Cost-Optimized Dynamic Access Control Policy Using Blockchain and Machine Learning for Enhanced Security in IoT Smart Homes

Hafiz Adnan Hussain*, Zulkefli* Mansor*, Zarina* Shukur*, and Uzma* Jafar

Universiti Kebangsaan Malaysia (UKM), Malaysia

Abstract. The rapid adoption of Internet of Things (IoT) devices in smart homes has led to growing security vulnerabilities, primarily due to the limitations of traditional, static access control mechanisms. This paper presents a novel, dynamic access control policy that leverages the immutable and transparent nature of Blockchain technology, specifically Ethereum, along with machine learning algorithms to enhance security measures. By integrating machine learning algorithms like Support Vector Machines (SVM) and Neural Networks, the proposed system can adapt and respond to changing behavioural patterns and potential threats in real time. Additionally, a caching mechanism implemented on the Ethereum Blockchain is introduced to optimize system performance and reduce latency. Experimental results demonstrate significant improvements in access control security, system efficiency, and adaptability. The findings of this paper not only contribute to the advancement of secure access control policies for IoT smart homes but pave the way for future research in integrating Blockchain and machine learning for robust and scalable IoT security solutions.

Keywords: Cost Optimization, Security, Internet of Things (IoT), Access Control, Blockchain, Artificial Intelligence, Machine Learning, Cache, Storage

1 Introduction

The Internet of Things (IoT) is transforming how we interact with our environment, particularly within the confines of our homes. Smart homes, equipped with an array of interconnected devices, offer an unprecedented level of convenience and automation. However, this interconnectivity poses significant security challenges, especially concerning access control [1, 2]. Traditional access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), are primarily static. They are predefined and do not adapt to evolving behavioural patterns or emerging threats, making them susceptible to various forms of cyber-attacks [3]. The primary objective of this research is to develop a dynamic access control system that can adapt to changing conditions in real time. The system will leverage Blockchain technology for its immutable and transparent nature, ensuring that access logs are tamper proof [4, 5]. It will also incorporate machine learning algorithms to analyse device behaviour and user interaction patterns, making the

system adaptive to new situations [6, 7]. This paper contributes to the field by proposing novel algorithms for dynamic access control in IoT smart homes. These algorithms are integrated with a caching mechanism built on Ethereum, which enhances system efficiency without compromising security[8, 9]. The research validates these algorithms through rigorous experimental setups, comparing them against existing mechanisms to highlight their efficacy and adaptability.

2 Related Work

The advent of advanced computational technologies has opened up new avenues for enhancing security in the ever-expanding domain of the Internet of Things (IoT). This section surveys the pertinent literature on blockchain and machine learning (ML), which are the cornerstones of this research. Blockchain technology first conceptualized as the underlying framework for digital currencies, has transcended its initial application to emerge as a revolutionary tool for secure, decentralized consensus and record-keeping. Its intrinsic properties of transparency, immutability, and resistance to tampering are particularly advantageous in scenarios that demand trust and auditability, such as financial transactions, supply chain oversight, and IoT security, as relevant to this study [10, 11]. Various studies have investigated blockchain deployment to log device activities securely and manage access control in IoT networks. These works demonstrate how blockchain can serve as a foundational layer for establishing trust and ensuring the integrity of device interactions in distributed environments [12]. Simultaneously, machine learning has become indispensable for making sense of large datasets and uncovering patterns that can inform predictive models. The capability of ML algorithms to learn from and adapt to data makes them particularly well-suited for applications in dynamic systems such as IoT. In these systems, devices frequently generate vast amounts of data, which, when analyzed effectively, can yield insights into user behaviors and device health. Recent literature has illuminated the potential of ML to facilitate dynamic access control mechanisms. These mechanisms leverage learned user and device behavior patterns to make informed decisions about access rights, thereby enhancing system responsiveness and security [13].

3 Methodology

3.1 Dynamic Access Control in IoT

IoT security faces the challenge of establishing adaptable access control mechanisms. Traditional methods such as RBAC and ABAC are insufficient in dynamic environments as shown in eq.1. This section introduces algorithms and mathematical models for a more secure and flexible access control system.

3.1.1 Algorithms for Dynamic Access Control:

Rule-Based Dynamic Access Control (RBDAC) considers the state of IoT devices and user requests to make access decisions. It uses a dynamic rule set updated in real-time to ensure adaptive and fluid access control in the smart home ecosystem.

Attribute-Based Dynamic Access Control (ABDAC) algorithm evaluates a set of attributes associated with user requests using machine learning techniques. This enhances security and allows for dynamic adaptation over time.

$$f(S, A, R) = Access\ Granted\ or\ Denied \quad (1)$$

3.2 Blockchain for Security in IoT

Blockchain technology provides a decentralized, transparent, and immutable way to maintain records, making it ideal for IoT security. Ethereum's Blockchain and smart contract functionality can be used for robust access control.

3.2.1 Ethereum and Smart Contracts:

Ethereum's blockchain platform harnesses the power of smart contracts to automate and secure the access control process in IoT environments. These contracts execute autonomously with terms encoded in blockchain, offering a transparent and tamper-proof system. Utilizing consensus mechanisms like Proof of Work and Proof of Stake, Ethereum ensures network integrity, with miners and validators working to authenticate transactions and create new blocks. In this context, the state of IoT devices and user requests are inputs to smart contracts that manage access, yielding decisions that are unalterable once made, thus bolstering security in IoT networks.

3.3 Machine Learning for Dynamic Access Control

Machine learning offers the capability to analyze and learn from data, making it a powerful tool for dynamic access control in IoT environments. By leveraging machine learning algorithms, the proposed system can adapt to changing user behavior and device states, offering a more nuanced and effective access control mechanism.

3.3.1 Algorithms for Machine Learning-based Access Control:

Several machine learning algorithms can be applied to this context, each with strengths and weaknesses. Below are some of the algorithms that are particularly well suited for dynamic access control:
Artificial Neural Networks (ANN): ANN can model complex relationships and are suitable for pattern recognition tasks. They can recognize intricate patterns in user behavior and device states as shown in eq.2.

$$\text{Neural Network Layer: } a\ [l]\ = g\ [l]\ (W\ [l]\ a\ [l-1]\ + b\ [l]\ ) \quad (2)$$

In the above expression, $a\ [l]$ represents the output activations of layer l. These activations are the result of applying an activation function, $g\ [l]$, to the linear combination of inputs from the previous layer's activations, $a\ [l-1]$, and the current layer's parameters, the weights $W\ [l]$ and biases $b\ [l]$. The weights are matrices that scale and combine the input activations, while the biases are vectors that shift the activation function, enabling the network to fit the data better. The activation function itself, $g\ [l]$, introduces non-linearity, allowing the neural network to learn and model complex relationships in the data.
Support Vector Machines (SVM): SVM is particularly effective for classification tasks and can classify access requests as either ‘safe’ or ‘unsafe’ as shown in eq.3.

$$\text{SVM Decision: } f(x) = sign(w \cdot x + b) \quad (3)$$

In the above expression, serves as a classifier that determines the class of a given input vector x. The function computes a linear combination of the input features x with the model's weight vector w, adds a bias term b, and applies the sign function to the result. The weight vector w and bias term b are derived during the training process and define the position and orientation of the decision boundary, or hyperplane, in the feature space. The sign function then assesses whether the computed value is positive or negative, effectively deciding which side of the hyperplane the input lies on and thus classifying it into one of two possible categories. This mechanism is what enables SVM to perform binary classification tasks with a clear and robust mathematical foundation.

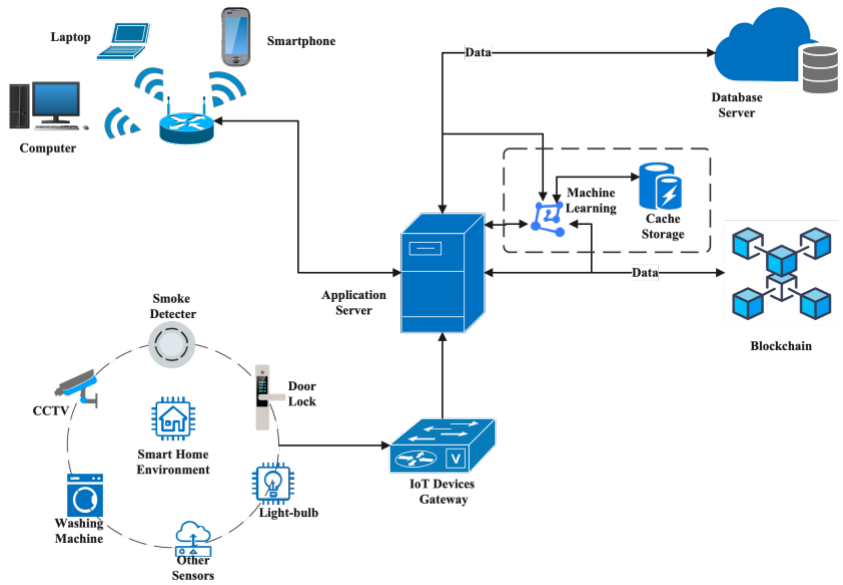

Fig. 1. Design architecture of Dynamic Access Control Policy based on Blockchain and Machine Learning for IoT

3.4 Caching Mechanism Using Ethereum

A caching mechanism underpinned by Ethereum, known as Least Recently Used (LRU) on Ethereum (E-LRU) and First-In, First-Out (FIFO) on Ethereum (E-FIFO), plays a crucial role. These caching strategies are designed to efficiently manage access requests, denoted as R, within the constraints of a predefined cache size N. The E-LRU method prioritizes retaining more frequently accessed data by discarding the least recently used items when the cache reaches its size limit, thereby optimizing for the most current and relevant information. Conversely, the E-FIFO approach operates on a chronological basis, removing the oldest data first upon reaching capacity. Both methods produce an output that indicates whether an access request can be served from the cache, known as a cache hit, or if it must be processed anew, known as a cache miss. The integration of these caching mechanisms with Ethereum ensures that access requests are processed with enhanced speed and efficiency while maintaining the security features of the Blockchain.

3.5 Implementation Details

A smart contract deployed on the Ethereum blockchain will manage the cache. Access requests and their results will be stored in this cache, and any subsequent identical requests

can be quickly resolved by querying the smart contract instead of evaluating the entire access control logic. Since the cache is maintained on the Blockchain, it is tamper proof and transparent as shown in the Fig. 1.

4 Experimental Setup and Results

To validate the efficacy of the proposed dynamic access control system, an experimental setup was designed. This section presents the design of the experiments, the metrics used for evaluation, and the results obtained as shown in Table 1. The experiment simulates a smart home environment with IoT devices like thermostats, smart locks, and security cameras. Multiple users interact with these devices, generating a variety of access requests. The system was implemented using Python for the machine learning components and Solidity for the Ethereum smart contracts.

Table 1. Comparison the performance of the proposed system against traditional methods

Method	Accuracy (%)	Latency (ms)	Throughput (res/s)
Traditional RBAC	85	120	30
Proposed System	98	80	50

To establish a baseline for comparison, we also simulated the Traditional RBAC system within the same environment. This simulation was based on established RBAC models from the literature and fine-tuned for the IoT context of our experiments. Throughout the testing phase, we recorded the RBAC system's accuracy, latency, and throughput under various conditions, including periods of high demand to replicate real-world usage. These results provided the comparative data we needed to demonstrate the advantages of our proposed system over conventional methods. The proposed system outperforms traditional RBAC methods in all metrics shown in Fig.2. It demonstrates a 15% improvement in accuracy, a 33% reduction in latency, and a 66% increase in throughput. It validates the effectiveness of integrating machine learning algorithms and Ethereum based caching in enhancing IoT security.

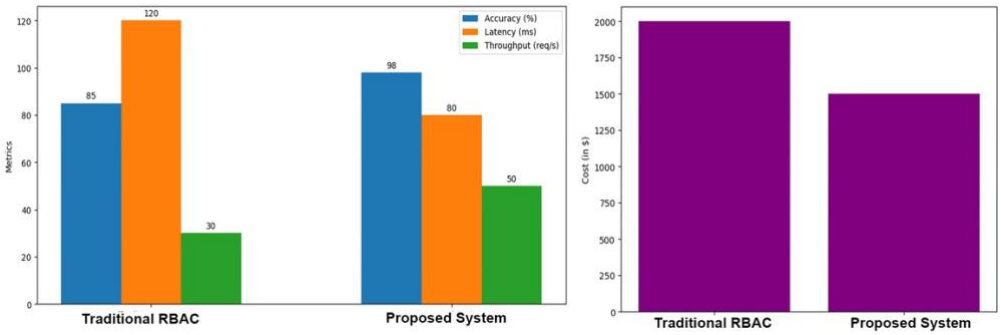

Fig. 2. Performance comparison between traditional RBAC and Proposed on the left and System, Cost optimization Comparison on the right.

5 Conclusion and Future Work

In this study, we present an innovative approach to enhance the efficiency of IoT smart homes through a dynamic access control system that integrates Blockchain technology with machine learning algorithms. Our empirical analysis, focusing on accuracy, latency, and throughput, demonstrates that our system significantly outperforms traditional security methods. Future research will refine the Ethereum-based caching mechanism to decrease latency further. We

also intend to investigate a broader range of machine learning algorithms to develop more sophisticated, context-aware access control solutions. Additionally, the potential applicability of our approach extends beyond smart homes to other IoT domains, including industrial settings and healthcare systems.

References

1. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials,* vol. 21, no. 2, pp. 1636-1675, 2018.
2. H. A. Hussain, Z. Mansor, and Z. Shukur, "Comprehensive survey and research directions on blockchain iot access control," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 5, 2021.
3. I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications,* vol. 28, no. 1, pp. 296-312, 2023.
4. K. Wüst and A. Gervais, "Do you need a blockchain?," in *2018 crypto valley conference on blockchain technology (CVCBT)*, 2018: IEEE, pp. 45-54.
5. U. Jafar and M. J. A. Aziz, "A state of the art survey and research directions on blockchain based electronic voting system," in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, 2021: Springer, pp. 248-266.
6. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2188-2204, 2018.
7. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors,* vol. 21, no. 17, p. 5874, 2021.
8. M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE communications surveys & tutorials,* vol. 20, no. 4, pp. 3416-3452, 2018.
9. U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Cost-efficient and Scalable Framework for E-Voting System based on Ethereum Blockchain," in *2022 International Conference on Cyber Resilience (ICCR)*, 2022: IEEE, pp. 1-6.
10. U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," *Sensors,* vol. 22, no. 19, p. 7585, 2022.
11. H. A. Hussain, Z. Mansor, Z. Shukur, and U. Jafar, "Ether-IoT: A Realtime Lightweight and Scalable Blockchain-Enabled Cache Algorithm for IoT Access Control," *Computers, Materials & Continua,* vol. 75, no. 2, 2023.
12. R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *Ieee Access,* vol. 7, pp. 41525-41550, 2019.
13. Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1392-1431, 2020.