processes

MDPI

Article

Smart Home Gateway Based on Integration of Deep Reinforcement Learning and Blockchain Framework

Zeinab Shahbazi, Yung-Cheol Byun * and Ho-Young Kwak *

Department of Computer Engineering, Institute of Information Science Technology, Jeju National University, Jejusi 63243, Korea; zeinab.sh@jejunu.ac.kr
* Correspondence: ycb@jejunu.ac.kr (Y.-C.B.); kwak@jejunu.ac.kr (H.-Y.K.)

Abstract: The development of information and communication technology in terms of sensor technologies cause the Internet of Things (IoT) step toward smart homes for prevalent sensing and management of resources. The gateway connections contain various IoT devices in smart homes representing the security based on the centralized structure. To address the security purposes in this system, the blockchain framework is considered a smart home gateway to overcome the possible attacks and apply Deep Reinforcement Learning (DRL). The proposed blockchain-based smart home approach carefully evaluated the reliability and security in terms of accessibility, privacy, and integrity. To overcome traditional centralized architecture, blockchain is employed in the data store and exchange blocks. The data integrity inside and outside of the smart home cause the ability of network members to authenticate. The presented network implemented in the Ethereum blockchain, and the measurements are in terms of security, response time, and accuracy. The experimental results show that the proposed solution contains a better outperform than recent existing works. DRL is a learning-based algorithm which has the most effective aspects of the proposed approach to improve the performance of system based on the right values and combining with blockchain in terms of security of smart home based on the smart devices to overcome sharing and hacking the privacy. We have compared our proposed system with the other state-of-the-art and test this system in two types of datasets as NSL-KDD and KDD-CUP-99. DRL with an accuracy of 96.9% performs higher and has a stronger output compared with Artificial Neural Networks with an accuracy of 80.05% in the second stage, which contains 16% differences in terms of improving the accuracy of smart homes.

Keywords: smart home; blockchain; deep reinforcement learning; internet of things

Citation: Shahbazi, Z.; Byun, Y.-C.; Kwak, H.-Y. Smart Home Gateway Based on Integration of Deep Reinforcement Learning and Blockchain Framework *Processes* **2021**, *9*, 1593. https://doi.org/10.3390/pr9091593

Academic Editor: Frederic Cadet

Received: 5 July 2021
Accepted: 2 September 2021
Published: 5 September 2021

1. Introduction

The smart home is the combination of IoT systems and comfort, high-quality lifestyle, security, convenience, etc. Smart home networks based on IoT are interconnected with smart devices such as wearable devices, smart homes, and smart meters. The smart home has the capability of encouraging human life to an independent lifestyle. The global market for smart homes is rapidly increasing, and it is anticipating to achieve 53.45 billion dollars in 2022, and this process has the growth of 20.8% during years 2018–2022 [1]. As stated by Gartner [2], the previously visualized records reporting 500 million smart home devices increases to 700 million in a year, and this is a challenging record in terms of security of these devices [3]. One of the advantages of an IoT network is to be sensitive to the security threads. The devices are normally without a manager and no one to supervise [4–6]. The devices are interrelated together from a gateway using different wireless protocols which clear the way for eavesdropping for attackers with less processing steps for which applying the security technique for each device is troublesome [7,8]. A real criminal hacking case happens in 2018 in a North American casino to steal data using fish tank [9,10]. Discovering that the treads from casinos performs some security prudence, but the hackers could send data from the tank to Finland. The IoT techniques should prepare and improve the architecture

to overcome more advanced attacks or terrorist attacks [11,12]. Smart home common security problems are in terms of data privacy, authentication, access control mechanism, the issue of system configuration, etc. [13–16]. The traditional IoT systems are centralized, connected with the cloud to lead the network failure in the compromised central server. In another case, IoT devices have computation power limitations that cause the delicate to different security threats. There are various solutions to overcome the mentioned problems based on the security layer presented in [17,18] and the decentralized network architecture implementation of blockchain for smart homes in [19–21]. In the past decades, the solve security is based on the blockchain identified which creates trust, reliability, scalability, and privacy based on the paradigm of IoT [22,23]. The smart home adoption with blockchain decreases the concern of massive security e.g., authentication, integrity, authorisation, and attacks single point [24]. The Comprehensive Intrusion Detection System (IDS) is enough to overcome this problem to identify the conventional approach's unique arrangements. The recent technology is known as Deep Reinforcement Learning (DRL), which can apply in the data flow evaluation to interference spots and patterns of attacks. This study presents blockchain and DRL combination in smart homes based on different applications such as data sharing in the smart home.

The main contributions of this paper include:

- Using a blockchain network for the smart home to investigate the problem of security.
- Evaluating the common IoT devices of the smart home based on hardware implementation.
- Presenting the architecture of a smart home gateway to relieve the recent challenges of the smart home.
- Improving the performance of the proposed system compared with other existing works.
- Deep Reinforcement Learning applied to predict and interpret the data.
- Deep Reinforcement Learning creates the safer smart home using IoT sensors for improving the performance of the process.

The remainder of this paper, organized as Section 2, describes the related studies for the smart home architecture. Section 3 describes the proposed machine learning approach for the smart home gateway based on the blockchain framework. Section 4 describes the implementation and experimental results of the proposed system, and we conclude this paper in discussion and conclusions.

2. Related Works

This section presents a detailed explanation of the existing studies in smart home security based on IoT [25–31], blockchain, and machine learning [10,32–40]. Due to the flexibility of the blockchain framework, a smart home ecosystem can shape easily. We have discussed the public and private blockchain framework in the smart home and smart home gateway in detail.

2.1. Smart Home Based on Public Blockchain

Varshney et al. [41] presented a blockchain-based secure platform using IoT sensors for the smart home to protect it from threads. The implementation of this system shows the secure communication between IoT devices in the distributed environment. Lazaroiu et al. [42] presents the integration of IoT and blockchain with a smart district model and gives access to users for the power grid. The developed system makes the connection between the user and blockchain in the power grid system. The one who accesses the solar panel configuration can amuse the network and buy and sell the energy through blockchain. Aggarwal et al. [43] proposed the scheme of secure energy trading, famous for Energy-Chain using the smart grid. The security of the implemented system evaluates based on the cost, communication, and computation time. Dorri et al. [44] presented the blockchain-based smart home for the representative case study. The author designed the smart home core building block. This system tested the transaction process in various

components. The privacy and security analysis performed in the smart home architecture. The final process claims the lower processing time and ease of use for IoT devices.

2.2. Smart Home Based on Private Blockchain

Dorri et al. [45] presented the lightweight, secure system based on blockchain for the smart home. The smart homeowner centralizes the blockchain. The connections are defined to use a shared key for communication. The transaction process checked through lightweight hashing to disclose any deflection. This system is secured from Distributed Denial-of-service (DDoS) attacks with availability, dentiality, and integrity. One of the disadvantages of IoT devices is less storage area and limited computation power. In another point of view, there is a need for huge money and time for data streaming which causes the author to combine the blockchain and smart contract for improving the system security [46–48], for which the novel approach is lightweight based on a smart contract for smart home architecture. Table 1 shows the existing studies of smart homes in terms of public and private blockchain. It compares this framework in terms of confidentiality, integrity, and scalability.

2.3. Smart Home Gateway

Smart home technology in terms of the residential environment is growing due to recent developments. There is the possibility of easily controlling the living environment using a control system and devices [49]. Environmental manipulation contains various conditions, e.g., cost, preferences, and type of dependent technologies. To control and monitor the smart home, various devices communicate through the gateway [50]. To design a network using a gateway connection, there is a need for some functionality in the concept of home network connection, internet connection, remote control, software update and expansion, and a remote operation with a secure and reliable method. The goal for implementing the mentioned gateways is to create a sustainable smart home. Sivaraman et al. [51] presented the smart home network based on security vulnerabilities. Using ISP, managing devices and certificate verification is possible but not enough in terms of security due to less user data information. Jamil et al. [52] presented the integration between machine learning and blockchain for the smart grid sustainable electrical power. The applied blockchain platform is hyperledger calliper based on the resource utilization, latency, and throughput. This system is useful for energy crowdsourcing system. Table 2 presents the overview of the recent opportunities in blockchain based smart home technology.

Table 1. Smart home blockchain-based architecture existing studies.

Authors	Building Block	Type of Blockchain	Confidentiality	Integrity	Scalability
[41]	Physical layer Sensors wifi Bluetooth Distributed ledger	Public	Yes	Yes	No
[42]	Distributed ledger Smart contract PoW PoS	Public	Yes	No	Yes
[43]	Pow Minor node Normal node	Public Private	Yes	No	Yes
[44]	Minor smart home Backup drive	Public	Yes	No	Yes
[53]	Data storage Pow Control module	Public	Yes	Yes	No
[46]	Smart contract Local minor IoT devices	Private	Yes	Yes	Yes
[54]	Ethereum	Private	Yes	No	No
[55]	Cloud network Smart contract	Consortium	Yes	No	Yes
[56]	Ethereum Cryptography Consensus algorithm	Public	Yes	Yes	No
[57]	Gateway of smart home Ethereum	Private	Yes	No	No
[58]	Nodes Encryption	Consortium	Yes	Yes	No

2.4. Smart Home Based on Reinforcement Learning

The spread of a home energy management system contains two types of software and hardware to allow users in terms of managing the energy and production. Due to this process, Cheng et al. [59] used Q-learning based on a model-free process for controlling and window systems in terms of energy saving which achieve 23% of saving energy. Wei et al. [60] used the DRL based on a data driven method and 20% cost reduction. Nagy et al. [61] applied a data driven method due to a rule-based control system. Wang et al. [62] applied model-free RL to reduce the energy consumption and Gao et al. [63] applied DRL for thermal comfort control and an energy optimization process.

Table 2. Blockchain technology applications' opportunities, problems, and answers.

Sectors	Opportunities	Problems	Answers
IoT	- Increasing the network IoT devices - Connection management between devices - Developing the IoT devices based on decentralized architecture - Data transaction security - smart home devices data collection facilitating	- Increasing the capacity of process - Necessity of high power consumption - Increasing the problem of copy right for data ownership	- Cloud computing development for related data using interoperability. - Managing social network using hierarchical processing - Identify the ownership based on management plan
Financial transaction	- Using digital currency between various nodes - Using cryptocurrency for speed up the financial transaction - Security improvement by transaction tracing - Electricity cost reduction compare to real-time environment	- Require a suitable cryptocurrency - Improving the transaction security because of the attack possibility - Need for flexibility addressing	- Avoid the increasing in huge amount by managing the cryptocurrency
Smart contract	- Using the decentralized node for simplifying financial transactions - Maximizing the security - defining the way to pay to consumers digital incentives - Inspire the consumers for participation in programs	- Lack of standard protocols, contracts and interface - Monitoring contracts require high resources	- Providing the draft of standard contract. - Based on the value of contract embedding the security - Applying the authorization and for standard security

3. Integration of Blockchain and Deep Reinforcement Learning in Smart Homes

This section presents the smart home technology based on the integration of blockchain and machine learning. In recent technology, the smart home became the famous process to secure and improve the performance of buildings in terms of usage of IoT devices and overcome the problem of attacks from hackers to get users' information. In this process, we proposed blockchain-based smart home security integrated with deep reinforcement learning. The main reason for applying deep reinforcement learning is that this algorithm is learning-based, and, based on this reason, improving the smart home's performance is higher than other existing works. Figure 1 shows the architecture of smart home based on blockchain framework with reinforcement learning. Collecting information is from different IoT sensors and smart devices. The dataset uses the deep reinforcement learning framework to process into the blockchain to remove the errors, e.g., disruption, repetition, data value loss. The related problems to data excluded from the DRL framework. DRL has the ability to focus on segments of the chain instead of the data collection process. This reason creates the unique framework for fraud detection, theft detection based on prediction, etc.

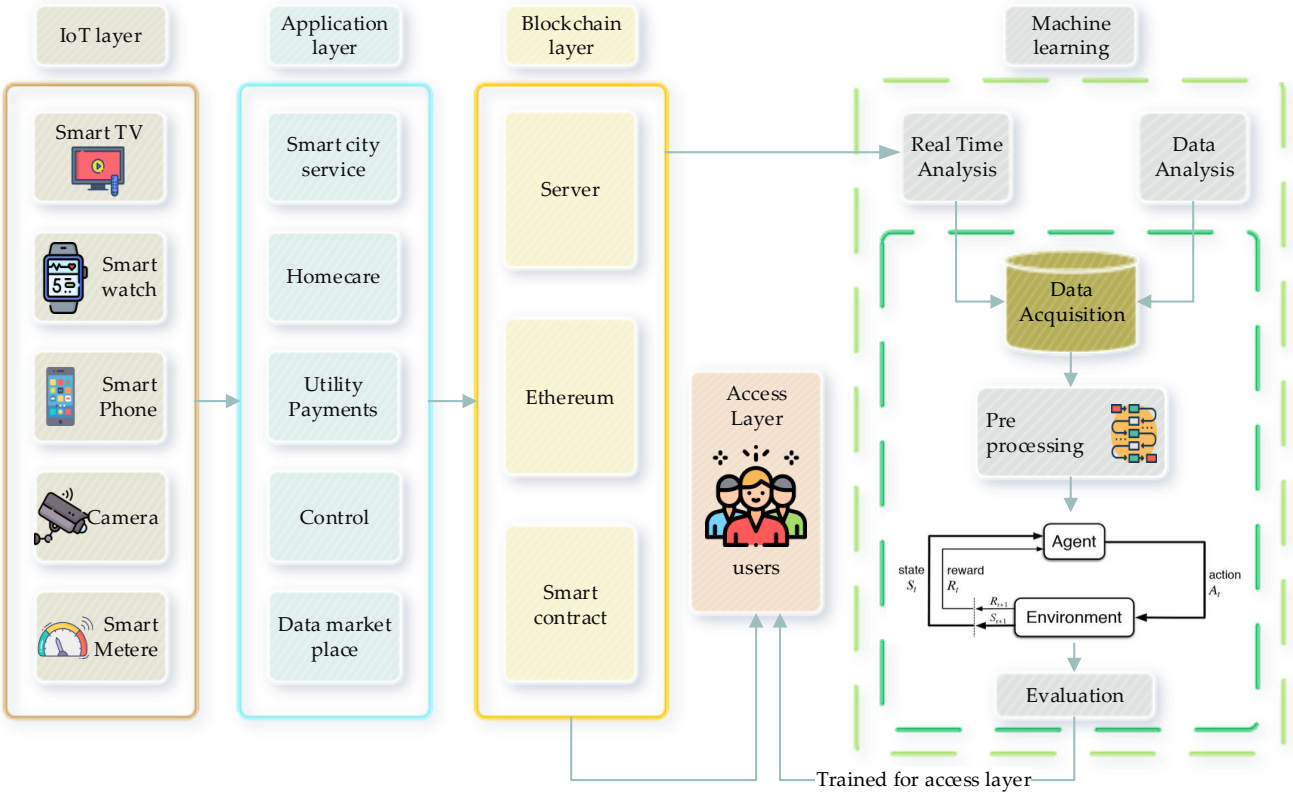


Figure 1. Smart home architecture based on combination of machine learning and blockchain.

3.1. Deep Reinforcement Learning

Applying machine learning techniques in the smart home framework became a permanent solution for various aspects. These techniques control the IoT devices, which are the most related to improving home security. In this process, the DRL technique directly optimizes and expresses the value function, environmental models, and strategies in an end-to-end process. DRL can build the model based on pattern extraction using original high-dimensional data and the basis of control policy. An optimization and decision control-based DLR is shown in Figure 2. There are two main parts in this process as training and execution sections. The training section is a learning-based section that executes parts and uses them to optimize decisions to learn knowledge in a real environment. In emergency cases, the agent links to the new environment and improves the captured reward to replace optimization.

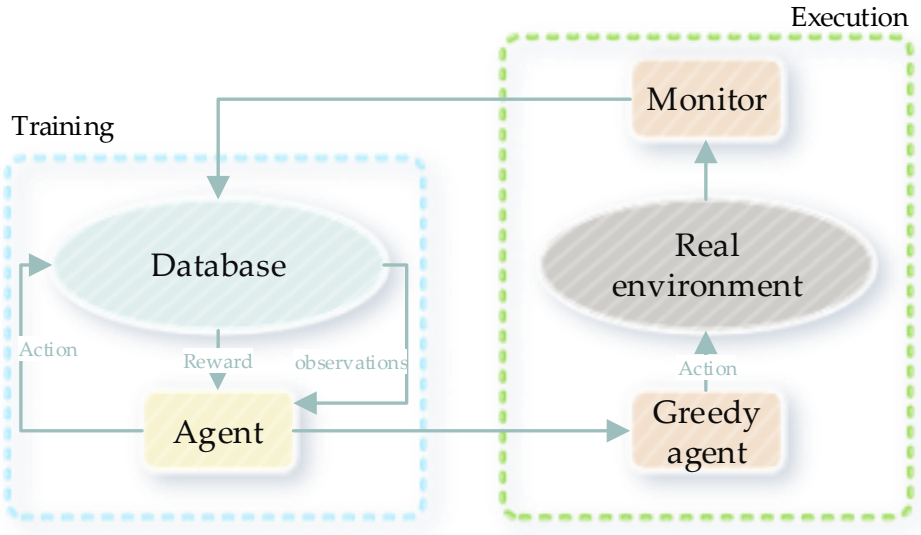


Figure 2. Deep reinforcement learning framework in smart home optimization and decision control.

Markov Decision Process and Q-Learning

There are four main components in Markov Decision Process (MDP) as state (E), actions (C), the probability of state transitions distribution ($p(|e,c)$), and probability of reward governing distribution ($q(|e,c)$). The details of each part are presented as: The responsibility of an agent in a presented smart home gateway is to select actions from environment based on maximizing reward. Following the home automation system, the agent controls the home energy system. The environment in a smart home system refers to the energy production of the smart products of home and the usage of price in this system e.g., Wi-Fi. The reward in this system is the key element of DRL algorithm which shows the Guidance of the agent to reach the acceptable value function in terms of the right direction. This strategy objective function is: more rewards equal more benefit from the real-world energy system. The action taken in the proposed smart home is the output of the DRL algorithm, which is the Q-value combined action. This means the time-shit load, power-shift load, power balance, devices physical constraint, satisfaction of demand, and other constraints. The task of MDP has a possibility to discretize to time periods. Each time period t, a state is occupied with agent $e_t \in E$ and selects the action in the current state from possible actions. Execute the result of the selected action in the transition state to $E_{(t+1)}$ and direct reward $W(E_t, c_t)$. The MDP can be applied in smart home technology and used in the completed model. Lack of information related to environment e.g., missing the transitions and reward probability, to generate the optimal policy, the model-free Q-learning can be used in this process. The temporal difference method contains the Q-learning that is able to incrementally predict online. The updated rule of Q-learning is defined in Equation (1):

$$Q(e,c) \longleftarrow Q_{e,c} + \beta[r + \alpha Q(\bar{e},\bar{c}) - Q(e,c)] \quad (1)$$

β represents the learning rate of the estimated value lower than one during the learning process. Algorithm 1 shows the simulation steps involved in the DRL process.

Algorithm 1 Smart home simulation process

Initialize: Parameter building
Initialize: $Q(e, c)$ arbitrarily
Repeat: **(for each episode)**
Initialize e
Repeat
Based on Q policy choose c from e
Take action c
Building state update
Evaluate reward r
$Q(e, c) \longleftarrow r + \alpha Q(\overline{e}, \overline{c})$
$e \longleftarrow \overline{e}$
Until terminal is e

In Q-learning for each state and action, Q-value pairs are saved in the Q-table. This process is updated with the stochastic gradient descent in Equation (2):

$$Q(e_t, c_t) \longleftarrow Q_{e_t, c_t} + \beta(R_{t+1} + \alpha max Q(e_{t+1}, \overline{c}) - Q(e_t, c_t)) \quad (2)$$

β is the control of step-size and $R_{t+1} + \alpha max Q(e_{t+1}, \overline{c})$ is the envisage reward which can capture from action c_t in terms of e_t state. In terms of high dimensions, the agent is slow at value learning. If the action and state are high-dimensional, then the Q-learning process becomes unrealistic. The state is the incorporation of the smart home total information and keeps all the historical records. Actions are selected based on the policy for each time interval using E-greedy. The strategy of E-greedy selects the best actions from the policy and extracts the governed time by E.

3.2. Gateway Network Based on Blockchain in Smart Homes

The applied blockchain in smart home gateways is a conclusive data transmission process, authority, authentication, and confidence between devices. A smart home is a centralized and distributed network at the cloud layer of blockchain. The presented smart home in blockchain framework contains three main layers: the device layer, gateway later, and cloud layer as shown in Figure 3. Smart devices are collected in device layers that collect and monitor smart home data in different IoT devices configured in smart homes. The gateway layer saves the generated data from the device layer and is based on user needs. The last layer, which is the cloud layer, registers the gateway ID and process data of each gateway in the blockchain. The blocks are shared for users that they can access anytime they are needed. The data collection process allows the devices to collect and save into blockchain. This process gives this opportunity to the user to create block, format, verify, etc.

Figure 4 shows the structure of blocks in this system. There are five main components: previous block hash, timestamp, nonce, fromdeviceid, and todeviceid.

- Previous Block Hash: To keep the blockchain framework tamper-proof, the blocks always record the previous block hash information.
- Timestamp: To record the start and end time of any event, the timestamp is added to the block, stores the metadata, and logs as temporal information.
- Nonce: Nonce is a mathematical evaluation target value for generating the random numbers.
- FromDeviceID: Record of the coming transactions of the source device.
- ToDeviceID: Record the destination of the transaction of the target device.

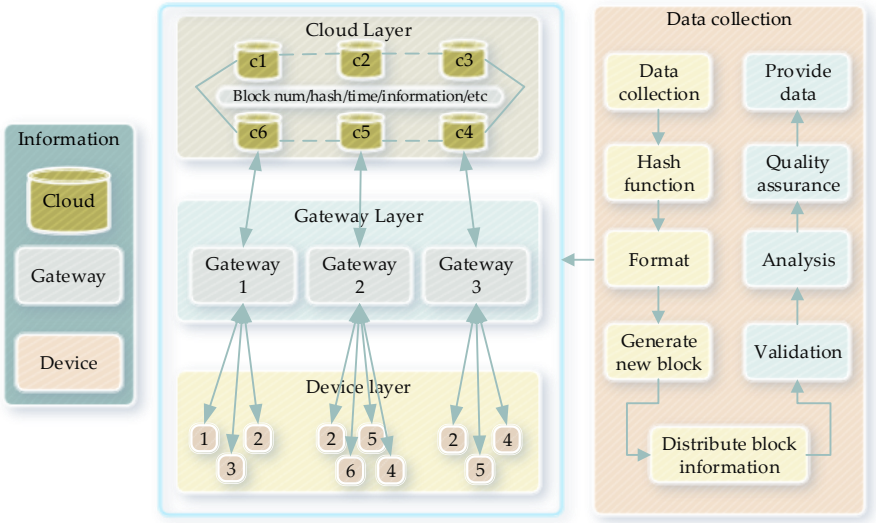


Figure 3. Smart home gateway architecture based on the blockchain cloud-enabled framework.

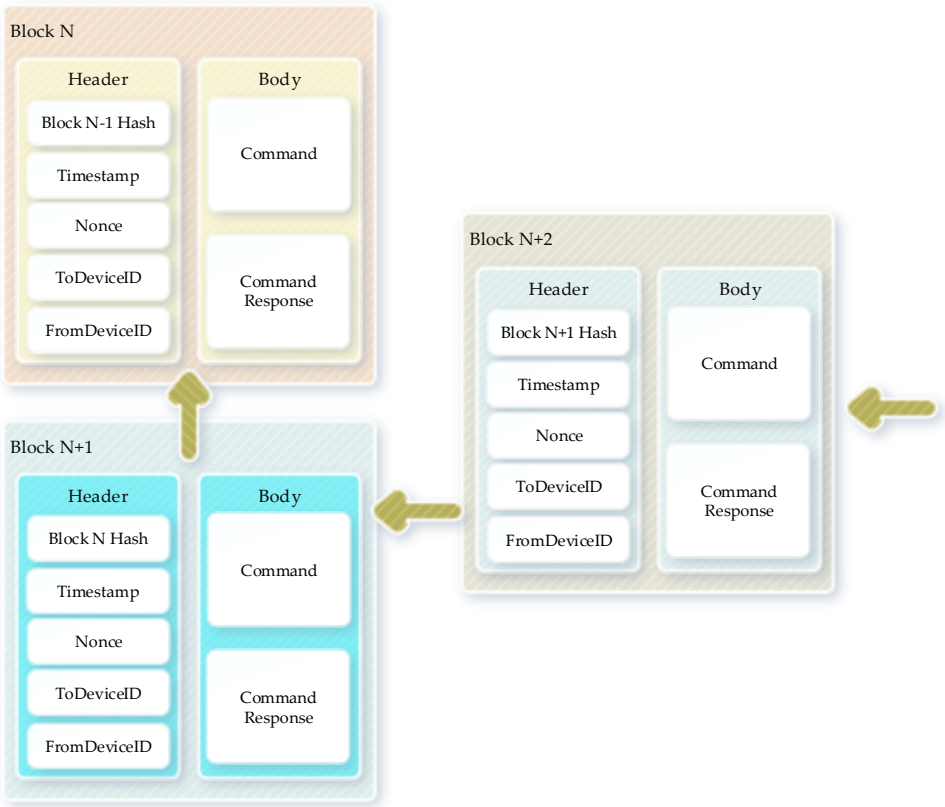


Figure 4. Block structure.

Figures 5 and 6 present the process of user authorization and verification request. The user authorization for the first step requires installing a smart application and generating the unique key for each user. Next is the registration of a unique key through Rest API, and, in terms of verification, it is possible to register the client in the super-node and confirm the registration.

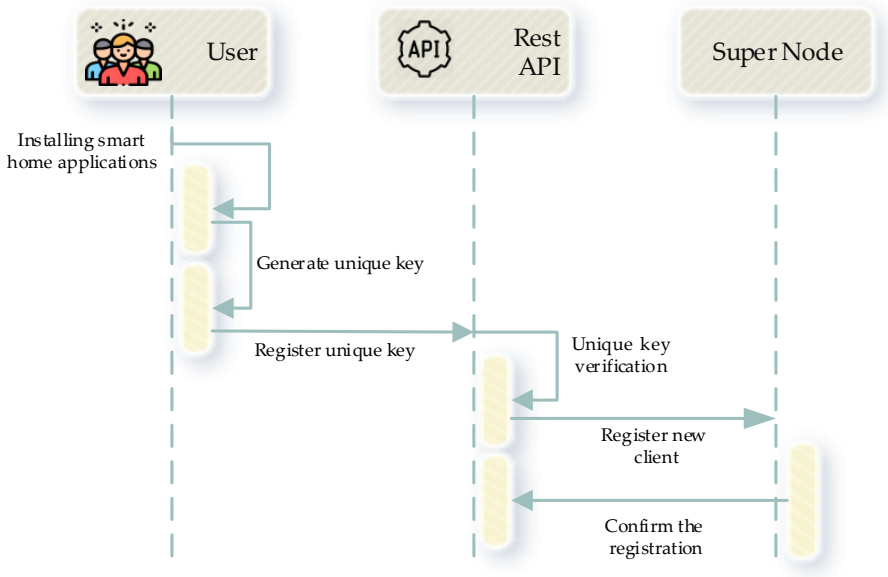


Figure 5. Process of user authorization.

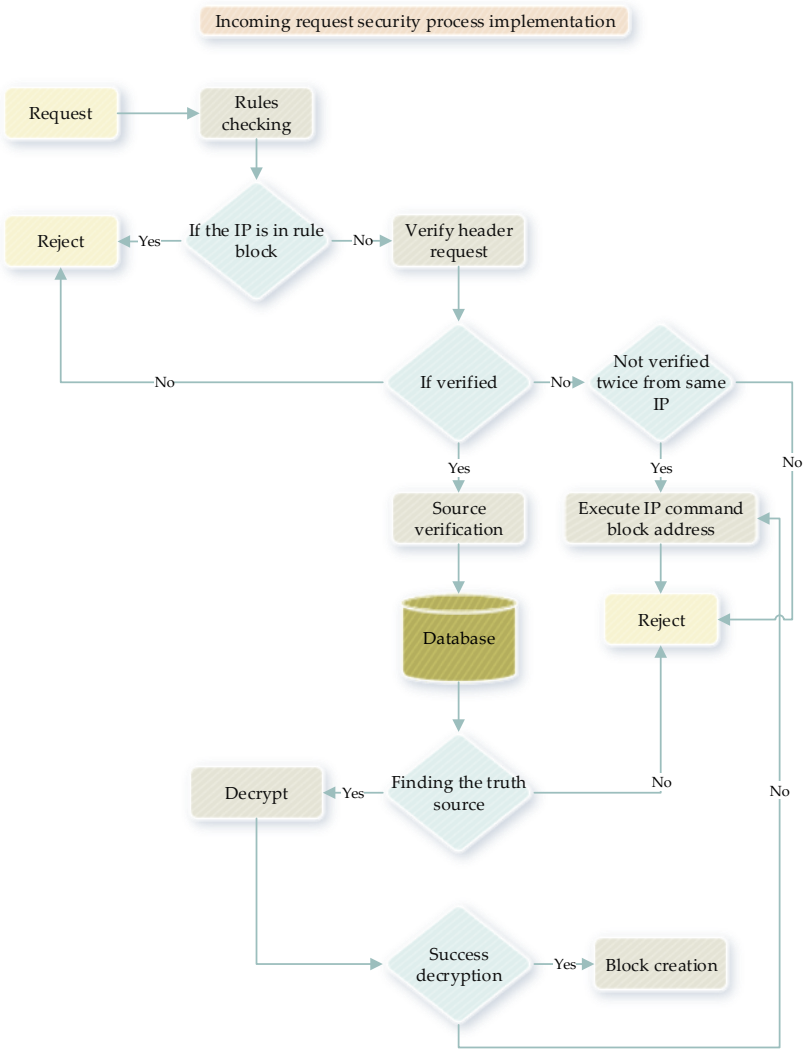


Figure 6. Process of verification request.

4. Results and Discussion

This section presents the experimental results and implementation of the smart home architecture based on DRL and blockchain.

4.1. Development Environment

Table 3 presents the implemented environment overview. The used memory in this system is 32 GB. The system processed CPU is Intel(R) Core(TM) i7-8700@3.20 GHz. The programming language for machine learning algorithm implementation is 3.6.2. The presented blockchain framework is Ethereum. The applied machine learning algorithm is deep reinforcement learning.

Table 3. Development environment of the proposed system.

Component	Description
Memory	32 GB
CPU	Intel(R) Core(TM) i7-8700@3.20 GHz
Python	3.6.2
Operating System	Ubuntu Linux 18.04.1 LTS
Docker Engine	Version 18.06.1-ce
Docker Composer	Version 1.13.0
Blockchain framework	Ethereum
Machine learning algorithm	Deep Reinforcement Learning

4.2. Data

The process data in this system collected from IoT sensors in a smart home. This process shows the data transformation from IoT sensors to the smart home gateway. The provided information is supplied in the data collecting layer as the input of the proposed system. The special data cleaning omitted the inconsistencies of knowledge. Figure 7 shows the gateway data management in the blockchain network. This process has three layers: data collecting layer, pre-processing data layer, and hashing layer. The data collection contains time setup, requesting the data, and storing data. The data pre-processing contains the filtering process, standardization, and classification. Finally, the hashing layer contains the encryption, hashing, and stored values. The generated data from the device contain the communication with the router at a special time. In case of the necessity of new data for a gateway, the stored raw data sent to the gateway. In the second layer, for creating enough storage, only the information with the device ID is storing based on the standardization and classification. Finally, the generated data in the smart home contain the important information from the users secured by encryption and require a password from the user and store in the hash function.

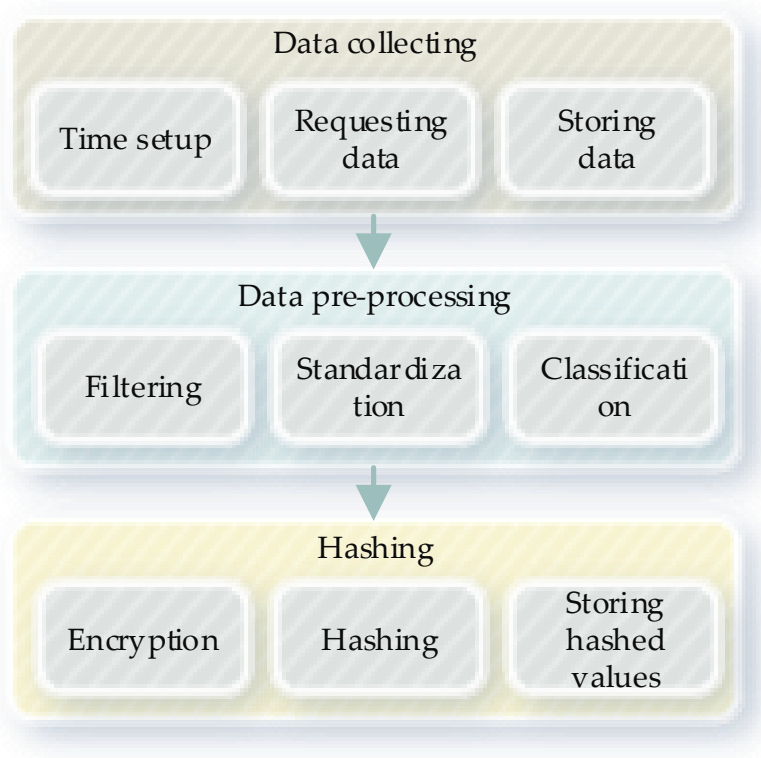
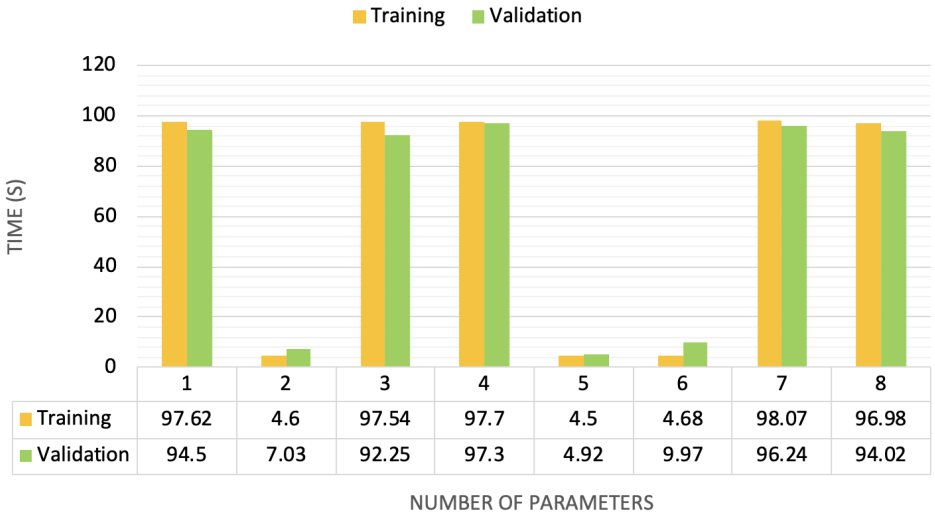


Figure 7. Gateway data management based on blockchain framework.

4.3. Blockchain Framework Performance in Smart Homes

In this section, the proposed architecture implementation is presented to validate the performance of the system. Figure 8 shows the various statistical parameters for smart home optimization in terms of security for training and validation. There are eight parameters discussed in Figure 8. One is accuracy, two is missing rate, three is sensitivity, four is specificity, five is false positive value, six is positive predictive value, and eight is negative prediction value.



	1	2	3	4	5	6	7	8
Training	97.62	4.6	97.54	97.7	4.5	4.68	98.07	96.98
Validation	94.5	7.03	92.25	97.3	4.92	9.97	96.24	94.02

Figure 8. Performance evaluation DRL and blockchain in smart home architecture.

Table 4 shows a blockchain-based smart home based on a DLR prediction set. There is a total of 150,317 records processed in the training set. These records are divided into two

categories of normal and attack samples. The normal records are 79,465, and attack records are 70,852. In addition, 3531 records are the invalid predicted records, and 67,321 are the correct predicted records.

Table 4. Blockchain-based smart home using a DRL training set records during prediction.

DRL Model (80% Training Data)		
Sample (M = 150.317)		**Output (Y0, Y1)**
Expected output (X0,X1)	Normal (Y0)	Attack (Y1)
X0 = 79.465 Normal	76.477	2.988
X1 = 70.852 Attack	3.531	67.321
Decision Tree		
X0 = 63.586 Normal	59.521	4.065
X1 = 86.731 Attack	2.320	84.411
ANN		
X0 = 60.719 Normal	57.430	3.289
X1 = 89.598 Attack	2.060	87.538
SVM		
X0 = 58.952 Normal	54.211	4.741
X1 = 91.365 Attack	1.742	89.623

4.4. Deep Reinforcement Learning Performance in Smart Homes

The performance evaluation of the DRL is based on Q-learning. The value function is defined in Equation (3):

$$Q_{e,c,w} \approx Q_{\pi}(e, c). \tag{3}$$

Based on the following Equation (3), the w parameter is defined as (4):

$$J(w) = B[(R_{t+1} + maxQ(e_{t+1}, \bar{c}; \hat{w}) - Q(e_t, c_t; w))^2] \tag{4}$$

Table 5 shows the validation records of the presented system. There are in total 33,886 validation samples, which are divided into 10,931 normal and 22,955 attack records. The observed 10,348 records are considered as normal and 583 records as the wrong prediction while there is no actual attack. Furthermore, 22,046 records show the correct prediction samples, and 909 show the invalidated records.

Table 5. Blockchain-based smart home using DRL training set records during validation.

DRL Model (20% Validation Data)		
Sample (M = 33.886)		**Output (Y0, Y1)**
Expected output (X0,X1)	Normal (Y0)	Attack (Y1)
X0 = 10.931 Normal	10.348	583
X1 = 22.955 Attack	909	22.046
Decision Tree		
X0 = 9.820 Normal	9.126	694
X1 = 24.066 Attack	1.020	23.046
ANN		
X0 = 8.719 Normal	7.920	799
X1 = 25.167 Attack	1.560	23.607
SVM		
X0 = 8.210 Normal	7.711	499
X1 = 25.676 Attack	1.626	24.050

Figure 9 shows the capability of DRL algorithms according to the taken actions. The process is in one hour, and it shows that the DRL optimization range from 2 to 10 in the morning and from 5 to 9 in the afternoon is high.

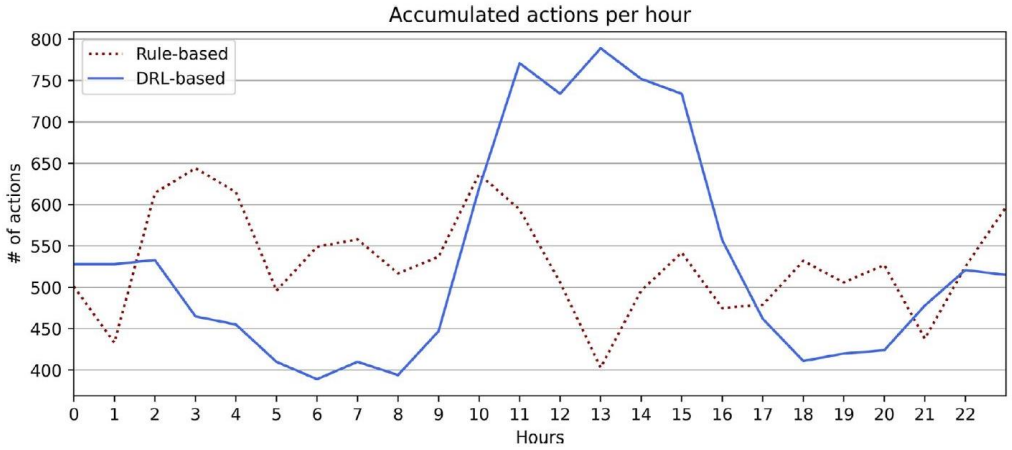


Figure 9. DRL action distribution in smart home architecture.

Table 6 shows the comparison of the performance of the proposed system with other state-of-the-art. Artificial Neural Network (ANN), in the second stage after DRL with an accuracy of 80.05, performs better in the provided data type. NSL-KDD and KDD-CUP-99 are two types of datasets that we used to process the proposed system.

Table 6. DRL comparison with other machine learning algorithms.

Algorithm	**NSL-KDD**	**KDD-CUP-99**
Decision tree	79.04	81.15
ANN	80.05	89.40
SVM	70.60	90.85
DRL	96.92	97.04

Figure 10 presents the performance evaluation of the smart home based on various machine learning algorithms due to predicted results in terms of false positive value, false negative value, positive prediction value, and negative prediction value.

Figures 11 and 12 show the response time and accuracy records in terms of security measures of data traffic quantity. It is clear that the gateway layer contains the faster response and similarly has the higher security measurement. The presented process based on blockchain employs security, authentication, confidentiality, and integrity to the smart home.

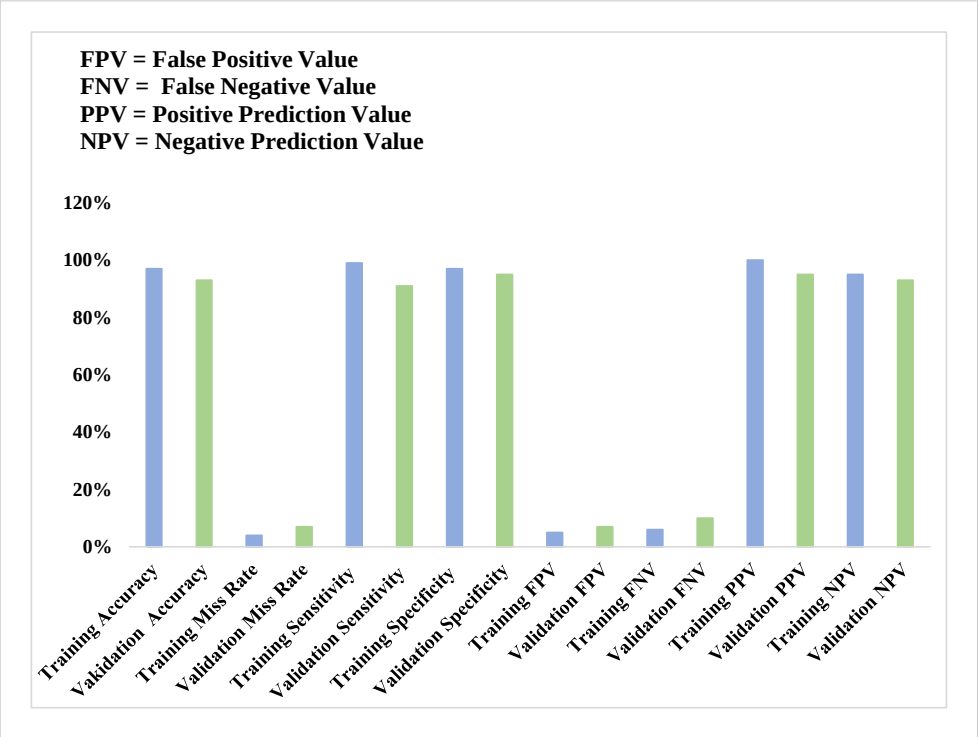


Figure 10. Performance evaluation of prediction comparison in proposed algorithms.

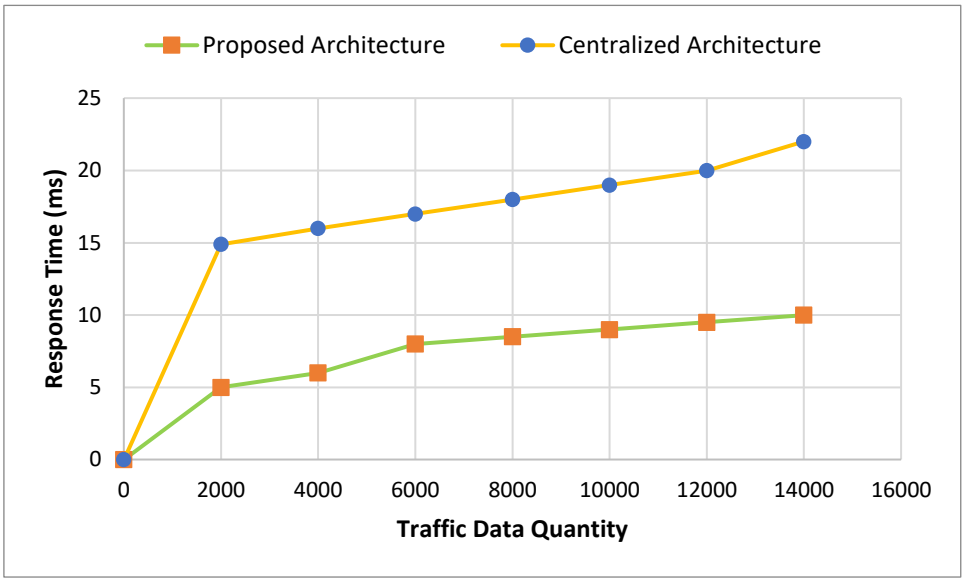


Figure 11. Response time measurement security in data traffic quantity.

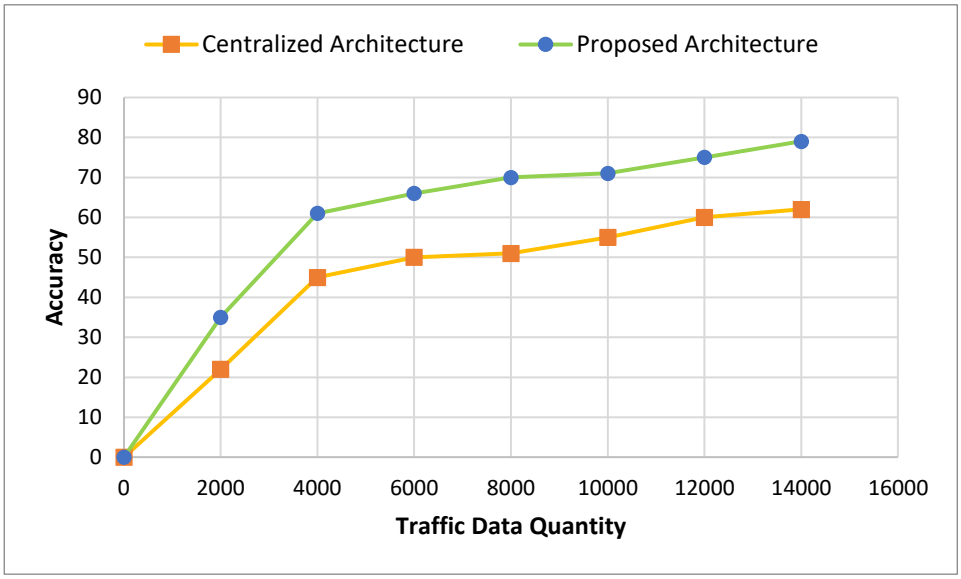


Figure 12. Accuracy measurement of security in data traffic quantity.

We designed the broadcast and block using ESP32 device to test proposed architecture. According to the process, SN has the possibility of creating the broadcast and block for verification of transaction. Figure 13 shows the mined two blocks. The selected green parts present the block one and two start times and the selected yellow parts show the block one and two completion times. The mining time of block has the possibility of human-readable time.

Figure 13. Result of block mining in Espruino view.

The difficulty target in this system is used to control the working phase of machines for new block generation. During the time limitation, if a new block is created, then the difficulty requires an adequate amount of time—in the same way, changing the difficulty and mining time which is run by code that are summarized in Table 7. Table shows the difficulty and mining time differences for block one. The actual difficulty is one and possible delay time is 0.22 for each block from difficulty two, and Figure 14 presents the time taken for the transaction and the difficulty within the processing time. Based on the figure, at difficulty four, it takes 60 s to consume. The main reason for evaluation of the difficulty and time together is to show the records of difficulty in terms of time per second.

Table 7. Differences between block one mining time and difficulty.

Difficulty	Mining Time (S)
1	0.5
2	0.22
3	0.3
4	60

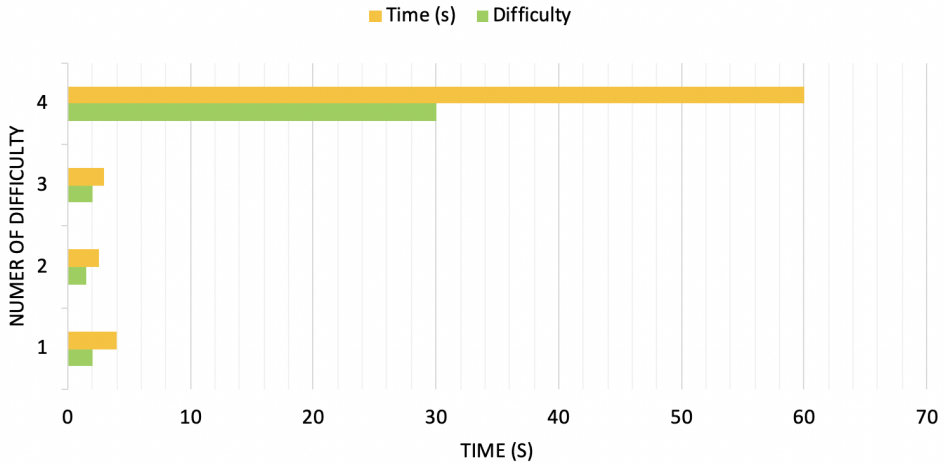


Figure 14. Difficulty level of time taken for transaction.

5. Conclusions

A smart home is one of the recent technologies in the IoT and sensors framework. Interference and identification of smart homes are huge challenges in predicting and evaluating which blockchain and machine learning have great potential to achieve this objective. The limitation of power and processing in smart home deployment can not easily be applied in this system. Therefore, we have presented the Deep Reinforcement Learning integration with blockchain to minimize the authentication, confidentiality, and integrity problem of the smart home's contradictory IoT and centralized gateway. This article proposed the existing works for smart home security and a simple model for the security architecture of a blockchain. The user's performance in the blockchain framework as a node was eliminated, but, as an alternative, the IoT devices made the system unique.

Author Contributions: Data curation, Z.S.; funding acquisition, H.-Y.K.; investigation, Z.S.; methodology, Z.S.; project administration, H.-Y.K.; supervision, Y.-C.B.; writing—original draft, Y.-C.B.; validation, Z.S.; visualization, Z.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Alam, M.R.; St-Hilaire, M.; Kunz, T. Peer-to-peer energy trading among smart homes. *Appl. Energy* **2019**, *238*, 1434–1443. [CrossRef]
2. Rivera, J.; Meulen, R. *Competition Is Increasing to Be the IoT Gateway to the Connected Home*; Gartner. 2015; Available online: https://www.gartner.com/en/newsroom/press-releases/2015-08-06-gartner-says-competition-is-increasing-to-be-the-iot-gateway-to-the-connected-home (accessed on 6 August 2015).

3. Shouran, Z.; Ashari, A.; Priyambodo, T. Internet of things (IoT) of smart home: Privacy and security. *Int. J. Comput. Appl.* **2019**, *182*, 3–8. [CrossRef]
4. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
5. Sovacool, B.K.; Martiskainen, M.; Del Rio, D.D.F. Knowledge, energy sustainability, and vulnerability in the demographics of smart home technology diffusion. *Energy Policy* **2021**, *153*, 112196. [CrossRef]
6. Ullah, F.; Al-Turjman, F. A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. *Neural Comput. Appl.* **2021**, 1–22. [CrossRef]
7. Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.K.R. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 17–25. [CrossRef]
8. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. *Future Gener. Comput. Syst.* **2019**, *100*, 144–164. [CrossRef]
9. Woodier, J.R.; Zingerle, A. The internet and cybersecurity: Taking the virtual fight to cybercrime and cyberwarfare. In *Handbook of Terrorism and Counter Terrorism Post 9/11*; Edward Elgar Publishing. 2019. Available online: https://www.elgaronline.com/view/edcoll/9781786438010/9781786438010.00011.xml (accessed on 4 December 2019).
10. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: Challenges, issues and solutions at different IoT layers. *J. Supercomput.* **2021**, *1*, 37.
11. Tzezana, R. Scenarios for crime and terrorist attacks using the internet of things. *Eur. J. Future Res.* **2016**, *4*, 1–7. [CrossRef]
12. Li, T.; Xiao, Y.; Song, L. Integrating Future Smart Home Operation Platform With Demand Side Management via Deep Reinforcement Learning. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 921–933. [CrossRef]
13. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; IEEE: New York, NY, USA, 2017; pp. 1292–1297.
14. Abdullah, T.A.; Ali, W.; Malebary, S.; Ahmed, A.A. A review of cyber security challenges attacks and solutions for Internet of Things based smart home. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 139.
15. Verma, A.; Prakash, S.; Srivastava, V.; Kumar, A.; Mukhopadhyay, S.C. Sensing, controlling, and IoT infrastructure in smart building: A review. *IEEE Sens. J.* **2019**, *19*, 9036–9046. [CrossRef]
16. Brotsis, S.; Limniotis, K.; Bendiab, G.; Kolokotronis, N.; Shiaeles, S. On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Comput. Netw.* **2021**, *191*, 108005. [CrossRef]
17. Tao, M.; Zuo, J.; Liu, Z.; Castiglione, A.; Palmieri, F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Gener. Comput. Syst.* **2018**, *78*, 1040–1051. [CrossRef]
18. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors* **2018**, *18*, 2796. [CrossRef] [PubMed]
19. Kamran, M.; Khan, H.U.; Nisar, W.; Farooq, M.; Rehman, S.U. Blockchain and Internet of Things: A bibliometric study. *Comput. Electr. Eng.* **2020**, *81*, 106525. [CrossRef]
20. Özyılmaz, K.R.; Yurdakul, A. Iot Blockchain integration: A Security Perspective. In *Security Analytics for the Internet of Everything*; 2020; p. 29. Available online: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003010463-3/iot-blockchain-integration-kaz (accessed on 4 September 2021).
21. Baucas, M.J.; Gadsden, S.A.; Spachos, P. IoT-based Smart Home Device Monitor Using Private Blockchain Technology and Localization. *arXiv* **2021**, arXiv:2103.15896.
22. Spathoulas, G.; Negka, L.; Pandey, P.; Katsikas, S. Can Blockchain Technology Enhance Security and Privacy in the Internet of Things? In *Advances in Core Computer Science-Based Technologies*; Springer: Berlin, Germany, 2021; pp. 199–228.
23. Alam, S.R.; Jain, S.; Doriya, R. Security threats and solutions to IoT using Blockchain: A Review. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 25–27 May 2021; IEEE: New York, NY, USA, 2021; pp. 268–273.
24. Rathee, G.; Balasaraswathi, M.; Chandran, K.P.; Gupta, S.D.; Boopathi, C. A secure IoT sensors communication in industry 4.0 using blockchain technology. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 533–545. [CrossRef]
25. Shahbazi, Z.; Byun, Y.C. Improving the Product Recommendation System based-on Customer Interest for Online Shopping Using Deep Reinforcement Learning. *Soft Comput. Mach. Intell.* **2021**, *1*, 31–35.
26. Shahbazi, Z.; Byun, Y.C. Integration of Blockchain, IoT and Machine Learning for Multistage Quality Control and Enhancing Security in Smart Manufacturing. *Sensors* **2021**, *21*, 1467. [CrossRef] [PubMed]
27. Kumar, P.; Chouhan, L. A secure authentication scheme for IoT application in smart home. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 420–438. [CrossRef]
28. Alani, S.; Mahmood, S.N.; Attaallah, S.Z.; Mhmood, H.S.; Khudhur, Z.A.; Dhannoon, A.A. IoT based implemented comparison analysis of two well-known network platforms for smart home automation. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 442–450. [CrossRef]

29. Rastogi, R.; Jain, R.; Jain, P. IoT Applications in Smart Home Security: Addressing Safety and Security Threats. In *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*; IGI Global. 2021; pp. 251–277. Available online: https://www.igi-global.com/chapter/iot-applications-in-smart-home-security/266143 (accessed on 4 September 2021).
30. Reyes-Campos, J.; Alor-Hernández, G.; Machorro-Cano, I.; Olmedo-Aguirre, J.O.; Sánchez-Cervantes, J.L.; Rodríguez-Mazahua, L. Discovery of Resident Behavior Patterns Using Machine Learning Techniques and IoT Paradigm. *Mathematics* **2021**, *9*, 219. [CrossRef]
31. Jafari, S.; Shahbazi, Z.; Byun, Y.C. Improving the Performance of Single-Intersection Urban Traffic Networks Based on a Model Predictive Controller. *Sustainability* **2021**, *13*, 5630. [CrossRef]
32. Cvitić, I.; Peraković, D.; Periša, M.; Gupta, B. Ensemble machine learning approach for classification of IoT devices in smart home. *Int. J. Mach. Learn. Cybern.* **2021**, 1–24. [CrossRef]
33. Shahbazi, Z.; Byun, Y.C. A framework of vehicular security and demand service prediction based on data analysis integrated with blockchain approach. *Sensors* **2021**, *21*, 3314. [CrossRef]
34. Javed, A.R.; Fahad, L.G.; Farhan, A.A.; Abbas, S.; Srivastava, G.; Parizi, R.M.; Khan, M.S. Automated cognitive health assessment in smart homes using machine learning. *Sustain. Cities Soc.* **2021**, *65*, 102572. [CrossRef]
35. Kaya, M.M.; Taşkiran, Y.; Kanoğlu, A.; Demirtaş, A.; Zor, E.; Burçak, İ.; Nacak, M.C.; Akgül, F.T. Designing a Smart Home Management System with Artificial Intelligence & Machine Learning. 2021. Available online: https://www.researchgate.net/profile/Mehmet-Muecahit-Kaya/publication/349869633_Designing_a_Smart_Home_Management_System_with_Artificial_Intelligence_Machine_Learning/links/604506e392851c077f241fd2/Designing-a-Smart-Home-Management-System-with-Artificial-Intelligence-Machine-Learning.pdf (accessed on 7 March 2021).
36. Abbas, A.F.; Abdullah, M.Z. Design and Implementation of Tracking a user's Behavior in a Smart Home. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1094*, 012008. [CrossRef]
37. Elsayed, N.; Zaghloul, Z.S.; Azumah, S.W.; Li, C. Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model. *arXiv* **2021**, arXiv:2105.12096.
38. Bokka, R.; Sadasivam, T. Deep Learning Model for Detection of Attacks in the Internet of Things Based Smart Home Environment. In Proceedings of the International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, Hyderabad, India, 28–29 March 2021; Springer: Berlin, Germany, 2021; pp. 725–735.
39. Suman, S.; Etemad, A.; Rivest, F. Potential Impacts of Smart Homes on Human Behavior: A Reinforcement Learning Approach. *arXiv* **2021**, arXiv:2102.13307.
40. Shahbazi, Z.; Byun, Y.C. Smart Manufacturing Real-Time Analysis Based on Blockchain and Machine Learning Approaches. *Appl. Sci.* **2021**, *11*, 3535. [CrossRef]
41. Varshney, G.; Gupta, H. A security framework for IOT devices against wireless threats. In Proceedings of the 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, India, 10–11 August 2017; IEEE: New York, NY, USA, 2017; pp. 1–6.
42. Lazaroiu, C.; Roscia, M. Smart district through IoT and blockchain. In Proceedings of the 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), San Diego, CA, USA, 5–8 November 2017; IEEE: New York, NY, USA, 2017; pp. 454–461.
43. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Jindal, A.; Dua, A.; Kumar, N. Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem. In Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities, 2018; pp. 1–6. Available online: https://dl.acm.org/doi/abs/10.1145/3214701.3214704 (accessed on 25 June 2018).
44. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, Big Island, HI, USA, 13–17 March 2017; IEEE: New York, NY, USA, 2017; pp. 618–623.
45. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
46. Zhou, Y.; Han, M.; Liu, L.; Wang, Y.; Liang, Y.; Tian, L. Improving iot services in smart-home using blockchain smart contract. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: New York, NY, USA, 2018; pp. 81–87.
47. Jamil, F.; Kim, D. Enhanced Kalman filter algorithm using fuzzy inference for improving position estimation in indoor navigation. *J. Intell. Fuzzy Syst.* **2021**, *40*, 8991–9005. [CrossRef]
48. Jamil, F.; Cheikhrouhou, O.; Jamil, H.; Koubaa, A.; Derhab, A.; Ferrag, M.A. PetroBlock: A blockchain-based payment mechanism for fueling smart vehicles. *Appl. Sci.* **2021**, *11*, 3055. [CrossRef]
49. Chandramohan, J.; Nagarajan, R.; Satheeshkumar, K.; Ajithkumar, N.; Gopinath, P.; Ranjithkumar, S. Intelligent smart home automation and security system using Arduino and Wi-fi. *Int. J. Eng. Comput. Sci. (IJECS)* **2017**, *6*, 20694–20698.
50. Lin, H.; Bergmann, N.W. IoT privacy and security challenges for smart home environments. *Information* **2016**, *7*, 44. [CrossRef]

51. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015; IEEE: New York, NY, USA, 2015; pp. 163–167.
52. Jamil, F.; Iqbal, N.; Ahmad, S.; Kim, D. Peer-to-Peer Energy Trading Mechanism based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid. *IEEE Access* **2021**, *9*, 39193–39217. [CrossRef]
53. Han, D.; Kim, H.; Jang, J. Blockchain based smart door lock system. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 18–20 October 2017; IEEE: New York, NY, USA, 2017; pp. 1165–1167.
54. Xu, Q.; He, Z.; Li, Z.; Xiao, M. Building an ethereum-based decentralized smart home system. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; IEEE: New York, NY, USA, 2018; pp. 1004–1009.
55. Singh, S.; Ra, I.H.; Meng, W.; Kaur, M.; Cho, G.H. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719844159. [CrossRef]
56. Mohanty, S.N.; Ramya, K.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.; Khanna, A. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Gener. Comput. Syst.* **2020**, *102*, 1027–1037. [CrossRef]
57. Lee, Y.; Rathore, S.; Park, J.H.; Park, J.H. A blockchain-based smart home gateway architecture for preventing data forgery. *Hum. Centric Comput. Inf. Sci.* **2020**, *10*, 1–14. [CrossRef]
58. She, W.; Gu, Z.H.; Lyu, X.K.; Liu, Q.; Tian, Z.; Liu, W. Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. *IEEE Access* **2019**, *7*, 62058–62070. [CrossRef]
59. Chen, Y.; Norford, L.K.; Samuelson, H.W.; Malkawi, A. Optimal control of HVAC and window systems for natural ventilation through reinforcement learning. *Energy Build.* **2018**, *169*, 195–205. [CrossRef]
60. Wei, T.; Wang, Y.; Zhu, Q. Deep reinforcement learning for building HVAC control. In Proceedings of the 54th Annual Design Automation Conference 2017, Austin, TX USA, 18–22 June 2017; pp. 1–6.
61. Nagy, A.; Kazmi, H.; Cheaib, F.; Driesen, J. Deep reinforcement learning for optimal control of space heating. *arXiv* **2018**, arXiv:1805.03777.
62. Wang, Y.; Velswamy, K.; Huang, B. A long-short term memory recurrent neural network based reinforcement learning controller for office heating ventilation and air conditioning systems. *Processes* **2017**, *5*, 46. [CrossRef]
63. Gao, G.; Li, J.; Wen, Y. Energy-efficient thermal comfort control in smart buildings via deep reinforcement learning. *arXiv* **2019**, arXiv:1901.04693.