracts providing solid security and borderless agility. The system incurs and mitigates critical security risks, such as unauthorized access, counterfeiting, and dummy payments using a decentralized framework and cryptographic verification. The use of blockchain offers transparency and immutability, while the need for encryption to multiple authorized devices is resolved by CP-ABE, eliminating the need for multiple unnecessary key generations. IPFS provides the instant availability and low cost of storing encrypted files; and during the entire procedure, ECDSA safeguards the data integrity. The construction was successfully tested and demonstrated strong performance against rollback and spoofing attacks. Thus, in addition to boosting security and reliability in IoT ecosystems, this framework reduces operational complexity for manufacturers. It has real-world applicability in healthcare, smart homes, and industrial automation, paving the way for more innovations for secure, decentralized software update mechanisms.

REFERENCES

[1] S. Poslad, ‘‘Ubiquitous computing: Basics and vision,’’ in Ubiquitous Computing: Smart Devices, Environments and Interactions. Hoboken, NJ, USA: Wiley, 2011, pp. 1–40.

[2] F. Wortmann and K. Fluchter, ‘‘Internet of Things,’’ Bus. Inf. Syst. Eng., vol. 57, no. 3, pp. 221–224, 2015.

[3] (Jun. 2019). Global Internet of Things (IoT) Market Size and Forecast To 2026. [Online]. Available: https://www.verifiedmarketresearch. com/product/global-internet-of-things-iot-market-size-and-forecast-to2026/

[4] (Dec. 2020). Global Internet of Things (IoT) Market By Software Solution, Report ID 6403. [Online]. Available: https://www.verifiedmarketresearch. com/product/global-internet-of-things-iot-market-size-and-forecast-to2026/

[5] (Jan. 2020). Internet of Things (IoT) in the US. [Online]. Available: https://www-statista-com.libproxy.scu.edu/study/61733/internet-ofthings-iot-in-the-us/

[6] (Jan. 2020). Size of the Internet of Things (IoT) in Retail Market in the United States From 2014 to 2025. [Online]. Available: https://wwwstatista-com.libproxy.scu.edu/statistics/688756/iot-in-retail-market-inthe-us/

[7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ‘‘DDoS in the IoT: Mirai and other Botnets,’’ Computer, vol. 50, no. 7, pp. 80–84, 2017.

[8] L. H. Newman. (2016). The Botnet That Broke the Internet Isn’t Going Away. [Online]. Available: https://www.wired.com/2016/12/botnet-brokeinternet-isnt-going-away/

[9] C. Zhang and R. Green, ‘‘Communication security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network,’’ in Proc. 18th Symp. Commun. Netw., 2015, pp. 8–15.

[10] Newman. (Oct. 2016). What We Know About Friday’s Massive East Coast Internet Outage. [Online]. Available: https://www.wired.com/ 2016/10/internet-outage-ddos-dns-dyn/

[11] (Mar. 2016). Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid. [Online]. Available: https://www.wired.com/2016/03/insidecunning-unprecedented-hack-ukraines-power-grid/

[12] (Mar. 2016). Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. [Online]. Available: https://media. kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/2008 1514/E-ISAC_SANS_Ukraine_DUC_5.pdf

[13] J. Cappos, J. Samuel, S. Baker, and J. H. Hartman, ‘‘A look in the mirror: Attacks on package managers,’’ in Proc. 15th ACM Conf. Comput. Commun. Secur., New York, NY, USA, Oct. 2008, pp. 565–574.

[14] E. Alsaadi and A. Tubaishat, ‘‘Internet of Things: Features, challenges, and vulnerabilities,’’ Int. J. Adv. Comput. Sci. Inf. Technol., vol. 4, no. 1, pp. 1–13, 2015.

[15] S. Huh, S. Cho, and S. Kim, ‘‘Managing IoT devices using blockchain platform,’’ in Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT), 2017, pp. 464–467.

[16] M. Samaniego and R. Deters, ‘‘Blockchain as a service for IoT,’’ in Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun.

(GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), 2016, pp. 433–436.

[17] M. Samaniego and R. Deters, ‘‘Using blockchain to push software-defined IoT components onto edge hosts,’’ in Proc. Int. Conf. Big Data Adv. Wireless Technol., Nov. 2016, pp. 110–119.

[18] D. Li, R. Du, Y. Fu, and M. H. Au, ‘‘Meta-key: A secure data-sharing protocol under blockchain-based decentralized storage architecture,’’IEEENetw. Lett., vol. 1, no. 1, pp. 30–33, Mar. 2019.

[19] A. Dorri, S. S. Kanhere, and R. Jurdak, ‘‘Towards an optimized BlockChain for IoT,’’ in Proc. 2nd Int. Conf. Internet-Things Design Implement., Apr. 2017, pp. 173–178.

[20] T. Placho, C. Schmittner, A. Bonitz, and O. Wana, ‘‘Management of automotive software updates,’’ Microprocessors Microsyst., vol. 78, Oct. 2020, Art. no. 103257.