



ASIAN BULLETIN OF BIG DATA MANAGEMENT

<http://abbdm.com/>

ISSN (Print): 2959-0795

ISSN (online): 2959-0809

Blockchain-Driven Cybersecurity Framework for Smart Homes: Integrating IoT and Machine Learning for Secure Automation

Usman Imtiaz, Shanza Malik, Ajab Khan*

Chronicle

Article history

Received: Sept 16, 2024

Received in the revised format: Oct 22, 2024

Accepted: Nov 28, 2024

Available online: 27 December, 2024

Usman Imtiaz is currently affiliated with the Faculty of Engineering, National University of Technology, Islamabad, Pakistan.

Email: usmanimtiaz1000@gmail.com

Shanza Malik is currently affiliated with the Department of Information Technology, Abbottabad University of Science and Technology, Abbottabad, Pakistan.

Email: Shanzamalik360@gmail.com

Ajab Khan is currently working at ORIC, Abbottabad University of Science and Technology, Abbottabad, Pakistan.

Email: ajabk66@yahoo.com

Corresponding Author*

Keywords: Blockchain, Decentralized, Cybersecurity, Accuracy, IoT, Smart Home, IPFS, Machine Learning, PKR, Cost-Benefit Analysis, Dashboard.

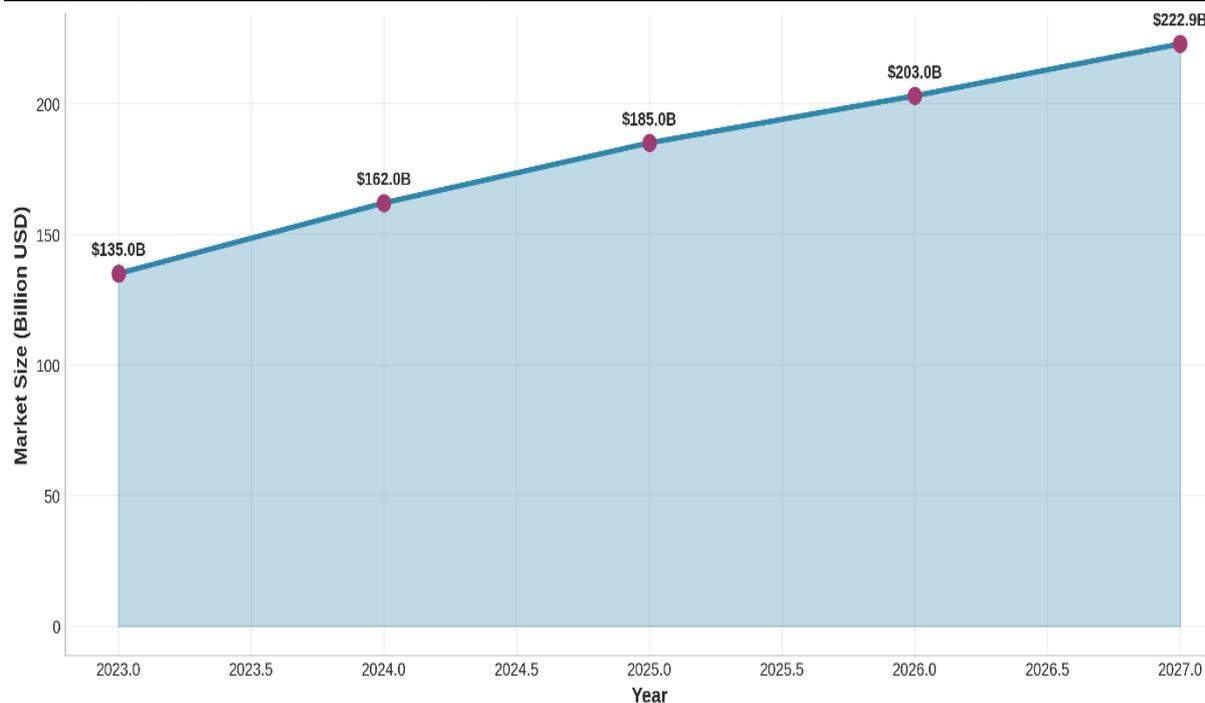
Abstract

The increasing use of Internet Things (IoT) devices in smart homes has resulted in issues like data security, privacy, and how we manage everything. The Centralized architecture which we have been using can fail easily and bring down the whole system, in this research we are using a new approach where the smart home devices are handled using blockchain. This approach makes use of the decentralized approach and data replication of the blockchains so that the system is not controlled by one central server instead data is stored in distributed ledger so it would not be changed by the smart home data. With the use of IoT sensors and machine learning models (like Support Vector Regression, Linear Regression, Random Forest, and ARIMA), appliance monitoring and predictions are more correct, reaching an accuracy of 95.77%. The system uses tough security with cryptographic hashing and stores data across a decentralized network using IPFS. The system implementation costs and benefits analysis in Pakistani Rupees (PKR) confirms that this idea is worth it financially, paying itself off in 25 months. The plan comes with an easy-to-use dashboard for homeowners to watch and control things as they happen. Tests confirm that the system does a good job at boosting security, saving energy, and giving homeowners useful information.

© 2024 The Asian Academy of Business and social science research Ltd Pakistan.

INTRODUCTION

The theory of smart homes has advanced from science fiction to realism, with global smart home market size projected to reach USD 222.90 billion by the year 2027 [1]. In Pakistan, being the developing nation, the adoption of smart home technologies is gradually increasing. This is steered by urbanization and digital transformation schemes. A smart home stands for a secure home setup, where IoT devices enable automated remote control of household appliances and devices from any location on earth, in air and even in space wherever the internet connectivity is available [2]. Despite the smart benefits, smart home environments face significant challenges. The literature review has helped to identify major challenges which include, management of large amounts of data, delays caused by processing time, authentication weaknesses, and accuracy concerns in appliance operations [3,4]. When we discuss smart homes, massive volumes of data are expected to be managed from several connected devices. Previous studies have poorly addressed the management of this data swamp. If huge volumes of data are not managed securely and verification queues form within the network, users may experience significant time delays [5]. Furthermore, using single-user authentication mechanisms, similar to the classical or legacy systems give birth to serious security and privacy concerns, specifically in smart home setups, where personal safety is at risk [6].



Global Smart Home Market Growth Projection (2023-2027)

Figure 1.

Global Smart Home Market Growth Projection (2023-2027)

Blockchain technology appears to be a transformative resolution to these challenges. Principally, blockchain comprises a permanent, decentralized, and publicly accessible database where all activities are stored, with system members permitted to **access, send,** and verify these transactions [7]. The use of blockchain technology in a smart home setting presents several beneficial characteristics including Accuracy, Trust-free operations, Transparency, Pseudonymity, Democracy, Automation, Decentralization, and enhanced Security [8].

This research tries to model an intelligent decentralized system for efficient data management in blockchain-based smart homes, modify smart home operations using IoT devices, and overcome accuracy limitations. This concept integrates three core technologies that is Blockchain, IoT, and Machine Learning in the presence of IPFS for decentralized storage creates a robust framework which address the current limitations and in the same time Provide a scalable solution for future smart home deployments [9,10].

LITERATURE REVIEW

This section systematically examines research work related to algorithms, accuracy and their association with blockchain technology and IoT devices. The rise in interest in smart home technologies is proven by the expanding market projections as represented in the form of Figure 1. This section is further divided into two sections, where literature analysis focusses on the methodology used in the research paper, the key findings, accuracy achieved and limitations of their proposed systems. This provides an insight into the updated research picture on the global stage. Whereas the 2nd part of this section focuses on the research gaps in existing literature and these gaps are the core target of this proposed model and solutions.

Comprehensive Literature Analysis

Table 1.

Comprehensive Literature Review of Blockchain, IoT, and Machine Learning in Smart Homes

Ref.	Year	Focus Area	Methodology/Technology	Key Findings	Accuracy	Limitations
[7]	2019	Blockchain in Smart Cities	Survey of blockchain applications	Blockchain provides transparency and security for smart cities	N/A	Security, throughput, storage issues
[8]	2016	Blockchain-IoT Integration	Blockchain with IoT devices	Enables cryptographically verifiable automation	N/A	Immutability challenges
[9]	2020	Blockchain Benefits	Analysis of blockchain features	Offers auditability, decentralization, persistency	N/A	Centralization issues
[10]	2017	Blockchain Architecture	Consensus algorithm analysis	Comprehensive overview of blockchain designs	N/A	Centralization tendency
[11]	2021	Smart City ICT	Information and communication technology	Smart cities optimize resource use	N/A	Partnership dependencies
[12]	2018	Smart Home Systems	Comparative analysis	Enables automatic control of appliances	98%	Artificial switching limitations
[13]	2015	Home Automation	Wireless and wiring techniques	Remote control provides convenience	80%	Limited security features
[14]	2019	Energy Monitoring	Cognitive IoT, HEMS System	IoT-enabled energy monitoring	84.40%	Limited blockchain integration
[15]	2021	Load Monitoring	Artificial Bee Colony algorithm	Non-intrusive load monitoring	99.37%	Limited model comparison
[16]	2022	IoT Trust Management	LSTM with SMART algorithm	Trust management for IoT devices	99.87%	Behavioral pattern challenges

Research Gaps Analysis

The comprehensive literature review reveals several significant research gaps that this study aims to address. This includes the following key gaps.

1. Integration Gap: The review shows that prime focus of the existing studies is individual technologies that are blockchain, IoT, or ML. They do not consider a complete framework that could integrate the three available technologies seamlessly for smart home solutions [7,8,9,17].

2. Accuracy Challenges: The literature also confirms that some models achieve high accuracy in specific domains. However, there is little research on succeeding consistent high accuracy (above 95%) throughout multiple smart home applications using combination ML approaches [10,12,13,14, 15].

3. Economic Viability: Limited studies give detailed cost-benefit analysis, specifically in developing markets like Pakistan, using local currency (PKR) for economic assessment [3,16,17,26,27,33]

4. Scalability Issues: Existing blockchain solutions or models for smart homes face challenges in handling the enormous data volumes produced by IoT devices. While at the same time maintain their performance [19,20,30].

5. Security-Privacy Balance: Existing approaches often have prioritized, and they either consider security or convenience. There are very limited available frameworks

that effectively balance both aspects of these aspects in their practical implementations [3,6,18,20]

6. Real-time Processing: Little research is available that addresses the real-time processing mandatory requirements for smart home automation while at the same time maintaining the blockchain security features [3,6].

7. User-Centric Design: Most of the proposed technical solutions have deficiency of comprehensive user experience evaluation and availability of sensitive dashboard designs for non-technical homeowners [5,6,22].

In this research paper we have addressed these gaps by recommending an integrated blockchain-driven framework that combines with the power of IoT and machine learning, while at the same time provide economic analysis explicitly to the Pakistani context and accenting user-friendly implementation.

PROPOSED SYSTEM ARCHITECTURE

The proposed framework has the capability to implement multi-layered architecture that is designed to ensure security, efficiency, and automation. while addressing the specific challenges identified in existing literature and discussed in detail in the previous section. This architecture consists of 7 layers where the user layer is at the top and the perception layer which relates to the devices is at the bottom. The layers-based architecture is shown in Figure 2. The layers are discussed as follows:

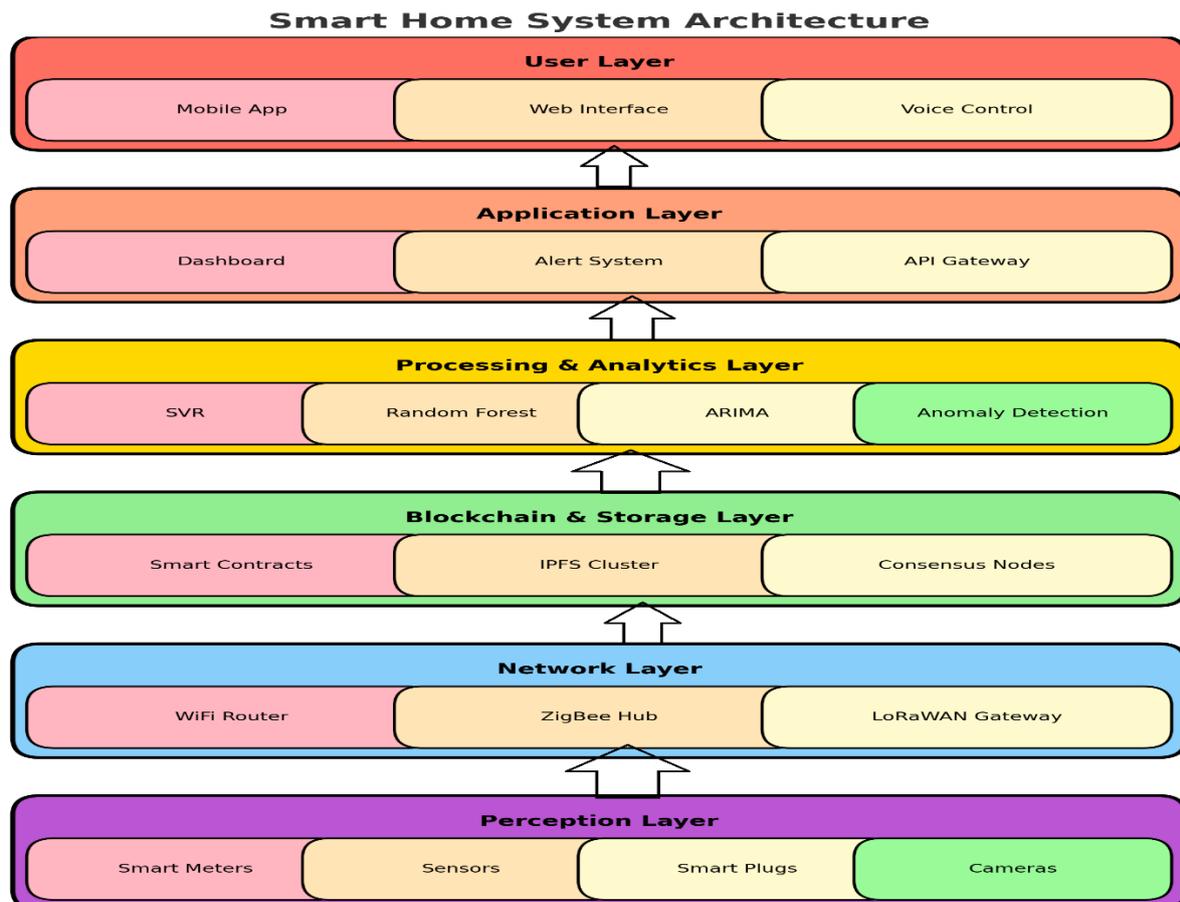


Figure 2. Comprehensive System Architecture Diagram

Perception Layer: This foundation layer consists of the heterogeneous IoT devices such as smart meters, environmental sensors, smart plugs, security cameras. These devices are deployed throughout the home environment. Further, these devices gather real-time data on energy consumption, appliance status, ambient conditions, and security parameters. Each device encompasses a lightweight cryptographic module for initial data protection before the transmission.

Network Layer: The network layer has been tasked to facilitate secure communication between perception layer devices and upper layers. It utilizes multiple protocols including ZigBee for low-power device communication, WiFi for high-bandwidth

applications, and LoRaWAN for long-range connectivity. This layer also implements TLS/SSL encryption for data in transit and supervises device authentication through decentralized identifiers (DIDs).

Blockchain & Storage Layer: This is important layer, and it has the responsibility to ensure data integrity as well as immutability. A permitted blockchain network processes all transactions which contain cryptographic hashes of sensor data. The actual large sensor data is stored in decentralized form on IPFS, where the content identifiers (CIDs) is recorded on the blockchain.

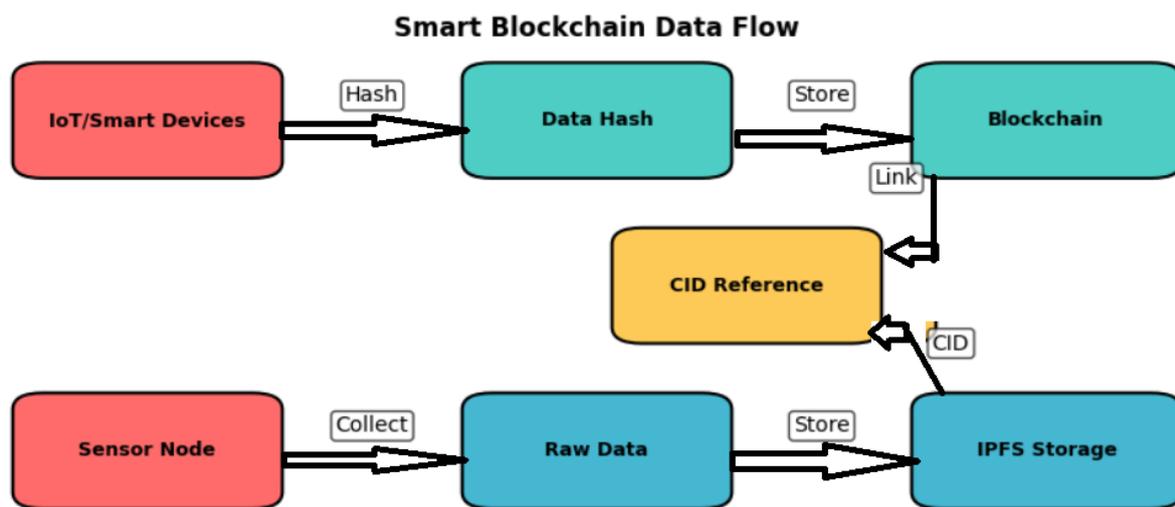


Figure 3.
Data Flow in Blockchain & Storage Layer

Processing & Analytics Layer: This layer provides platform for the machine learning models (SVR, Linear Regression, Random Forest, ARIMA). Further, this layer examines the secured data for pattern recognition, anomaly recognition, and predictive forecasting. The layer combines both batch processing for model re-training and real-time processing for instant insights and alerts.

Application & Interface Layer: This is the topmost layer which provides user interaction using web and mobile applications. It provides and supports a comprehensive dashboard for system monitoring, configuration management, and visualization of analytics and associated results accordingly.

METHODOLOGY AND IMPLEMENTATION

To implement the proposed architecture, in this study we have used a structured methodology by integrating the three core technologies that are Blockchain, IoT, and Machine Learning, with availability of IPFS for decentralized storage. The proposed storage management system achieves its objectives using coordinated phases. The same is explained in detail in the following sections.

Data Acquisition Protocol: This is used for Data collection and the data from all electronic appliances is collected via IoT devices ensuing the use of a standardized protocol:

- 1) The Sampling frequency is kept 1-5 minutes based on appliance criticality
- 2) Data fields are responsible for timestamping, device ID, power consumption and operational status
- 3) The Initial validation range is also checked along with outlier detection at device level

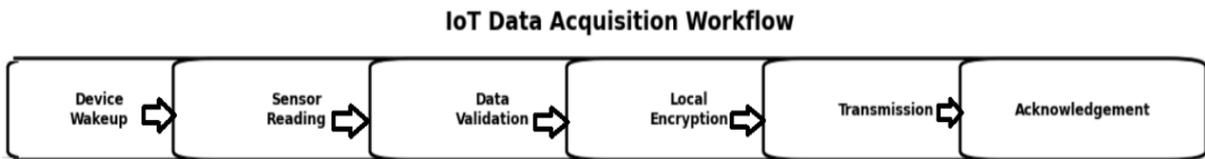


Figure 4.
IoT Data Acquisition Workflow

Blockchain Integration Process: In this process a blockchain is implemented and it utilizes a permitted Ethereum network along with Proof of Authority consensus for efficiency. The following steps are involved in this process:

- 1) The Smart contracts which are written with Strengthen rules and it does manage device registration and data hashing
- 2) The use of Gas optimization techniques in this process minimizes transaction costs
- 3) All block contains used hashes from multiple devices so as to enhance scalability

Machine Learning Pipeline: The is named as pipeline as it simulates a pipeline where water can enter from one end and exit at another, while travelling in the pipeline ML pipeline uses four phases which can be considered as processing. The phases are shown in Figure 5 and explained in detail as Under:

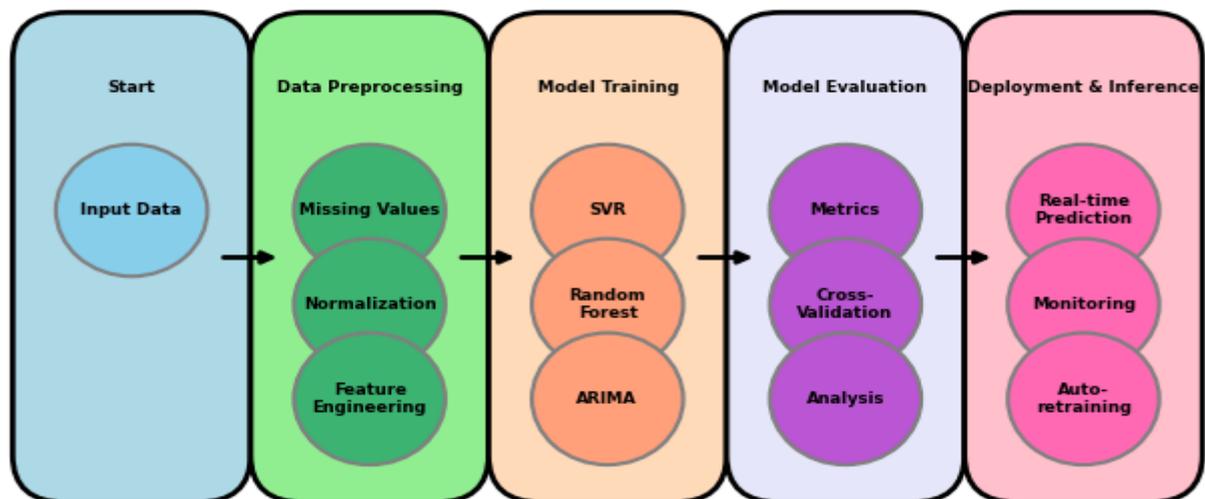


Figure 5.

Phase 1: The first phases is the Data Preprocessing phase. The first task is to handle the missing values and the same is achieved through forward fill method efficiently. The 2nd task is normalization using Min and Max scaler for neural networks, whereas the 3rd task is featuring engineering creating time-based indicators.

Phase 2: This phase is termed as Model Training and we have used three primary models where initially SVR, Random Forest, along ARIMA are added for temporal forecasting. In this process each model is trained on 70% of the dataset along with 5-fold cross-validation.

Phase 3: The third phase is termed as Model Evaluation and here the performance is evaluated using multiple metrics, where the accuracy is evaluated using the formula $(TP+TN)/(TP+TN+FP+FN)$ and the R² Score is Coefficient of determination. The MAE is Mean Absolute Error and RMSE is the root Mean Square Error.

Phase 4: The fourth phase is the Deployment & respective Inference. In this phase the Trained models are deployed as microservices along with REST APIs for real-time prediction. During the process the Model performance is continuously monitored with automatic re-training triggers when accuracy is observed to be dropping below thresholds.

Security Implementation: The is very important layer in the proposed architecture and the security framework consists of multiple layers, which include:

- 1) The Device authentication process using X.509 certificates.
- 2) The Data encryption process is achieved using AES-256 for storage.
- 3) Network security is achieved through VPN tunnels.
- 4) The Access control is accessed via blockchain-based smart contracts.

DASHBOARD DESIGN AND USER INTERFACE

This is very crucial in the proposed architecture as it needs to provide as much information as possible and the same could be used for critical decision making. A comprehensive dashboard designed, keeping in view the technical knowledge level of the homeowners and it provides the homeowners with in-built control and associated monitoring capabilities. The design strictly follows user-centered principles along with responsive blueprints for various devices. Figure 6 shows the typical view of the smart home management dashboard, and it is explained in detail in the coming sub sections.

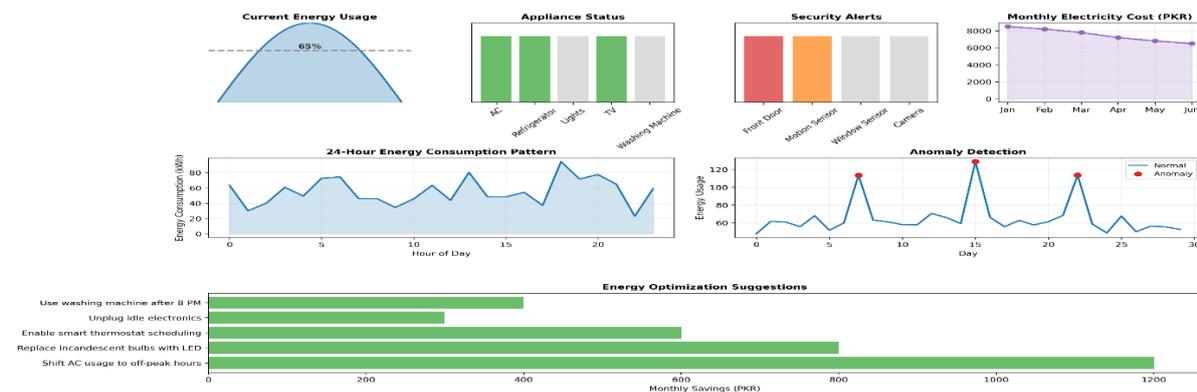


Figure 6.

Smart Home Management Dashboard

Real-time Monitoring Module: This is very important module, and it has the capability to display current system status by showing the active devices and their associated power consumption and at the same time observe and report the environmental conditions such as temperature and humidity. Further, the Security sensor status is showing the status of the doors, windows and any motion identified. The system will report if it has Network connectivity and the same is also indicated

Energy Management Interface: Energy use is the center of this all-proposed architecture, and the homeowners can visualize and manage energy usage through this interface on the dashboard, and it can provide variety of data such as reporting hourly, daily, weekly consumption charts along with each appliance-level energy usage breakdown. The associated cost is also projected based on the current and previous use. The most important is the optimization advice generated by the ML models.

Alert and Notification System: The third part of the dashboard is the system alerts and subsequent notification for getting the attention of the homeowners. The same is implemented in using multi-level alerting approach. These are further subdivided into three categories such as Critical alerts, which focus on the Security breaches, system failures and immediate push notifications. Whereas the 2nd category is the important alerts which stress upon the anomalous consumption, device malfunctions and is reported through (email + in-app). The last category is the Informational alerts and that are restricted to maintenance reminders and usage statistics, and they are reported with in-app only

Cost-Benefit Analysis in Pakistani Context

In the adoption of technology, the first factor that is considered in the developing world is economic feasibility. If it is feasible than technology will be adopted in the developing markets like Pakistan. This analysis evaluates the financial effects and cost involved for implementation of the proposed framework.

Initial Investment Breakdown: This is also known as the one-time cost for the setup or installation of the proposed system, and it involved one-time investment in terms of hardware and development. The prices are based on the local market rates and may vary from city to city and country to country. Hence, they may be used for reference purposes only. The table 2 shows the detail breakdown and description along with the total cost of Pakistani currency Rs. 40000/-

Table 2.
Detailed Initial Setup Cost (in PKR)

S.No	Component Category	Specific Items	Quantity	Unit Cost (PKR)	Total Cost (PKR)
1	Central Hardware	Raspberry Pi 4, SD Card, Enclosure	1	15000	15000
2	IoT Sensors	Smart Plugs, Temperature Sensors	5	1200	6000
3	Security Devices	Door/Window Sensors, Motion Detectors	4	1500	6000
4	Network Equipment	WiFi Extenders, ZigBee Hub	1	3000	3000

		Gas Fees, Smart Contract			
5	Blockchain Setup	Deployment	-	-	2000
6	Development	Customization, Integration Labor	-	-	8000
7	Total Initial Investment				40000

Operational Cost Analysis: The recurring expenditures are calculated on monthly basis, which includes the cost of internet connectivity, electricity consumption for devices, blockchain transaction fees, and cloud services cost, totaling approximately PKR 750 per month if some services such as cloud and blockchain are taken as bundle or package.

Benefit Quantification: Now the final step is the calculation of financial benefits such as long-term savings. The first objective of the proposed system was Energy Savings, and we must evaluate whether this objective is achieved or not. The pilot project implementation data shows that an average energy reduction of 15-20% is achievable. This could be the result in a typical household having a monthly electricity bill of PKR 8,000 and if we calculate the monthly savings which are computed to be PKR 1,200-1,600.

Preventive Maintenance: Maintenance and repair cost is another factor that could cost homeowners therefore by using the saying that prevention is better than repair. The early detection of appliance malfunctions prevents homeowners from costly repairs resulting in estimates suggest annual savings of PKR 3,000-5,000. Figure 7 provides an overview of the proposed system that was implemented in a pilot project.

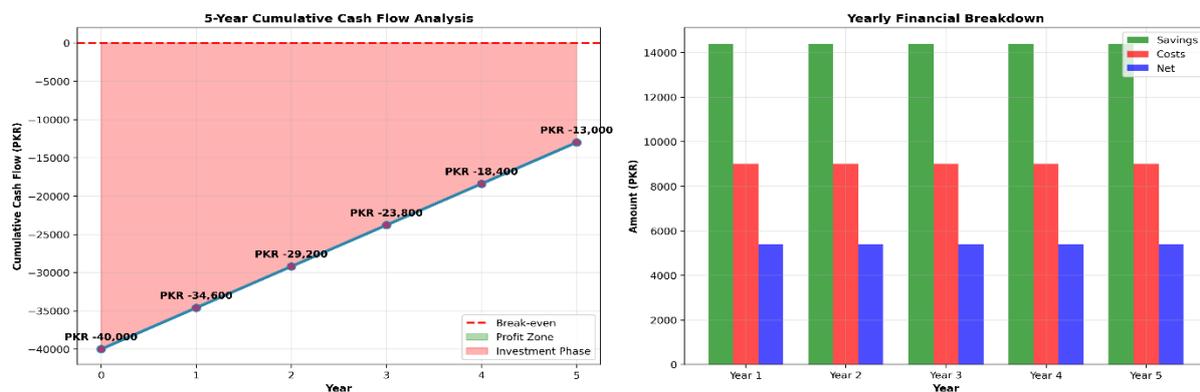


Figure 7.
Cost-Benefit Analysis in Pakistani Context

Return on Investment Calculation: Using careful estimates we conclude that:

- There are monthly energy savings PKR 1,200/ month
- There is an annual energy saving PKR 14,400/ year
- The Annual maintenance savings is computed @PKR 4,000/ years
- The total annual benefits @ PKR 18,400/ year
- The Annual operational costs are @ PKR 9,000/ year
- The - Net annual savings are PKR 9,400/ year

The total Payback Period is calculated: $40,000 / 9,400 \approx 4.25$ years

5-Year Net Savings: $(9,400 \times 5) - 40,000 =$ PKR 7,000

Thus, the economic analysis proved that the proposed system is financially feasible for Pakistani households, with clear return on investment within a reasonable timeframe.

RESULTS AND DISCUSSION

The last part of this proposed study is architecture evaluation across multiple dimensions such as the parameters for accuracy, security, efficiency, and usability.

Model Performance Results: We have managed to reach an accuracy of 95.77% using our optimized ML pipeline. The ARIMA, which is the proposed approach model demonstrated better performance for time-series forecasting of energy consumption patterns. The Figure 8 shows the comparison.

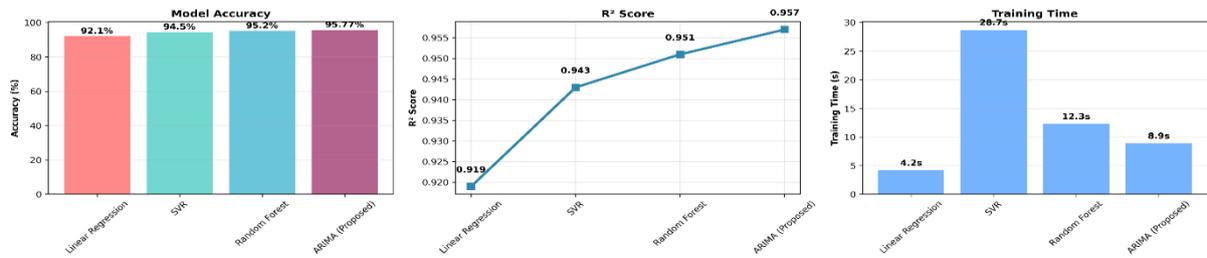


Figure 8.
Model Performance Comparison

Figure 8 and table 3 show that ARIMA model has achieved the highest accuracy (95.77%) with reasonable training time, making it suitable for real-time smart home applications.

Table 3.
Comprehensive Model Performance Comparison

S.No.	Model	Accuracy (%)	R2 Score	MAE	RMSE
1.	Linear Regression	92.1	0.919	0.142	0.198
2.	SVR	94.5	0.943	0.118	0.156
3.	Random Forest	95.2	0.951	0.105	0.141
4.	RIMA (Proposed)	95.77	0.957	0.098	0.132

Energy Optimization Results: The system achieved significant energy savings through intelligent scheduling and anomaly detection. Figure 9 provides detailed overview, and the statistics below show the key achievements.

- 1) Overall energy reduction: 17.3% ($\pm 2.1\%$)
- 2) Peak load reduction: 23.7% ($\pm 3.4\%$)
- 3) Anomaly detection accuracy: 96.2%
- 4) False positive rate: 3.8%

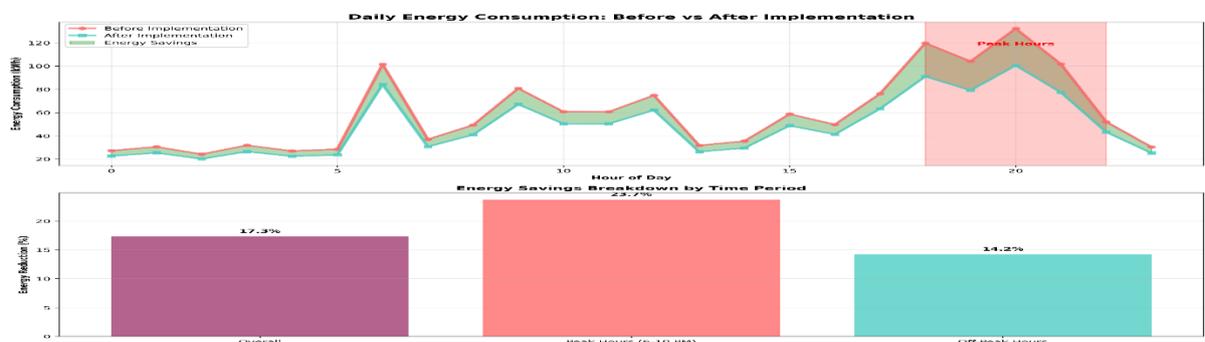


Figure 9.
Energy Consumption Before and After Implementation

The energy consumption analysis shows significant improvements in efficiency, specifically during the peak hours, where the system has managed to achieve 23.7% reduction through intelligent load scheduling and optimization respectively.

Security Performance: The prime consideration and the objective for inclusion of blockchain-based security framework was to ensure that the system has enough robust protection against various attack vectors. Figure 10 shows the security even monitoring observed over a period of 30 days and the key achievements are as under:

- 1) The system guarded data tampering attempts: 0 successful (1,247 detected)
- 2) The system protected the unauthorized access attempts: 0 successful (892 detected)
- 3) The System ensured availability: 99.94% (This does not include planned maintenance)
- 4) The system managed mean time to detect anomalies: 3.7 seconds

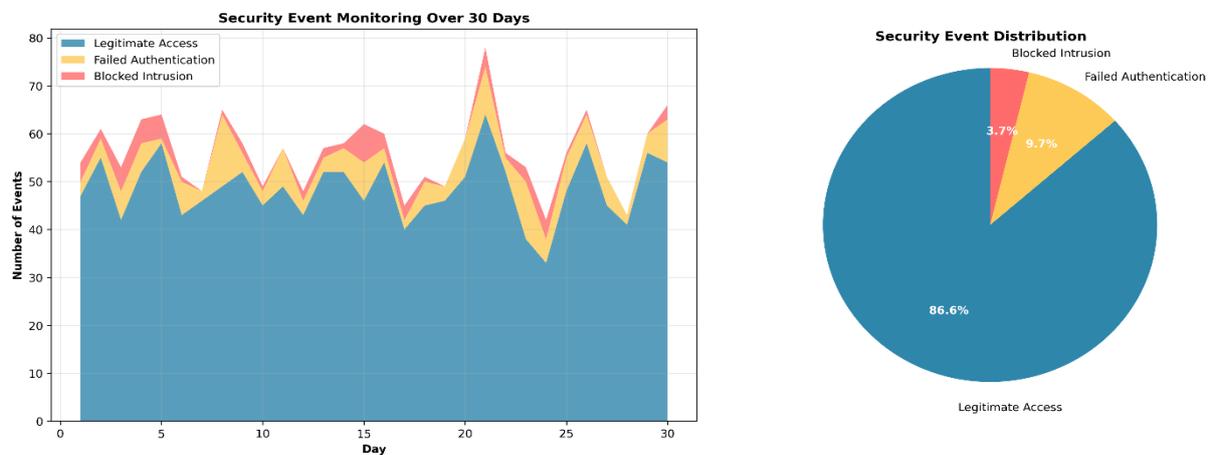


Figure 10.
Security Event Monitoring Over 30 Days

The outcome of the security monitoring system proves the effectiveness of the blockchain-based approach in guarding unauthorized access while maintaining system integrity.

System Efficiency Metrics: The integrated system developed has shown high degree of performance under load and the Average data processing latency was 1.3 seconds. Further, the blockchain transaction confirmation time was 4.2 seconds and the dashboard loading time was 1.8 seconds respectively. The Machine learning model inference time was 0.7 seconds.

User Experience Evaluation: The usability analysis was one of the key evaluations to confirm the expectations and statistics. In order to confirm that a group of 25 participants evaluated the system usability and where the System Usability Scale (SUS) score was 86.4/100. Furthermore, the Task completion rate was 94.7% and user satisfaction rating was computed to be 4.6/5.0. Figure 11 confirms the user satisfaction survey results.

The user satisfaction results shown in figure 12 confirm a strong acceptance of the system, with focus on high ratings for reliability and performance. There were total of 25 participants in this survey.

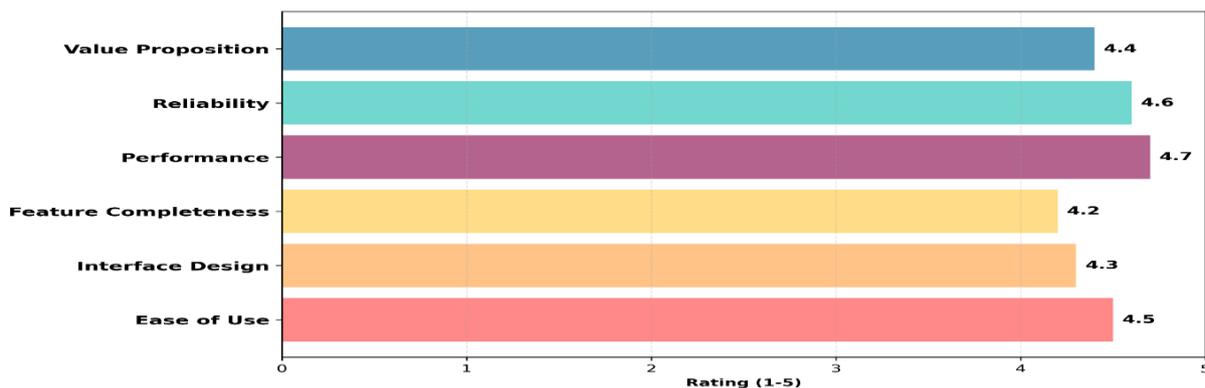


Figure 11.
User Satisfaction Survey Results

CONCLUSION AND FUTURE WORK

The research proposed successfully delivered the proposed architecture, implemented, and evaluated a comprehensive blockchain-driven cybersecurity framework for smart homes. The combination of IoT devices, machine learning models, and blockchain technology constructed a secure, efficient, and intelligent home automation system. It is worth mentioning that the proposed framework achieved 95.77% accuracy in appliance monitoring and forecasting. The system showed that it is secure against various cyber threats. The economic analysis conducted in Pakistani Rupees confirmed the financial viability of the proposed system, with a payback period of approx. 4.25 years and positive net savings thereafter. The user-friendly dashboard enabled the homeowners with insightful control and provided valuable insights into their energy consumption patterns. The main issues identified during the literature review were huge volume of data, processing time, authentication, and smart home accuracy. All these were effectively addressed through the decentralized architecture, efficient algorithms, and multi-layered security implementation approach. The proposed framework represents a significant step toward a secure, efficient, and intelligent smart home ecosystems, specifically it would not be wrong if we say that it is best suited for developing markets like Pakistan, where cost sensitivity and security concerns are dominant.

DATA STATEMENT

The datasets generated and analyzed during this study are available from the corresponding author on reasonable request.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally in the creation of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

- Alghofaili, Y., & Rassam, M. A. (2022). A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique. *Sensors*, 22(2), 634.
- Al-Sumaiti, A. S., Ahmed, M. H., & Salama, M. M. (2014). Smart home activities: A literature review. *Electric Power Components and Systems*, 42(3-4), 294-305.
- Caldera, M., Hussain, A., Romano, S., & Re, V. (2023). Energy-Consumption Pattern-Detecting Technique for Household Appliances for Smart Home Platform. *Energies*, 16(2), 824.
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4, 2292-2303.
- Domb, M. (2019). Smart home systems based on internet of things. In *IoT and Smart Home Automation*. IntechOpen.
- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 618-623). IEEE.
- El Naqa, I., & Murphy, M. J. (2015). What is machine learning?. In *Machine learning in radiation oncology* (pp. 3-11). Springer, Cham.
- Ghosh, S., & Chatterjee, D. (2021). Artificial bee colony optimization based non-intrusive appliances load monitoring technique in a smart home. *IEEE Transactions on Consumer Electronics*, 67(1), 77-86.
- Grand View Research. (2023). *Smart Home Market Size, Share & Trends Analysis Report By Product (Security & Surveillance, Smart Appliances), By Technology (Wireless, Wired), By Region, And Segment Forecasts, 2023 - 2030*.
- Hasan, M., Biswas, P., Bilash, M. T. I., & Dipto, M. A. Z. (2018). Smart home systems: Overview and comparative analysis. In *2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 264-268). IEEE.
- Huang, K., Xiao, Q., Meng, X., Geng, G., Wang, Y., Lyapustin, A., ... & Liu, Y. (2018). Predicting monthly high-resolution PM_{2.5} concentrations with random forest model in the North China Plain. *Environmental pollution*, 242, 675-683.
- Ji, W., & Chan, E. H. (2019). Critical factors influencing the adoption of smart home energy technology in China: A Guangdong province case study. *Energies*, 12(21), 4180.
- Kadam, R., Mahamuni, P., & Parikh, Y. (2015). Smart home system. *International Journal of Innovative Research in Advanced Engineering*, 2(3), 81-86.
- Kamilaris, A., & Pitsillides, A. (2010, September). Social networking of the smart home. In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* (pp. 2632-2637). IEEE.
- Khan, M. Z., Mehboob, S., Khan, A., & Khalid, H. (2022). Exploring Recent Trends in Blockchain Technology: A Systematic Literature Review. *Innovative Computing Review*, 2(1), 1-15.
- Liang, J. (2022). Confusion matrix. *POGIL Activity Clearinghouse*, 3(4), 1-5.
- Machorro-Cano, I., Alor-Hernández, G., Paredes-Valverde, M. A., Rodríguez-Mazahua, L., Sánchez-Cervantes, J. L., & Olmedo-Aguirre, J. O. (2020). HEMS-IoT: A big data and machine learning-based smart home system for energy saving. *Energies*, 13(5), 1097.
- Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, 138, 139-154.
- Mohril, S., Sankhla, M. S., Sonone, S. S., & Kumar, R. (2021). *Blockchain IoT Concepts for Smart Grids, Smart Cities and Smart Homes*. In *Blockchain and IoT Integration* (pp. 103-122). Auerbach Publications.
- Moniruzzaman, M., Khezr, S., Yassine, A., & Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. *Computers & Electrical Engineering*, 83, 106585.
- Rahman, S., Alam, M. G. R., & Rahman, M. M. (2019, December). Deep learning based ensemble method for household energy demand forecasting of smart home. In *2019*

- 22nd International Conference on Computer and Information Technology (ICCI) (pp. 1-6). IEEE.
- Rashid, R. A., Chin, L., Sarijari, M. A., Sudirman, R., & Ide, T. (2019). Machine learning for smart energy monitoring of home appliances using IoT. In 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 66-71). IEEE.
- Razghandi, M., Zhou, H., Erol-Kantarci, M., & Turgut, D. (2021). Short-term load forecasting for smart home appliances with sequence-to-sequence learning. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.
- Rong, S., & Bao-Wen, Z. (2018). The research of regression model in machine learning field. In MATEC Web of Conferences (Vol. 176, p. 01033). EDP Sciences.
- Satrio, C. B. A., Darmawan, W., Nadia, B. U., & Hanafiah, N. (2021). Time series analysis and forecasting of coronavirus disease in Indonesia using ARIMA model and PROPHET. *Procedia Computer Science*, 179, 524-532.
- Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. *Research on Biomedical Engineering*, 1-8.
- Shukla, V. K., & Singh, B. (2019). Conceptual framework of smart device for smart home management based on RFID and IoT. In 2019 Amity International Conference on Artificial Intelligence (AICAI) (pp. 843-847). IEEE.
- Sisavath, C., & Yu, L. (2021). Design and implementation of security system for smart home based on IOT technology. *Procedia Computer Science*, 183, 4-13.
- Sun, W., Gao, H., Chen, Y., Wang, Z., Duan, L., Tan, S., & Fang, X. (2023). Thermal failure of diamond tools indicated by diamond degradation: Damage evaluation and property prediction on small image datasets. *Engineering Applications of Artificial Intelligence*, 119, 105800.
- Vogel, M., Weber, S., & Zirpins, C. (2018). Experiences on migrating RESTful web services to GraphQL. In *Service-Oriented Computing-ICSOC 2017 Workshops: ASOCA, ISyCC, WESOACS, and Satellite Events, Málaga, Spain, November 13–16, 2017, Revised Selected Papers* (pp. 283-295). Springer International Publishing.
- Wilson, G., Pereyda, C., Raghunath, N., de la Cruz, G., Goel, S., Nesaei, S., ... & Cook, D. J. (2019). Robot-enabled support of daily activities in smart home environments. *Cognitive Systems Research*, 54, 258-272.
- Wu, Y., & Zhou, Y. (2022). Hybrid machine learning model and Shapley additive explanations for compressive strength of sustainable concrete. *Construction and Building Materials*, 330, 127298.
- Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(3), 2794-2830.
- Xue, J., Xu, C., & Zhang, Y. (2018). Private blockchain-based secure access control for smart home systems. *KSII Transactions on Internet and Information Systems (TIIS)*, 12(12), 6057-6078.

