AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

Efficient IOT Firmware Management System with Hybrid Encryption and Cross-Interface Compatibility

N. Rajender Reddy[1], Gunda Narender Reddy[2], Anthargam Pavan[2], Gade Laxmiprasanna[2], Jittaboina Anusha[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

The Internet of Things (IoT) has rapidly evolved, transforming how devices communicate, collect data, and automate processes. Since its introduction in 1999, IoT has benefited from advancements in embedded systems, wireless communication, and networking protocols. However, early IoT infrastructures faced significant limitations, including low computational capacity, weak security mechanisms, and heavy reliance on centralized systems for software updates. Traditional update methods, such as centralized servers and Over-The-Air (OTA) systems, introduce vulnerabilities like single points of failure, cyberattack risks, scalability issues, and lack of transparency, ultimately affecting system reliability and trust. To overcome these challenges, this work proposes a decentralized software update management framework that integrates blockchain technology with the Inter-Planetary File System (IPFS). The system leverages Ethereum smart contracts to securely manage user registration, update metadata, and transaction records in a transparent and immutable manner. A hybrid encryption approach combining Elliptic Curve Integrated Encryption Scheme (ECIES) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used to ensure secure data transmission, fine-grained access control, and strong confidentiality. Encrypted software updates are stored on IPFS as content-addressed data, enabling tamper-resistant and distributed storage without dependence on centralized infrastructure. Additionally, a Django-based web interface facilitates user interaction, while a Tkinter-based simulation models real-time IoT update distribution. The proposed framework enhances security, scalability, and transparency, offering a robust and efficient solution for modern IoT software update management.

Keywords: Internet of Things (IoT), blockchain, decentralized software update management, Ethereum smart contracts, InterPlanetary File System (IPFS), hybrid encryption.

1.INTRODUCTION

The Internet of Things (IoT) has gained widespread adoption in recent years due to its ability to provide convenience, ease of use, and numerous benefits across various aspects of human life. Particularly over the last five years, its rapid growth has established IoT as a dominant standard for low-power and lossy networks with constrained resources [1]. However, this increasing popularity has also made IoT devices attractive targets for cyber adversaries.

According to Miessler and Smith, IoT systems exhibit several critical vulnerabilities, many of which arise from inadequate device management practices. As shown as Figure 1 These vulnerabilities include insecure network services and interfaces, lack of secure update mechanisms [2], reliance on outdated or insecure components, insufficient privacy protection, insecure data transmission and storage, weak device management protocols, and unsafe default configurations. Ineffective management of IoT devices by manufacturers or users can lead to multiple adverse consequences for the devices themselves. To safeguard IoT devices against cyber threats and malware attacks, it is essential to keep their firmware up to date [3]. Firmware refers to the set of instruction codes and commands embedded within an IoT device to perform specific functions. These instructions consist of programmed routines that manage

various components and operations of the device. Traditionally, firmware updates are distributed from the device manufacturer (vendor) to IoT devices via the Internet, a process commonly known as Firmware Over-the-Air (FOTA) [4].

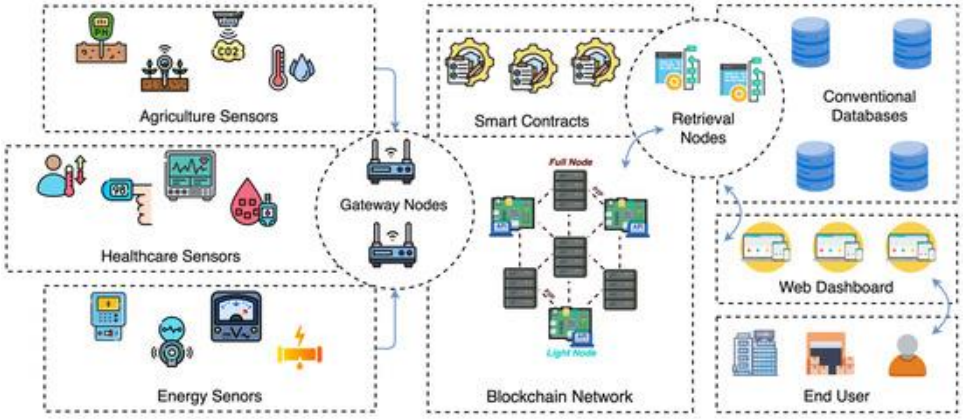


Figure 1: Detailed overview of blockchain-integrated framework.

The FOTA approach follows a centralized client-server model, where the manufacturer's firmware management center (FMC) functions as the server and IoT devices act as clients during the update process. However, as the number of deployed IoT devices increases significantly, the FMC may struggle to deliver updated firmware to all devices within a limited timeframe [5]. Additionally, simultaneous update requests from numerous devices can lead to excessive network congestion. Furthermore, IoT devices must maintain continuous Internet connectivity to receive firmware updates from the FMC [6]. Therefore, a secure and reliable firmware update framework for IoT environments should eliminate dependence on centralized architectures and enable efficient firmware distribution even for devices with limited Internet connectivity.

2.LITERATURE SURVEY

Behnam Khayer et al. [7] Proposed blockchain-based solutions that provided robust authentication through mechanisms such as Physical Unclonable Functions (PUFs), enhanced transparency via smart contract-enabled reputation systems, and significantly mitigate vulnerabilities, including single points of failure and Sybil attacks. Smart contracts enabled secure interactions by automating resource allocation, access control, and verification. Cryptographic tools, including zero-knowledge proofs (ZKPs), proxy re-encryption, and Merkle trees, further improve data privacy and device integrity. Despite these advantages, challenges persist in areas such as scalability, regulatory and compliance issues, privacy and security concerns, resource constraints, and interoperability. Elizabeth Nathania Witanto et al. [8] proposed a blockchain-based OCF firmware update for IoT devices. Specifically, they introduced two types of firmware update protocol, direct and peer-to-peer updates, integrated into OCF firmware update specifications. In the direct scenario, the device, through the IoT gateway, can download the new firmware update from the manufacturer's server. Meanwhile, in the peer-to-peer scheme, the device can query the update from the nearby gateways.

Alexandru A. Maftei et al. [9] introduced efficient methods for managing, transmitting, and securing data packets within a blockchain-enabled IoT network. The proposed framework uses a gateway node to aggregate multiple data packets into single transactions, increasing throughput, optimizing network bandwidth, reducing latency, simplifying data retrieval, and improving scalability. Almarri, S. et al. [10] examined how blockchain's decentralized, immutable, and transparent features contribute to enhancing security and trust in IoT networks. Key findings indicate that blockchain integration can prevent data

manipulation, ensure robust identity management, and facilitate transparent, verifiable transactions, supporting both security and trust in IoT systems.

Andreas Polyvios Delladetsimas et al. [11] reviewed lightweight consensus mechanisms to reduce computational demands. They also utilized established platforms, such as Ethereum and Hyperledger, or custom blockchains designed to meet marine-specific requirements. Additional approaches incorporated technologies such as fog and edge layers, software-defined networking (SDN), the InterPlanetary File System (IPFS) for decentralized storage, and AI-enhanced security measures, all adapted to each application's needs. Renan Yamaguti et al. [12] proposed a approach that extended the Three-Phase Methodology (TpM) by introducing an innovative entity, the IoT Operator, which acted as a custody caretaker, contract enforcer, and mediator. By leveraging blockchain's secure and immutable ledger, the IoT Operator ensures the reliable monitoring and governance of IoT applications. Xuesong Xu et al. [13] proposed a resource constrained Layered Lightweight Blockchain Framework (LLBF) and implementation mechanism. The framework consists of a resource constrained layer (RCL) and a resource extended layer (REL) blockchain used in IIoT. They redesigned the block structure and size to suit to IIoT edge computing devices. A lightweight consensus algorithm and a dynamic trust right algorithm is developed to improve the throughput of blockchain and reduce the number of transactions validated in new blocks respectively.

Muath A. Obaidat et al. [14] highlighted the unique challenges and opportunities in IoT–blockchain integration, providing a foundation for advancing secure and scalable IoT applications. By exploring consensus mechanisms and resource-constrained deployments, provide a framework for developing secure and efficient IoT applications utilizing blockchain technology and providing a basis for future research and practical applications. Giuseppe D'Aniello et al. [15] assessed the practical implications of these solutions, discussing both their strengths and inherent limitations. Furthermore, they identified key open issues such as scalability, data protection, and interoperability across platforms, and they outlined potential research directions to support the development of more robust and adaptable trust frameworks for the evolving IoT landscape.

3. PROPOSED SYSTEM

The system presents a secure framework for IoT software update distribution by integrating encryption techniques, decentralized storage, and blockchain-based transaction management. The process begins with the manufacturer uploading firmware updates through a web-based application interface.

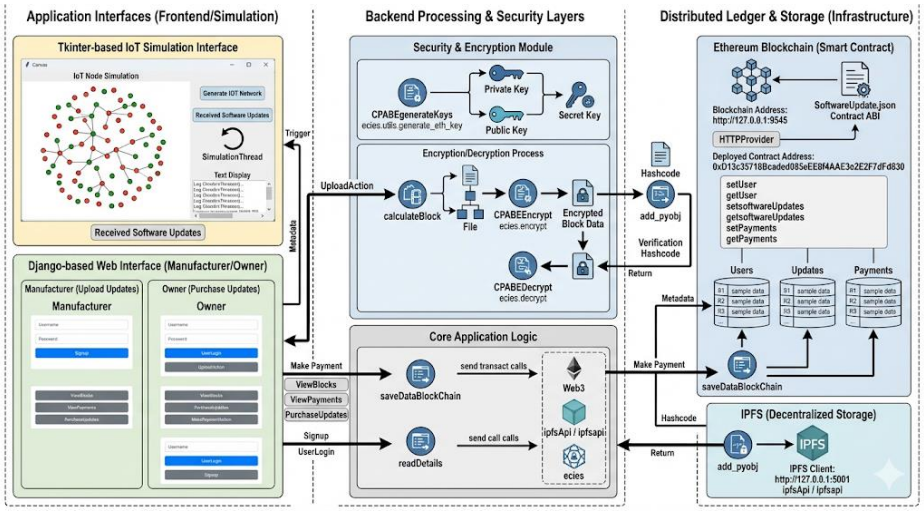


Figure 2: Proposed system architecture.

The uploaded firmware is segmented into multiple blocks and encrypted using ECIES and CP-ABE, ensuring data confidentiality and fine-grained access control. As shown as Figure 2 these encrypted blocks are stored in the Interplanetary File System (IPFS), where each block is associated with a unique Content Identifier (CID) for secure and tamper-evident storage. At the same time, essential metadata including user information, file name, block identifiers, and corresponding hash values is recorded on the Ethereum blockchain using smart contracts. The IoT owner interacts with the system to browse and purchase available updates, while payment transactions are securely stored on the blockchain. A dedicated key management module handles the generation and usage of public and private keys required for encryption and decryption operations. On the IoT side, the simulation module continuously monitors blockchain transactions to verify successful payments. Once validation is confirmed, the system retrieves the corresponding encrypted firmware blocks from IPFS using their CIDs.

Description of the Proposed Methodology

- The system addresses key challenges in IoT environments, including unauthorized access, data tampering, and inefficient update distribution, by utilizing blockchain technology with immutable records and smart contracts.
- A Django-based web application handles user authentication, registration for manufacturers and IoT owners, firmware uploads, and secure payment processing.
- Firmware files are divided into smaller blocks and encrypted using a hybrid approach combining ECIES and CP-ABE to ensure both confidentiality and controlled access.
- Encrypted blocks are stored in IPFS, while the blockchain maintains only hash references and transaction details (users, updates, and payments), ensuring transparency and auditability.
- A simulation module models IoT network nodes and demonstrates the update distribution process based on verified blockchain payment records.
- IoT nodes receive updates dynamically once payment confirmation is detected, with visual indicators representing the update status and progression.
- Smart contracts automate authentication, authorization, and payment verification processes, reducing manual intervention and improving security.
- Encryption ensures that only authorized devices can decrypt and reconstruct firmware updates, maintaining both data integrity and confidentiality.
- Multi-threading within the simulation enables real-time update processing while maintaining a responsive graphical interface.
- The architecture supports scalability and is applicable to domains such as smart homes, healthcare IoT, and industrial automation, providing a secure and decentralized update mechanism.

Benefits and Innovation

- Eliminates centralized points of failure commonly found in traditional IoT update systems.
- Enables secure and efficient distribution of software updates through decentralized storage and blockchain validation.
- Simplifies operational processes for manufacturers using automated blockchain-based workflows.

- Builds trust among manufacturers, IoT owners, and devices through transparent and verifiable transactions.

4. RESULTS ANALYSIS

The results demonstrate the effective implementation of a decentralized IoT software update management system integrating blockchain, IPFS, and hybrid encryption techniques. The system successfully enables secure user registration, encrypted software upload, and immutable recording of update and payment transactions on the blockchain. Manufacturers can upload and manage firmware updates, while IoT owners can securely purchase and access them through a transparent interface. The use of IPFS ensures distributed and tamper-resistant storage of update blocks, enhancing system reliability. Additionally, the Tkinter-based simulation visually represents real-time update distribution across IoT devices. The results validate improved security, transparency, and scalability compared to traditional centralized update systems.

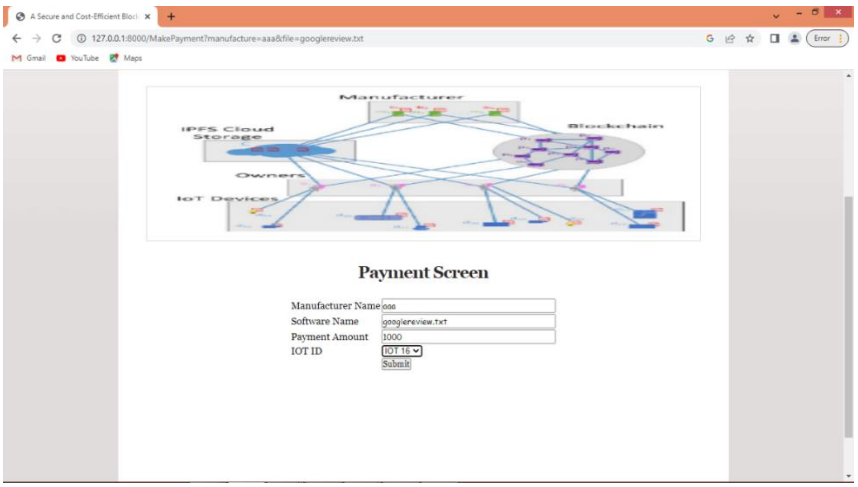


Figure 3 Payment screen

The illustrated Figure 3 depicts the payment screen used for completing software update transactions. It describes a form-based interface that collects payment-related details such as manufacturer name, software name, payment amount, and IoT device identification. A submission control is provided to confirm and process the payment. This screen ensures structured handling of transaction information. It plays a crucial role in completing the secure software purchase workflow.

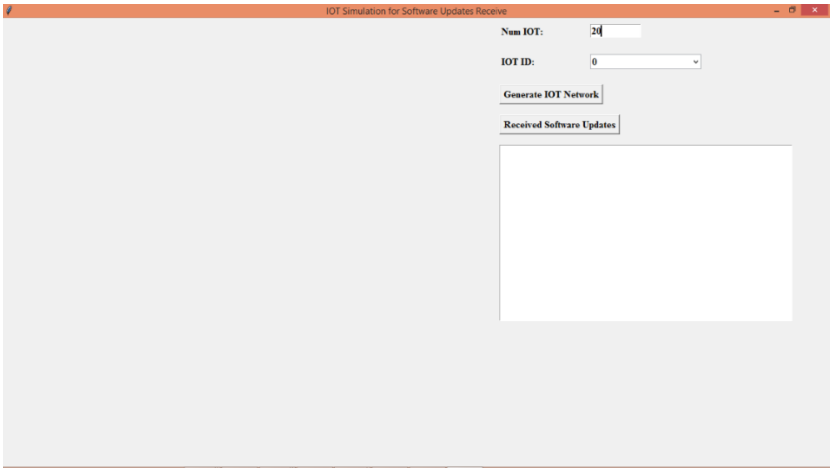


Figure 4: Generating Iot Network

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

The illustrated Figure 4 depicts the interface for generating an IoT network simulation. It describes a control panel where the user specifies the number of IoT devices and selects an IoT identifier. An action option is provided to generate the IoT network dynamically. The screen prepares the environment for simulating software update distribution. It enables visualization of multiple IoT nodes within the network. This interface initiates the update reception process.

The illustrated Figure 5 depicts the generated IoT network with software updates distribution capability. It shows multiple IoT nodes represented in a structured layout after network generation. Each node is labeled to uniquely identify individual IoT devices. The interface allows the system to simulate the readiness of devices to receive updates. A panel is provided to display received software update information. This screen demonstrates the operational IoT network environment.

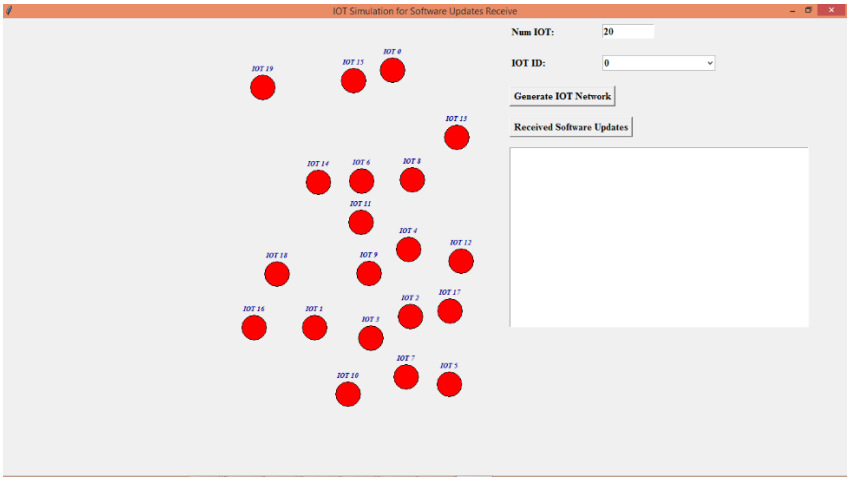


Figure 5: Generated Software updates for IOT

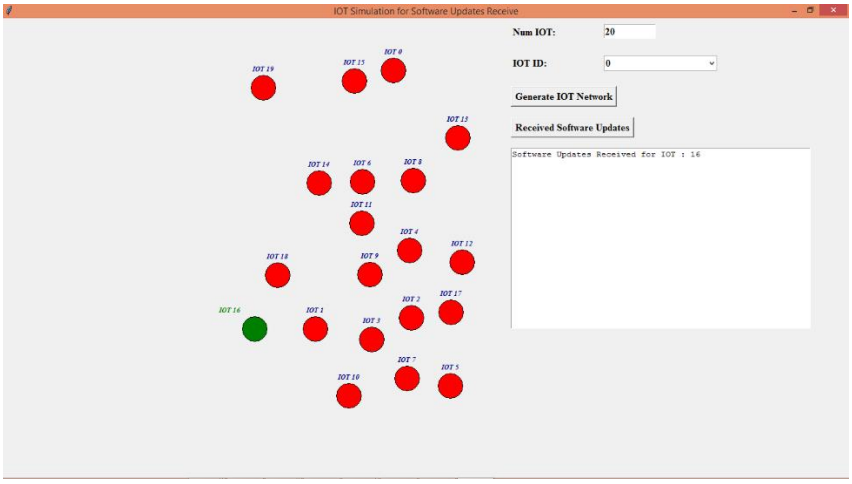


Figure 6: purchased Software Updates

The illustrated Figure 6 depicts the screen showing purchased software updates successfully delivered to an IoT device. It describes a network view where the selected IoT device is highlighted to indicate update reception. The received software update details are displayed in a dedicated section. This interface confirms successful delivery of purchased updates. It validates the end-to-end software update process. The screen represents the final stage of the update lifecycle.

5. CONCLUSION

This research successfully demonstrates a secure, decentralized, and scalable framework for IoT software updates using the synergy of blockchain, IPFS, and modern cryptographic techniques. By integrating Ethereum-based smart contracts via web3, the system achieves an immutable and transparent ledger to record users, updates, and payment transactions, significantly enhancing trust and auditability. The use of IPFS as decentralized storage ensures large software update files are handled efficiently and resiliently without overloading the blockchain, preserving decentralization benefits. The cryptographic layer, leveraging ECIES with CP-ABE encryption, secures update blocks with selective access control, safeguarding IoT devices against unauthorized or malicious software. The Django web application provides robust user registration, login, and interface for uploading updates and carrying out payments, while real-time Tkinter simulation visually demonstrates the update distribution process across an IoT network, reflecting blockchain-recorded transactions. Together, these components address traditional IoT update challenges such as centralization risks, lack of transparency, and weak security. Extensive testing in simulated environments shows the system's efficacy in rendering encrypted update delivery both secure and efficient, with encryption and blockchain interactions optimized for resource-constrained IoT contexts. Modular design and clear functional separation ease maintenance and pave the way for future extensibility. With this architecture, stakeholders gain confidence in update authenticity, payment integrity, and seamless delivery.

REFERENCES

[1] Khan MA, Salah K (2018) Iot security: Review, blockchain solutions, and open challenges. Future Gen Comput Syst 82:395–411. https://doi.org/10.1016/j.future.2017.11.022

[2] Miller C (2011) Battery firmware hacking: Inside the innards of a smart battery. Technical report, Accuvant Labs

[3] Zetter K How the NSA's Firmware Hacking Works and Why It's So Unsettling. https://www.wired.com/2015/02/nsa-firmware-hacking/

[4] Kolias C, Kambourakis G, Stavrou A, Voas J (2017) Ddos in the iot: Mirai and other botnets. Computer 50(7):80–84. https://doi.org/10.1109/MC.2017.201

[5] Vlajic N, Zhou D (2018) Iot as a land of opportunity for ddos hackers. Computer 51(7):26–34. https://doi.org/10.1109/MC.2018.3011046

[6] Kalae, U. K. (2020). Developing scalable Power BI dashboards for enhanced data analysis and strategic business decision-making. International Journal of Enhanced Research in Science, Technology & Engineering, 9(3), 8–15.

[7] Khayer, B.; Mirzaei, S.; Alavizadeh, H.; Salehi Shahraki, A. Blockchain for Secure IoT: A Review of Identity Management, Access Control, and Trust Mechanisms. IoT 2025, *6*, 65. https://doi.org/10.3390/iot6040065

[8] Saai Reddy Purmani, S. (2023). The Transformation of IT Leadership in Business Organizations: Shifting from Technical Supervision to Strategic Empowerment. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(5). https://doi.org/10.56975/jaafr.v1i5.503885

[9] Maftei, A.A.; Petrariu, A.I.; Popa, V.; Lavric, A. A Blockchain Framework for Scalable, High-Density IoT Networks of the Future. Sensors 2025, *25*, 2886. https://doi.org/10.3390/s25092886

[10] Almarri, S.; Aljughaiman, A. Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. Sustainability 2024, *16*, 10177. https://doi.org/10.3390/su162310177

[11] Delladetsimas, A.P.; Papangelou, S.; Iosif, E.; Giaglis, G. Integrating Blockchains with the IoT: A Review of Architectures and Marine Use Cases. Computers 2024, *13*, 329. https://doi.org/10.3390/computers13120329

[12] Yamaguti, R.; Ferreira, L.C.B.C.; Lui Motta, L.; Montali Assumpção, R.; Branquinho, O.C.; Iervolino, G.; Cardieri, P. IoT and Blockchain for Support for Smart Contracts Through TpM. Sensors 2025, *25*, 5001. https://doi.org/10.3390/s25165001

[13] Xu, X.; Zeng, Z.; Yang, S.; Shao, H. A Novel Blockchain Framework for Industrial IoT Edge Computing. Sensors 2020, *20*, 2061. https://doi.org/10.3390/s20072061

[14] Obaidat, M.A.; Rawashdeh, M.; Alja'afreh, M.; Abouali, M.; Thakur, K.; Karime, A. Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. Big Data Cogn. Comput. 2024, *8*, 174. https://doi.org/10.3390/bdcc8120174

[15] Giuseppe D'Aniello, Lidia Fotia, Blockchain and AI-based methods for trust management in IoT: A comprehensive survey, Internet of Things, Volume 34,2025,101755, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2025.101755.