Advanced Industrial SCIence
Vol. 4, No. 1, pp. 34-40, 2025
ISSN 2951-2476
https://doi.org/10.23153/AI-Science.2025.4.1.034

A Research on building a Smart City Model based on DID(Decentralized-Identity) using Digital Twin

Sunghyuck Hong
Professor, Division of Advanced IT, IoT major, Baekseok University

디지털 트윈을 활용한 DID 기반 스마트시티 모델 구축 연구

홍성혁
백석대학교 첨단IT학부, IoT 전공 교수

Abstract Urbanization exacerbates challenges in housing, transportation, energy, environment, welfare, and safety. This study proposes a "DID-based safe smart city model using digital twin" to enhance citizens' quality of life and advance societal development. We develop a standardized layer model for the Cognitive Internet of Things (CIoT) environment, utilizing blockchain's distributed ledger technology and Decentralized-Identity (DID) for secure device communication. Emphasizing explainable AI (eXplainable Artificial Intelligence), the model ensures transparency in processing IoT-collected big data. By integrating autonomous decision-making algorithms and real-time 3D data visualization through digital twins, the model enhances problem-solving and preventive capabilities. This research distinguishes itself by combining CIoT, blockchain (DID), and digital twin technologies to create a comprehensive smart city standard model addressing content integration and scalability.

Key Words : Smart City, Digital Twin, Decentralized-Identity (DID), Cognitive Internet of Things (CIoT), Explainable Artificial Intelligence (XAI)

요 약 도시화는 주거, 교통, 에너지, 환경, 복지, 안전 등의 분야에서 환경을 파괴하고 있다. 이 연구는 시민의 삶의 질을 향상시키고 사회 발전을 촉진하기 위해 "디지털 트윈을 활용한 DID 기반 안전 스마트 시티 모델"을 제안한다. 본 연구에서는 사물 인터넷(IoT) 환경을 위한 표준화된 계층 모델을 개발하고, 블록체인의 분산 장부 기술과 DID(Decentralized Identity)를 활용하여 안전한 장치 통신을 보장함. 또한, 설명 가능한 인공지능(eXplainable Artificial Intelligence)을 이용하여 IoT로 수집된 빅데이터 처리의 투명성을 보장하고, 자율적인 의사 결정 알고리즘과 디지털 트윈을 통한 실시간 3D 데이터 시각화를 통합하여 이 모델은 문제 해결 및 예방 기능을 향상시킨다. 따라서 이 연구는 CIoT, 블록체인(DID) 및 디지털 트윈 기술을 결합하여 콘텐츠 통합 및 확장성 문제를 해결하는 종합적인 스마트 시티 표준 모델을 만드는 데 필요한 구성요소를 제공하여 향후 스마트 시티 구축에 기여하는 연구이다.

주제어 : 스마트 시티, 디지털 트윈, 분산 ID(DID), 인지 사물 인터넷(CIoT), 설명 가능한 인공지능(XAI)

*This research was supported by 2024 Baekseok University research fund.
*Corresponding Author : Sunghyuck Hong(shong@bu.ac.kr)
Received August 11, 2024
Revised September 20, 2024
Accepted January 20, 2025
Published Januaryr 30, 2025

1. Introduction

This study aims to take the concept of smart city one step further and propose a safe and smart city model. In particular, this study proposes a safe smart city model based on Decentralized Identity (DID) using Digital Twin. Digital twins create digital replicas of physical objects, enabling simulations and predictions based on real-time data. This will improve our ability to detect and respond to urban problems in real time.

This study develops a standardized layer model for the Cognitive Internet of Things (CIoT) environment. To achieve this, we utilize blockchain's distributed ledger technology and DID to implement secure communication between devices. In addition, we emphasize explainable artificial intelligence (XAI) to ensure transparency in the processing of big data collected through IoT. Improve problem solving and prevention capabilities by integrating autonomous decision-making algorithms and real-time 3D data visualization through digital twins.

This study differentiates itself from existing research by combining CIoT, blockchain (DID), and digital twin technologies to present a comprehensive smart city standard model with content integration and scalability. In particular, this study makes the following key contributions:

- Implementation of secure device-to-device communication: Utilizes blockchain distributed ledger technology and DID to solve security issues in the CIoT environment.
- Guaranteed transparency: By introducing explainable artificial intelligence (XAI), we increase the transparency of the big data processing process collected through IoT.
- Real-time problem solving and prevention: Integrates real-time data visualization through digital twins and autonomous decision-making algorithms, enabling rapid response and prevention of urban problems.

The development of smart cities is essential to solve various problems caused by urbanization. The DID-based safe smart city model proposed in this study combines CIoT, blockchain, and digital twin technologies to provide an innovative approach to improve the quality of life of citizens and promote social development. Through this, we will contribute to effectively managing complex urban problems and building a sustainable urban environment[1-7].

2. Cognitive Internet of Things (CIoT) and Smart Cities

2.1 Cognitive Internet of Things (CIoT)

The concept of smart cities has gained significant traction as urban areas continue to expand rapidly, bringing with them a host of challenges including traffic congestion, pollution, resource management, and public safety. The Cognitive Internet of Things (CIoT) emerges as a pivotal technology in addressing these urban challenges by integrating advanced cognitive computing and IoT capabilities to create more intelligent and responsive urban environments.

CIoT extends the traditional Internet of Things (IoT) by incorporating cognitive computing technologies such as machine learning, artificial intelligence (AI), and advanced data analytics. This combination allows CIoT systems to not only collect and transmit data but also to analyze and interpret it, leading to more autonomous and intelligent decision-making processes.

Key features of CIoT include:

- Context Awareness: Ability to understand the

environment and context in which IoT devices operate.

- Autonomous Learning: Continuous improvement of system performance through machine learning algorithms.
- Enhanced Interoperability: Seamless commu nication and operation across various devices and platforms.
- Scalability: Capability to handle large-scale deployments typical of urban environments.

2.2 Role of CIoT in Smart Cities

In smart cities, CIoT technologies are leveraged to enhance various urban systems, including transportation, energy management, environmental monitoring, and public safety. The following sections detail how CIoT contributes to each of these areas:

2.2.1 Transportation

CIoT systems can optimize traffic flow, reduce congestion, and enhance public transportation services. For instance, real-time data from connected vehicles and traffic sensors can be analyzed to provide dynamic traffic management solutions, route optimization for public transport, and predictive maintenance for infrastructure.

2.2.2 Energy Management

CIoT enables smart grids that efficiently balance supply and demand, integrate renewable energy sources, and reduce energy wastage. Smart meters and connected home devices provide data that helps in optimizing energy consumption patterns and identifying areas for improvement.

2.2.3 Environmental Monitoring

CIoT facilitates real-time monitoring of environmental parameters such as air quality, noise levels, and water quality. This data helps in early detection of pollution sources, compliance with environmental regulations, and informed urban planning decisions.

2.2.4 Public Safety

CIoT enhances public safety through intelligent surveillance systems, emergency response coordination, and predictive analytics for crime prevention. Connected devices such as smart streetlights and surveillance cameras provide data that can be analyzed to improve situational awareness and response times.

The Cognitive Internet of Things represents a transformative approach to managing and enhancing urban environments. By leveraging advanced cognitive computing and IoT technologies, CIoT enables smarter, more responsive, and sustainable cities. Integrating blockchain and digital twin technologies further enhances the security, transparency, and effectiveness of smart city initiatives. As research and development in CIoT continue to advance, the vision of truly intelligent and efficient urban ecosystems becomes increasingly attainable.

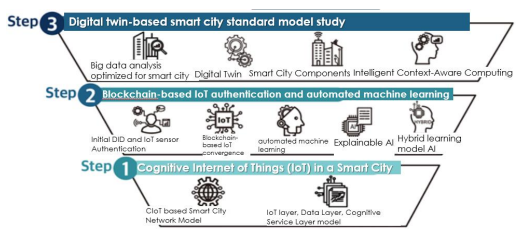

Fig. 1. Three Steps for Developing Smart City

There are three steps to developing my research in Fig. 1. The first step is Cognitive IoT in a Smart City. Decentralized Identity and Explainable AI are the second steps. The last step is the digital twin, which simulates based on collected data from IoT and gives us results

to make a decision[8-10].

3. Blockchain-based IoT Authentication and Automated Machine Learning

The rapid proliferation of Internet of Things (IoT) devices across various domains, including smart cities, healthcare, and industrial automation, necessitates robust security mechanisms and intelligent data processing capabilities. Blockchain technology, with its decentralized and immutable ledger, offers promising solutions for IoT authentication, while automated machine learning (AutoML) enhances the ability to analyze and utilize the vast amounts of data generated by IoT devices. This paper explores the integration of blockchain-based IoT authentication and AutoML to create secure and intelligent IoT ecosystems.

4. Blockchain-based IoT Authentication

4.1 Need for Secure IoT Authentication

As the number of IoT devices increases, so does the risk of cyber-attacks. IoT devices often lack strong security measures, making them vulnerable to unauthorized access and data breaches. Secure authentication mechanisms are essential to protect the integrity and confidentiality of IoT networks.

4.2 Blockchain Technology for Authentication

Blockchain technology provides a decentralized and tamper-proof method for IoT authentication. Key features include:

Decentralization: Eliminates the need for a central authority, reducing single points of failure.

Immutability: Ensures that once data is recorded on the blockchain, it cannot be altered or deleted, providing a secure audit trail.

Transparency: Allows all participants in the network to verify the authenticity of transactions.

4.3 Decentralized Identity (DID) Systems

Decentralized Identity (DID) systems leverage blockchain technology to manage digital identities. In a DID system, each IoT device is assigned a unique identifier recorded on the blockchain. This ensures secure authentication and authorization processes, as the identity of each device can be verified without relying on a central authority.

4.4 Implementation of Blockchain-based IoT Authentication

Implementing blockchain-based IoT authentication involves several steps:

Device Registration: Each IoT device is registered on the blockchain, receiving a unique DID.

Authentication Process: When a device attempts to connect to the network, its DID is verified against the blockchain ledger.

Smart Contracts: Smart contracts on the blockchain automate the authentication process, ensuring secure and efficient verification.

5. Automated Machine Learning (AutoML)

5.1 Importance of Machine Learning in IoT

IoT devices generate vast amounts of data that need to be processed and analyzed to extract valuable insights. Machine learning algorithms are essential for analyzing this data, enabling predictive maintenance, anomaly detection, and optimization of IoT systems.

5.2 Challenges in Traditional Machine Learning

Traditional machine learning approaches require significant human expertise and time to develop and fine-tune models. This can be a

bottleneck in rapidly evolving IoT environments where quick and accurate analysis is crucial.

5.3 Advantages of AutoML

Automated Machine Learning (AutoML) addresses the challenges of traditional machine learning by automating the end-to-end process of model development. Key advantages include:

- Efficiency: Reduces the time and effort required to develop machine learning models.
- Accessibility: Enables non-experts to leverage advanced machine learning techniques.
- Scalability: Facilitates the rapid deployment of models across large IoT networks.

5.4 AutoML in IoT Applications

AutoML can be applied to various IoT use cases, including:

- Predictive Maintenance: Automatically developing models to predict equipment failures based on sensor data.
- Anomaly Detection: Identifying unusual patterns in IoT data that may indicate security breaches or system malfunctions.
- Optimization: Enhancing the performance and efficiency of IoT systems through automated model tuning.

5.5 Integration of Blockchain and AutoML in IoT

5.5.1 Secure and Intelligent IoT Ecosystems

The integration of blockchain-based IoT authentication and AutoML creates secure and intelligent IoT ecosystems. Blockchain ensures that only authenticated devices can access the network, while AutoML enables the continuous analysis and optimization of IoT data.

5.5.2 Use Case: Smart Cities

In smart cities, blockchain-based IoT authentication ensures the security of connected devices, such as smart meters, traffic sensors, and surveillance cameras. AutoML analyzes the data from these devices to optimize traffic flow, reduce energy consumption, and enhance public safety.

5.5.3 Implementation Strategy

Blockchain Infrastructure: Deploy a blockchain network to manage the identities and authentication of IoT devices.

AutoML Framework: Implement an AutoML framework to develop and deploy machine learning models for various IoT applications.

Integration Layer: Create an integration layer that allows the seamless interaction between the blockchain infrastructure and the AutoML framework.

5.5.4 Challenges and Future Directions

Both blockchain and AutoML face scalability challenges. Blockchain networks must handle a large number of transactions efficiently, while AutoML systems need to process and analyze massive datasets.

5.5.5 Interoperability

Ensuring interoperability between different IoT devices, blockchain platforms, and AutoML frameworks is crucial for the seamless functioning of the integrated system.

While blockchain enhances security, it also raises privacy concerns, as the immutable nature of blockchain records can conflict with data privacy regulations. Ensuring compliance with privacy laws is essential.

Future research should focus on developing scalable blockchain solutions, enhancing the interoperability of IoT ecosystems, and addressing privacy concerns. Additionally, advancements in AutoML techniques will further improve the efficiency and effectiveness of IoT data analysis.

The integration of blockchain-based IoT authentication and automated machine learning represents a significant advancement in the development of secure and intelligent IoT ecosystems. By leveraging the strengths of both technologies, it is possible to create robust systems that not only protect IoT networks from unauthorized access but also harness the power of machine learning to optimize and enhance the performance of IoT applications. As research and development continue, these integrated solutions will play a crucial role in the evolution of smart cities and other IoT-enabled environments[10-13].

6. Conclusion

The integration of blockchain-based IoT authentication and automated machine learning represents an important step forward in developing a secure and intelligent IoT ecosystem. By leveraging the strengths of these two technologies, you can build a powerful system that prevents unauthorized access to your IoT network and leverages the power of machine learning to optimize and improve the performance of IoT applications. As research and development continues, these integrated solutions will play a critical role in the evolution of smart cities and other IoT-based environments.

REFERENCES

[1] Dorri, A., Moustafa, N., Bahri, Z., & Ghaleb, A. (2020). Blockchain for IoT security and privacy: A systematic survey. *IEEE Communications Surveys & Tutorials, 22(2),* 1100-1138. https://ieeexplore.ieee.org/document/8215429

[2] Guo, Z., Zhang, C., Sun, L., & Liu, X. (2019). Explainable artificial intelligence for decision-making in smart cities. *Artificial Intelligence, 272,* 804-819. DOI : 10.1016/j.artint.2018.12.001

[3] Jang, W., Lee, M., & Lim, J. H. (2018). Digital twins for smart cities. *Sustainability, 10(1),* 153. DOI : 10.3390/su10010153

[4] Lin, J., Yu, W., Zhang, N., Wee, X., & Zhu, L. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4(5),* 1278-1295. https://ieeexplore.ieee.org/document/7995200

[5] Qi, Q., Dou, Q., Li, Y., Zhao, T., & Guo, X. (2022). A comprehensive survey of explainable artificial intelligence (XAI) for network traffic analysis. *IEEE Communications Surveys & Tutorials, 24(2),* 1150-1173. https://ieeexplore.ieee.org/document/9626293

[6] Razo-Zapata, I., Contreras-Castillo, J. A., & Teran-Quintero, J. M. (2020). The role of artificial intelligence in smart cities: Survey and future perspectives. *Sustainable Cities and Societies, 58,* 102229. DOI : 10.1016/j.scs.2020.102229

[7] Salehi, H., Ghalehbandi, S., Guo, H., & Zhao, J. (2021). Internet of things (IoT) in smart water grids: Review of the applications and challenges. *Journal of Network and Computer Applications, 193,* 103220.

[8] Sun, Y., Zhuang, Z., Xu, J., Lu, C., Li, X., & Guo, S. (2020). Security and privacy issues in blockchain-based internet-of-things systems: A survey. *IEEE Access, 8,* 167910-167934.

[9] Zou, Y., Shen, J., & Zhou, K. (2022). Artificial intelligence for smart cities: A survey. *ACM Computing Surveys, 55(3),* 1-43. https://dl.acm.org/doi/fullHtml/10.1145/2858789

[10] Yildiz, H. U., Alper, O. F., & Amza, C. P. (2022). Blockchain-based smart cities: Survey, challenges, and future directions. *IEEE Access, 10,* 10272-10289. http://ieeexplore.ieee.org/document/8642861/

[11] Li, X., Ali, M. A., Zuo, M., Sun, Y., & Liu, Y. (2022). A survey on explainable artificial intelligence for smart cities. *ACM Computing Surveys, 55(3),* 1-41. https://www.mdpi.com/2079-9292/12/4/1020

[12] Ding, Y., Li, K., & Han, Y. (2022). Digital twin for smart cities: A survey of technologies, applications, and challenges. *IEEE Access, 10,* 10259-10271. https://ieeexplore.ieee.org/document/9576739

[13] Yu, W., Liang, F., & He, X. (2022). Blockchain-based

secure data sharing for smart cities. *IEEE Transactions on Emerging Topics in Computing, 10(1),* 1-14.
https://ieeexplore.ieee.org/document/7828539

홍 성 혁 (Sunghyuck Hong) **[종신회원]**

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 첨단IT학부, IoT 전공 주임 교수

- 관심분야 : 핀테크, 딥러닝, 블록체인, 사물인터넷 보안
- E-Mail : shong@bu.ac.kr