International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

BLOCKCHAIN-BASED ARCHITECTURE AND FRAMEWORK FOR CYBERSECURE SMART CITIES

CH. SHYAMALA RANI[1], rani.shyamala@gmail.com
SITA SOWJANYA PRAKHYA[2], sowjipavan14@gmail.com
Assistant Professor[1&2], Department Of It, Mvsr Engineering College

ABSTRACT

A smart city is one that uses digital technologies and other means to improve the quality of life of its citizens and reduce the cost of municipal services. Smart cities primarily use IoT to collect and analyze data to interact directly with the city's infrastructure and monitor city assets and community developments in real time to improve operational efficiency and proactively respond to potential problems and challenges. Today, cybersecurity is considered one of the main challenges facing smart cities. Over the past few years, the cybersecurity research community has devoted a great deal of attention to this challenge. Among the various technologies being considered to meet this challenge, Blockchain is emerging as a solution offering the data security and confidentiality essential for strengthening the security of smart cities. In this paper, we propose a comprehensive framework and architecture based on Blockchain, big data and artificial intelligence to improve smart cities cybersecurity. To illustrate the proposed framework in detail, we present simulation results accompanied by analyses and tests. These simulations were carried out on a smart grid dataset from the UCI Machine Learning Repository. The results convincingly demonstrate the potential and effectiveness of the proposed framework for addressing cybersecurity challenges in smart cities. These results reinforce the relevance and applicability of the framework in a real-world context.

Received: 18-11-2025 Accepted: 30-12-2025 Published: 10-01-2026

INTRODUCTION

In the digital age, everything is connected as part of the growing and accelerating digital transformation of modern societies, which involves all kinds of sectors and human activities such as education, healthcare, economy, energy, etc. Urban communities, and even some villages, are benefiting from the technologies and solutions available through digital transformation to engage in all kinds of smart city initiatives to put them at the service of sustainable, resilient and inclusive socio-economic development. The smart city achieves efficiencies, promotes sustainability, and improves the quality of life for its residents through the integration of technology. Planning for a smart city is essentially about bringing the Internet of Things (IoT) to scale. The Internet of Things (IOT) is the network of physical terminals, objects, incorporating software, connectivity, sensors, etc., to connect to other systems on the internet and exchange data to provide proper management and monitoring of city infrastructure and operations. Driven by the growing urban population, IOT and ICT are the main pillars of smart cities to improve their efficiency as well as the lives of their citizens [1], [2]. A smart city needs technological efficiency in areas as diverse as transportation and mobility, services, communication, security, citizen relations, etc. The implementation of IOT-based applications within cities allows for the optimization of: energy control, building performance, street furniture management, waste disposal, mobility, etc. The beneficiaries are citizens, consumers, private companies and local authorities [3]. By offering increasingly digitized services, smart cities are becoming ever more connected but also more exposed to cyber risks and cyber-attacks. Data collection is essential in IOT-based applications and services that are considered key assets for monitoring and operating smart cities. Therefore, managing data across the smart city

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

infrastructure is a big challenge given all the connected devices involved and their different architectures and urban data must be protected throughout its lifecycle. However, the main challenge is to protect IoT infrastructures throughout their deployment.

LITERATURE REVIEW

A Vademecum on Blockchain Technologies: When, Which, and How

- M. Belotti, Nikola Bozic, +1 author Stefano Secci
- Published in IEEE Communications Surveys… 12 July 2019

Blockchain is a technology making the shared registry concept from distributed systems a reality for a number of application domains, from the cryptocurrency one to potentially any industrial system requiring decentralized, robust, trusted, and automated decision making in a multi-stakeholder situation. Nevertheless, the actual advantages in using blockchain instead of any other traditional solution (such as centralized databases) are not completely understood to date, or at least there is a strong need for a vademecum guiding designers toward the right decision about when to adopt blockchain or not, which kind of blockchain better meets use-case requirements, and how to use it. In this paper, we aim at providing the community with such a vademecum, while giving a general presentation of blockchain that goes beyond its usage in Bitcoin and surveying a selection of the vast literature that emerged in the last few years. We draw the key requirements and their evolution when passing from permissionless to permissioned blockchains, presenting the differences between proposed and experimented consensus mechanisms, and describing existing blockchain platforms.

Role of IoT-Cloud Ecosystem in Smart Cities : Review and Challenges

- Ridhima Rani, Vijaita Kashyap, Meenu Khurana
- Published 9 November 2020

Smart Cities is one of the most important Internet of Things (IoT) applications. Billions of smart devices on IoT produce volumes of data directed to cloud for storage and processing. Sending complete data to cloud is least preferred from resource utilization perspective comprising of bandwidth and storage. Therefore, cloud computing paradigm limitations conquered by fog computing, acting as a bridge between IoT and cloud. Further, the limited computational capacity of end-devices in IoT infrastructure and inherited pros and cons of cloud and fog computing necessitates for all three paradigms to work together to full fill the needs of sustainable infrastructure for smart city. Keeping in view the need of integrating fog computing paradigm (due to its limited storage and computational capabilities), with IoT and cloud infrastructure, this article reviews the literature on role of IoT & cloud ecosystem in smart cities along with parameters of evaluation and future research directions in smart cities..

Smart Cities, Playable Cities, and Cybersecurity: A Systematic Review

- Gustav Verhulsdonck, Jennifer L. Weible, +1 author N. Hajduk
- Published in International journal of… 27 December 2021.

Smart cities connect humans to networks of information to create urban operating systems that optimize traffic management, sustainable energy use, and enact smart governance. The concept of playable cities has been advanced to create smart cities that are more human-centered. As smart cities are socio-technical structures involving technologies, people, and policies that each impact privacy and security, such an approach also has potential to develop stronger cybersecurity protocols for smart cities going beyond technological approaches. In this article, we conduct a systematic literature review of articles from 2015 to 2020 that discuss smart/playable cities and data gathering in relation to privacy and security.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Based on this systematic review, we found a disconnect exists between smart and playable cities literature in terms of exclusive focus on technological solutions for security and little focus on people and policies as part of cybersecurity in the literature analyzed. Seeing as playable cities embrace user-generated co-creation, we argue that this personal side is important to get people to participate meaningfully in smart cities that lets them embrace cybersecurity policies as part of personal behavior. For this purpose, we propose utilizing a cybersecurity lens (e.g., McCumber cube model) so that smart city designers can more fully develop and consider cybersecurity that includes both personal privacy and playable approaches.

EXISTING SYSTEM

Current systems for smart city operations often rely on centralized architectures to manage and process data from various domains, such as transportation, healthcare, and public utilities. These systems typically utilize traditional virtualization techniques, such as virtual machines, and lack integrated solutions for handling security and scalability. While centralized systems can manage large volumes of data, they are highly vulnerable to single points of failure, cyberattacks, and data breaches. Additionally, the lack of real-time interoperability between different smart city domains and inefficient data processing frameworks result in delays, higher costs, and security risks. These systems do not inherently ensure data integrity, transparency, or traceability, making them less suitable for the growing needs of cyber-secure smart cities.

Disadvantages:

1. **Vulnerability to Cyberattacks** Centralized architectures present a single point of failure, making them susceptible to hacking, ransomware, and other cyber threats, which can compromise the entire system.
2. **Inefficient Data Handling** Traditional virtualization methods and non-optimized data processing frameworks struggle to efficiently handle the massive datasets generated in smart cities, leading to delays and increased computational overhead.
3. **Limited Scalability** The existing systems lack the flexibility to scale efficiently as the size of the smart city grows, resulting in bottlenecks and degraded performance in larger deployments.
4. **Lack of Transparency and Traceability** Without blockchain integration, data in these systems lacks traceability and immutability, reducing trust in the system and making it challenging to verify data integrity.
5. **High Costs and Resource Utilization** Traditional virtualization methods, such as virtual machines, consume significant computational and storage resources, leading to higher operational costs compared to modern containerization techniques like Docker.

PROPOSED SYSTEM

In this section, we present the architecture of our solution that focuses mainly on security in smart cities using blockchain. For the deployment of our solution, we use Docker which is an open-source and secure containerization software platform designed for the creation, deployment, and management of virtualized applications. Knowing that traditional virtualization methods based on virtual machines have certain limitations,the containerisabetter alternativethatguarantees a lightweight and simpler execution environment. The architecture we propose is based on three layers: the perception layer, the data processing layer and the blockchain layer (Figure 1). Perception layer: In the perception layer, the objective is to collect, process and send data to the next layer. This layer includes various applications and domains of smart

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

cities such as (environment, mobility, government, economy, people, life). This layer consists of sensors and IoT devices to collect data, as well as Big Data real-time query components to ingest this data, API connectors and REST APIs that will enable web requests. In this layer, IoT data is sent to a data cube, then this data is aggregated to calculate key performance indicators and then it will be sent to the next layer.

Data processing layer: In this layer, we integrate machine learning. Preprocessing of data using machine learning is done because the collected data is in a raw format and it is not always possible to train/test the model using it. It is important to process this raw data in order to interpret it correctly and avoid any negative results in the prediction. In our case, we are dealing with too massive databases, which makes the computations too slow. We then decided to use PySpark DataFrame [10] which is one of the most optimized Machine Learning platforms for dealing with massive databases using distributed programming, and which consists of using multiple distributed computing units on multiple nodes to reduce the execution time of a query. Our algorithm uses the historical data of the Blockchain to build the model (training and testing), thus, after the end of the preprocessing and through PySpark the historical data of the Blockchain will be read in order to train/test the model, then, we use the linear regression model to predict the new records of the variable ‘‘stab’’, this prediction tool solves the binary classification problem (i.e., stable or unstable). We point out that the result of the linear regression model gave a high accuracy with an Rsquared of 0.9999998832117597. This data will be sent to the next blockchain layer.

Advantages :

1. Enhanced Security and Data Integrity
   - The integration of blockchain ensures that all data and predictions are stored securely and immutably, reducing the risk of tampering or unauthorized access. This is critical for maintaining trust and transparency in smart city operations.

2. Efficient and Scalable Data Processing
   - By using PySpark DataFrame for distributed computing, the architecture can efficiently handle massive datasets. This reduces execution times and makes the system scalable for large-scale smart city applications.

3. Improved Prediction Accuracy
   - The machine learning component, particularly the linear regression model, achieves exceptionally high accuracy (R-squared: 0.9999998832117597), ensuring reliable predictions for critical variables like "stab" (stability).

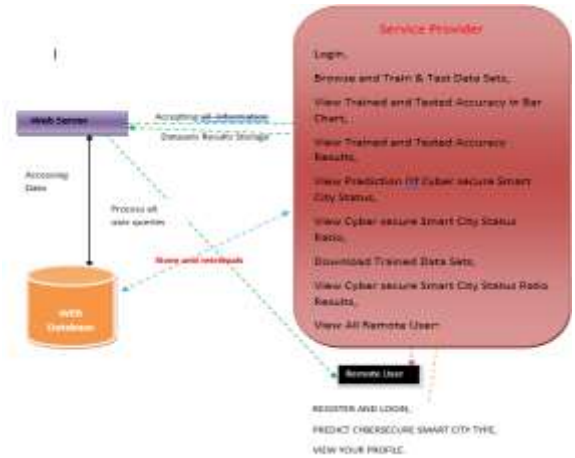
4. Lightweight and Portable Deployment
   - The use of Docker provides a lightweight, portable, and secure containerization solution. This simplifies deployment and ensures consistent performance across different environments without the overhead of traditional virtual machines.

5. Comprehensive Smart City Coverage
   - The architecture spans multiple domains of smart cities (e.g., environment, mobility, economy, government, people, and life) and includes a robust perception layer. This holistic approach ensures comprehensive data collection and processing tailored to diverse smart city needs.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

IMPLEMENTATION

SYSTEM ARCHITECTURE



MODULES

SERVICE PROVIDER

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Cyber secure Smart City Status, View Cyber secure Smart City Status Ratio, Download Trained Data Sets, View Cyber secure Smart City Status Ratio Results, View All Remote Users.

VIEW AND AUTHORIZE USERS

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

REMOTE USER

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBERSECURE SMART CITY TYPE, VIEW YOUR PROFILE.

RESULT

CONCLUSION

In this paper, we present a comprehensive and efficient approach for strengthening smart cities cyber security. Using block chain, big data and artificial intelligence algorithms, this approach offers a robust and a reliable framework for smart cities data security and privacy. This framework was illustrated using a real dataset on smart grid, demonstrating its efficiency and reliability. By focusing on data confidentiality, integrity and availability, our approach allows to guarantee a secure environment for smart cities, their infrastructures and services while improving

their resilience to cyber-attacks. In addition, this approach fosters mutual trust among the smart cities stakeholders and strengthens citizens confidence and engagement in smart cities applications and services.

REFERENCES

[1] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, ‘‘Sustainable smart cities: Convergence of artificial intelligence and blockchain,’’ *Sustainability*, vol. 13, no. 23, p. 13076, Nov. 2021, doi: 10.3390/su132313076.

[2] O. S. Neffati, S. Sengan, K. D. Thangavelu, S. D. Kumar, R. Setiawan, M. Elangovan, D. Mani, and P. Velayutham, ‘‘Migrating from traditional grid to smart grid in smart cities promoted in developing country,’’ *Sustain. Energy Technol. Assessments*, vol. 45, Jun. 2021, Art. no. 101125, doi: 10.1016/j.seta.2021.101125.

[3] F. Cui, ‘‘Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment,’’ *Comput. Commun.*, vol. 150, pp. 818–827, Jan. 2020.

[4] T. Alam, ‘‘Blockchain-based big data analytics approach for smart cities,’’ Tech. Rep., Nov. 2020, doi: 10.36227/techrxiv.13054244.v2.

[5] T. Alam, ‘‘IoT-fog: A communication framework using blockchain in the Internet of Things,’’ *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 1–10, 2019.

[6] Nandigama, N. C. (2025). Enterprise-Grade Aml Threat Detection Using Time Frequency Signals And Spring Boot Microservices. Journal of Computational Analysis and Applications, 26(02). https://doi.org/10.48047/jocaaa.2019.26.02.01.

[7] D. Minoli and B. Occhiogrosso, ‘‘Blockchain mechanisms for IoT security,’’ *Internet Things*, vol. 1, pp. 1–13, Sep. 2018.

[8] K. Christidis and M. Devetsikiotis, ‘‘Blockchains and smart contracts for the Internet of Things,’’ *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] T. Alam, ‘‘Blockchain and its role in the Internet of Things (IoT),’’ *Int. J. Sci. Res. Comput. Sci., Eng. Inf. Technol.*, vol. 5, no. 1, pp. 151–157, Jan. 2019, doi: 10.32628/CSEIT195137.

[10] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. Abd El-Latif, ‘‘Convergence of blockchain and IoT for secure transportation systems in smart cities,’’ *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Apr. 2021.

[11] Nandigama, N. C. (2016). Teradata-Driven Big Data Analytics For Suspicious Activity Detection With Real-Time Tableau Dashboards. International Journal For Innovative Engineering and Management Research, 5(1), 73–78.

[12] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker,
M. Hammoudeh, and I. Ghafir, ‘‘The security of big data in fog-enabled IoT applications including blockchain: A survey,’’ *Sensors*, vol. 19, no. 8, p. 1788, Apr. 2019.

[13] D. Bruneo, S. Distefano, F. Longo, G. Merlino, A. Puliafito, V. D’Amico, M. Sapienza, and G. Torrisi, ‘‘Stack4Things as a fog computing platform for smart city applications,’’ in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, San Francisco, CA, USA, Apr. 2016, pp. 848–853, doi: 10.1109/INFCOMW.2016.7562195.

[14] Nandigama, N. C. (2023). Data-Warehouse-Enhanced Machine Learning Framework for Multi-Perspective Fraud Detection in Multi-Stakeholder E-Commerce Transactions. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5), 592–600. https://doi.org/10.17762/ijritcc.v11i5.11808.

[15] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, ‘‘Blockchain technology: A survey on applications and security privacy challenges,’’ *Internet Things*, vol. 8, Dec. 2019, Art. no. 100107, doi: 10.1016/j.iot.2019.100107.