UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Enhancing Smart Home Security Using Adaptive Access Control with Blockchain and Machine Learning

Atikah Balqis Basri[1], Mohd Izzuddin Mohd Tamrin[2], Mohd Khairul Azmi Hassan[3], Muhammad Fahmi Mohamad[4], Amir 'Aatieff Amir Hussin[5], Muhammad Ammar Amsyar Mohd Azhar[6], Ahmad Anwar Zainuddin[6]* & Muhammad Aqil Hakimi Abdullah[7]
Department of Computer Science
International Islamic University Malaysia
Kuala Lumpur, Malaysia
Email: atikahbalqis@iium.edu.my[1]; izzuddin@iium.edu.my[2]; mkazmi@iium.edu.my[3]; mkazmi@iium.edu.my[4]; amiraatieff@iium.edu.my[5]; amsyarammar05@gmail.com[6]; anwarzain@iium.edu.my[6]; hakimiaqil014@gmail.com[7]

Submitted: 15/9/2025. Revised edition: 28/11/2025. Accepted: 5/1/2026. Published online: 28/7/2026
DOI: https://doi.org/10.11113/ijic.v16n1-2.697

***Abstract*—Smart homes, equipped with interconnected IoT devices such as locks, cameras, and sensors, face critical security challenges due to the limitations of static access control mechanisms like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which lack adaptability to dynamic, multi-user environments and evolving threats. To address this problem, this research introduces a hybrid Blockchain–Machine Learning (ML) framework that ensures secure, adaptive, and context-aware access control for smart home ecosystems. The proposed system integrates IoT devices with ML algorithms, including Support Vector Machines (SVM) and Neural Networks, to predict user behaviours and dynamically adjust access permissions in real time, while Blockchain ensures immutable, decentralized, and tamper-proof logging of access events. The methodology employed a mixed approach, beginning with an extensive literature review to identify shortcomings in existing static models, followed by system design using smart contracts, caching strategies to reduce latency, and a user perception survey involving 25 participants to validate acceptance and usability. Results demonstrated high user trust and readiness to adopt the proposed system, with 96% of respondents favouring Blockchain-ML-enabled dynamic access control over conventional methods despite concerns about privacy risks, costs, and implementation complexity. This work contributes to society by offering a scalable and intelligent smart home security solution that enhances trust, improves user experience, and strengthens resilience against cyber threats, ultimately supporting safer and smarter living environments.**

***Keywords*—Smart Home Security, Blockchain, Machine Learning, IoT Security**

I. INTRODUCTION

Smart homes are becoming central to contemporary living, providing comfort and control through interconnected devices such as locks, lights, cameras, and sensors. However, with this convenience comes an important concern: how secure are these digital entry points into private life? [29]. Traditional protections, such as PIN codes and simple passwords, have become insufficient in addressing increasingly sophisticated threats [26]. As shown in Fig. 1: Smart Home Security Challenges, common issues such as inflexible policies and single points of failure reveal why households remain vulnerable to intrusion and data misuse. In this context, security is not only about preventing cyberattacks but also about maintaining trust in technologies that are shaping daily routines and family interactions [26, 29].

At the core of smart homes is the Internet of Things (IoT), where devices of varying complexity communicate across shared networks. While this interconnected system offers efficiency and convenience, it also introduces multiple points of vulnerability [13, 29]. A simple thermostat or door sensor, if unprotected, can serve as a gateway for attackers. Multiuser households further complicate the situation, as access needs often differ between family members, guests, and service

providers. Fig. 2: Smart Home Access Control Policies highlights how current approaches struggle in these dynamic environments. This indicates the need for security solutions that are flexible and context-aware, rather than rigid, uniform rules that cannot reflect real household needs [16, 26, 29].

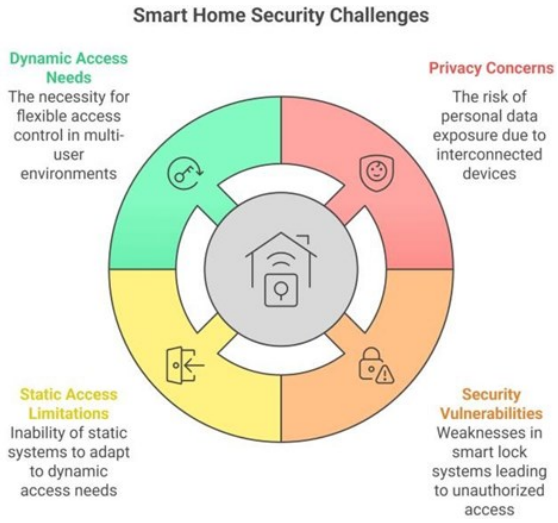


Fig. 1. Smart Home security challenges

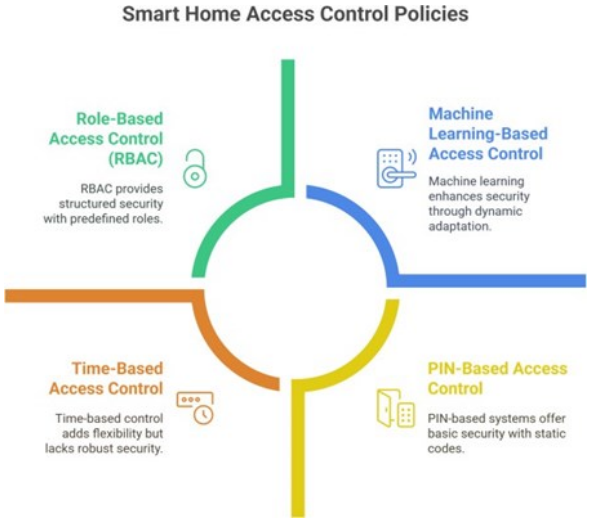


Fig. 2. Smart Home access control policies

Existing access control models, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), provide structured security but remain static [25]. These models freeze permissions at one point in time and fail to adjust when circumstances change. For example, providing temporary access to a guest or limiting a child's access to certain areas during specific times cannot be easily managed through static systems [15]. This rigidity creates opportunities for misuse and frustration among users. Dynamic access control offers an alternative by adapting rules in real time, considering contextual factors such as time, location, and behaviour [6]. Thereby balancing safety with everyday convenience.

Blockchain technology offers additional support by ensuring transparency and trust. Every access attempt can be recorded on an immutable ledger, making it impossible for malicious actors to alter or erase activity logs [2]. This is particularly useful in multi-user households, where disputes or misuse can be prevented by maintaining reliable records [8]. Moreover, smart contracts automate the enforcement of access policies, reducing reliance on centralized systems that may be compromised. In this way, blockchain embeds trust directly into the system design and reassures users that their security framework is reliable and tamper resistant [7, 11].

Machine learning (ML) further strengthens security by introducing adaptability and intelligence. By analyzing patterns of daily activity, ML can distinguish between legitimate access and potential threats, such as an intruder attempting entry [9, 22]. Algorithms such as Support Vector Machines (SVM) and Neural Networks enable the system to learn from past data and predict future needs, making access decisions more accurate and responsive [4, 18]. This not only improves safety but also reduces the need for constant manual management by users [28]. When integrated with blockchain, ML allows smart home systems to move from reactive to proactive security, creating an environment that is both secure and user-friendly.

This paper is organized as follows. Section I introduces background, motivation, and research objectives, with a focus on smart home security, IoT vulnerabilities, and the importance of dynamic access control. Section II reviews related literature on access control policies and the use of blockchain and ML in smart homes. Section III outlines the research methodology, including the literature review, system design, and a user perception survey. Section IV presents the results, including the proposed adaptive architecture and user feedback. Finally, Section V concludes the paper by summarizing contributions, highlighting challenges such as privacy and cost, and suggesting directions for future work in advancing secure and adaptive smart home systems.

II. LITERATURE REVIEWS

Several studies have explored access control mechanisms in smart homes, highlighting the limitations of static approaches and the potential of more adaptive models. [12] emphasizes that dynamic access control policies are particularly valuable in contexts where such mechanisms have not yet been implemented. The proposed system grants access rights based on user activity, context, and external conditions, while blockchain ensures that access logs remain tamper-resistant. The strength of this approach lies in its combination of machine learning, which enables adaptability, and blockchain, which ensures security, resulting in a flexible and secure solution for multiuser smart homes. However, the study acknowledges that the real-world scalability and deployment of such systems on a large scale remain uncertain.

An article by Touqeer *et al*. (2021) further reinforces this concern by arguing that static access control policies are insufficient to meet security needs across different IoT layers in smart homes. The study discusses challenges at the perception, network, and application layers, pointing out that more flexible models must be developed for complex multiuser environments. Its strength lies in offering a comprehensive overview of IoT security challenges, while its limitation is the

lack of a concrete solution for dynamic access control tailored specifically to smart homes.

In response to these limitations, Ameer *et al*. (2023) proposes a hybrid model that combines Attribute-Based Access Control (ABAC) with Role-Based Access Control (RBAC). This approach seeks to jointly incorporate user roles and attributes, preventing access control from becoming overly rigid. The hybrid design offers more flexibility compared to purely static models based on roles alone. Nevertheless, the proposed model has so far only been validated in theoretical contexts, with few real-world applications to demonstrate its practical effectiveness.

Similarly, Bhatt *et al*. (2021) focuses on the potential of ABAC as a solution to improve adaptability in IoT systems, particularly smart homes. The authors illustrate how ABAC can be applied on platforms such as AWS IoT, enabling policies to adjust dynamically according to user attributes like location and role. The key strength of ABAC lies in its ability to accommodate evolving security requirements using multiple attributes, rather than fixed roles. However, its implementation in smart homes must address challenges such as device compatibility and resource limitations, which could hinder large-scale adoption.

Finally, Hashmi *et al*. (2024) introduce the Smart Access Control and Authorization framework as a direct attempt to address the gaps in existing static systems. This framework allows access policies to change dynamically according to user roles, activities, and contextual factors. Designed specifically for multiuser smart home environments, Smart Access Control and Authorization framework is praised for its responsiveness to user needs. Still, its scalability and performance require further validation in larger infrastructures before it can be considered a fully reliable solution. Together, these studies demonstrate that while static access control policies have provided foundational security in smart homes, they are increasingly inadequate in the face of complex, dynamic, and multiuser environments. Hybrid models, ABAC-based approaches, and frameworks like Smart Access Control and Authorization framework represent important steps toward adaptable security, though their limitations underline the need for further development and large-scale validation of blockchain- and machine learning–enabled solutions. To address this shortfall, this study proposes a novel hybrid model that combines blockchain in order to provide immutable, secure access logging equipped with machine learning that enables context-aware dynamic access control. This integration, not fully explored in existing literature, forms the core innovation of the present work and aims to set a new standard for adaptive, trustworthy smart home security.

III. METHODOLOGY

This study employed a mixed-methods approach consisting of three main stages: a comprehensive literature review, the design of a proposed smart home dynamic access control system, and a user perception survey. The objective was to evaluate the weaknesses of static access control in IoT-based smart homes and to propose a blockchain–machine learning (ML) framework as a more adaptive and secure alternative.

The first stage involved an extensive literature review to assess the state of access control mechanisms in smart home IoT security. Research papers were retrieved from Google Scholar, IEEE Xplore, and SciSpace using keywords such as “smart home IoT security,” “static access control,” “machine learning in IoT,” and “blockchain in smart homes.” A total of 18 papers published between 2019 and 2024 were selected for analysis. Group members were assigned papers to summarize, followed by regular discussions to synthesize findings. This process emphasized the shortcomings of conventional Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) systems and evaluated the potential of advanced technologies such as blockchain and ML in addressing these limitations [1, 3, 5, 17, 24].

Based on the insights gained, a prototype of a dynamic access control system was designed. IoT devices such as smart locks, motion detectors, and surveillance cameras were incorporated to capture user activity data in real time. ML models, including Support Vector Machines (SVM) and Neural Networks, were applied to identify behavioral patterns and predict access requirements. Simultaneously, blockchain technology was implemented to ensure immutable and decentralized logging of access events. Smart contracts were utilized as autonomous agents to enforce policies automatically, reducing reliance on manual oversight. To enhance performance, caching strategies such as Enhanced Least Recently Used (E-LRU) and Enhanced First-In-First-Out (E-FIFO) were employed to reduce latency and improve decision responsiveness [10, 12, 14, 20,21]. The architecture of the proposed system is illustrated in Fig. 3, which presents the integration of IoT sensors, ML algorithms, and blockchain for adaptive access control in smart home environments.

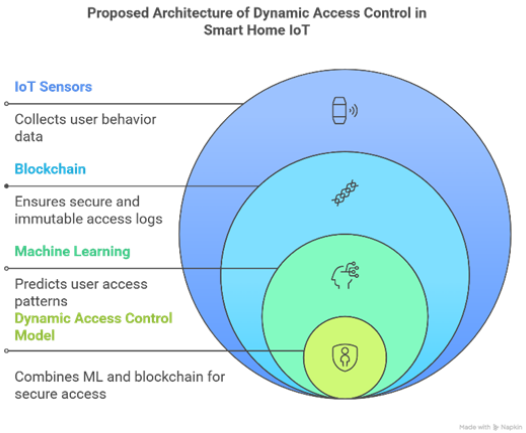


Fig. 3. Proposed Architecture of Dynamic Access Control in Smart Home IoT

The final stage involved a structured survey of 25 participants with varying levels of technical knowledge and experience in using smart home devices. The survey aimed to capture user awareness of smart home security, perceptions of traditional static access controls, and attitudes toward blockchain- and ML-driven adaptive security. Participants were also asked about concerns such as privacy, complexity of

implementation, and cost of adoption. Responses provided valuable insights that complemented the technical findings, confirming both the inadequacy of static systems and the potential acceptance of intelligent blockchain-ML solutions if concerns are properly addressed [30, 19, 21, 23, 27].

IV. Results and Discussion

The user perception survey provided meaningful insights into knowledge, experiences, and expectations regarding smart home IoT security. As shown in Fig. 4a, more than half of respondents (52%) reported having intermediate knowledge of IoT security, while 48% described themselves as beginners. This suggests that although smart home devices are becoming increasingly common, a significant portion of users remain unfamiliar with the underlying security challenges [19]. Figure 4b also highlights the growing adoption of IoT devices, with 72% of participants reporting active use of such technologies in their households. Despite this, user confidence in traditional access control mechanisms was mixed. As illustrated in Fig. 4c, 64% of respondents regarded static methods as only moderately effective, 24% considered them highly effective, and 12% saw them as minimally effective. These findings align with prior research that critiques the rigidity of static access control models in adapting to evolving threats [1, 17].

The perceived limitations of static systems were further reflected in Fig. 5d, where 56% of participants identified inflexibility against new threats as the primary weakness, followed by central points of failure (28%), latency in decision-making (12%), and lack of transparent access logs (8%). Such concerns mirror the technical vulnerabilities outlined in earlier studies on IoT security layers [1, 24]. Additionally, Figure 5e shows that 28% of respondents had personally experienced security breaches, such as unauthorized access, while 32% were unsure, reflecting the lack of real-time monitoring and feedback mechanisms noted in IoT environments. Awareness of emerging technologies was assessed in Fig. 5f. A large majority (80%) had some knowledge of blockchain and ML applications in IoT, 12% reported strong knowledge, and 8% had none. This demonstrates an openness to advanced technologies despite varied expertise. Importantly, Fig. 6g shows that 96% of participants trusted dynamic systems powered by blockchain and ML more than traditional static controls. Nonetheless, challenges were noted, including privacy risks (92%), implementation complexity (76%), blockchain transaction costs (64%), and concerns regarding algorithmic reliability (56%), consistent with the risks emphasized in prior literature [23, 27]. Figure 6h highlights user priorities for future smart home security systems. Real-time adaptability (88%) was identified as the most important feature, followed by low latency (84%), tamper-proof audit logs (80%), and ease of use (80%). Interestingly, 84% of respondents expressed willingness to pay more for solutions that integrate blockchain and ML, reinforcing the strong user demand for intelligent, trustworthy systems [21].

Finally, Figure 6i mentions that users overwhelmingly valued real-time adaptability (88%) as the most critical feature, followed closely by low latency (84%), tamper-proof audit logs (80%), and ease of use (80%). This shows that users are not only security-conscious but also emphasize usability and performance, aligning with findings that smart homes require both adaptive security and seamless user experiences [14, 21]. Finally, the data in Fig. 7j shows that 84% of respondents are willing to pay extra for advanced blockchain–ML-based security solutions, while only 16% were unwilling. This reflects strong market readiness and acceptance, consistent with prior studies that highlight user willingness to invest in enhanced privacy and reliability when trust and transparency are guaranteed [19, 23].

A. Dynamic Access Control Solution Proposed

The proposed solution directly addresses the limitations of static access control models by integrating blockchain and ML into a unified adaptive framework. Machine learning algorithms such as SVM and Neural Networks analyze real-time data from IoT sensors, enabling prediction of user behavior and dynamic adjustment of permissions. Meanwhile, blockchain ensures tamper-proof logging of every access event and employs smart contracts to autonomously enforce policies without human intervention. Figure 3 illustrates the architecture of the system, where IoT sensors such as door locks and cameras capture activity data, ML models analyze patterns, and blockchain validates and records access requests. This combination provides adaptability, accountability, and transparency. For example, time-based access rights can be automatically granted to family members, while temporary permissions can be assigned to guests. By combining contextual intelligence with immutable auditability, the system resolves many of the security gaps identified in static approaches.

B. Effectiveness and Usability Discussion

Survey findings support the effectiveness and acceptance of the proposed dynamic system. Respondents valued adaptability, responsiveness, and transparency, confirming that static systems are increasingly insufficient for modern multi-user households. The convergence of blockchain and ML was recognized by users as a practical advancement capable of offering higher security and reliability, aligning with previous studies advocating dynamic, trust-based approaches [3, 14]. Nonetheless, several challenges remain before widespread adoption is feasible. Concerns regarding privacy, implementation complexity, and operational costs were consistently highlighted, echoing earlier findings on IoT adoption barriers [19, 23]. To mitigate these, future development should prioritize user-friendly interfaces, optimization to reduce computational overhead, and transparent policies to ensure data privacy. Educational initiatives may also increase user confidence and trust in intelligent security systems. Overall, the results demonstrate that integrating blockchain and ML for adaptive access control significantly improves security in smart homes. By providing real-time adaptability, tamper-evident audit trails, and decentralized trust, the proposed framework offers a robust and user-centered model for protecting multi-user smart home environments.

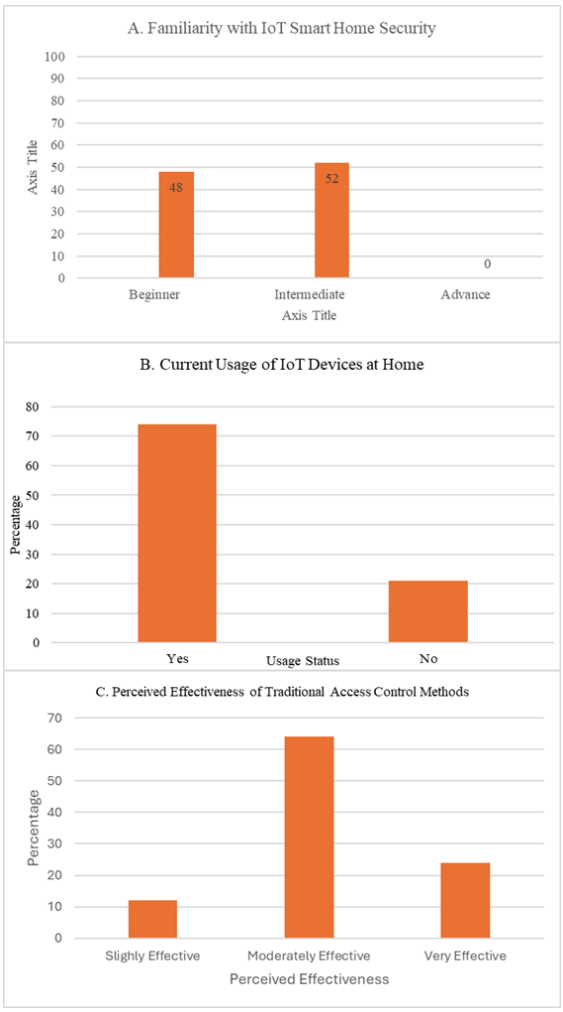
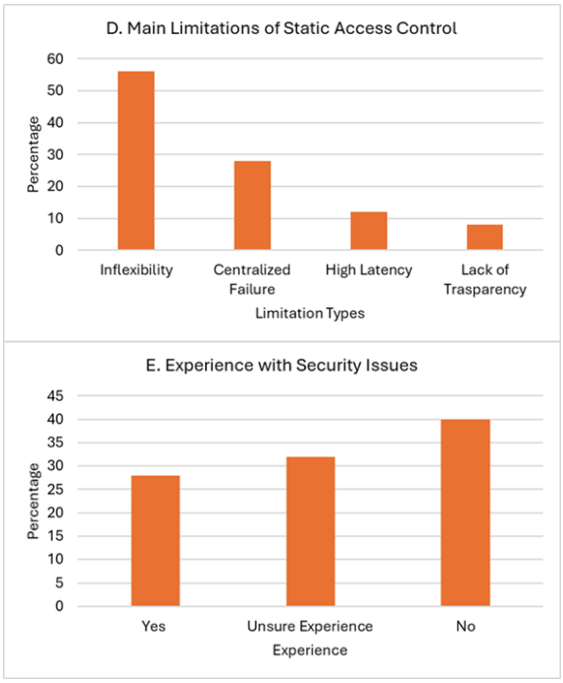


Fig. 4. (A-C) This Bar Chart Represent the Result from the Smart Home Iot Security-Limitations of Static Access Control Policies Survey



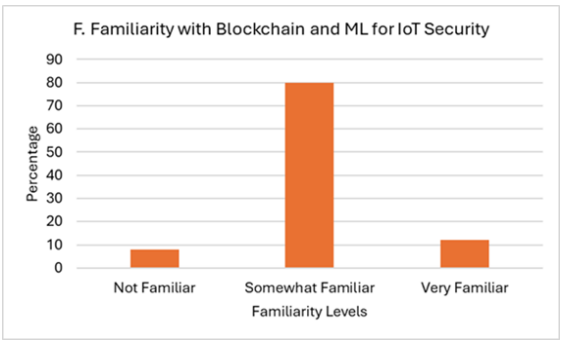


Fig. 5. (D-F) This Bar Chart Represent the Result from the Smart Home Iot Security-Limitations of Static Access Control Policies Survey

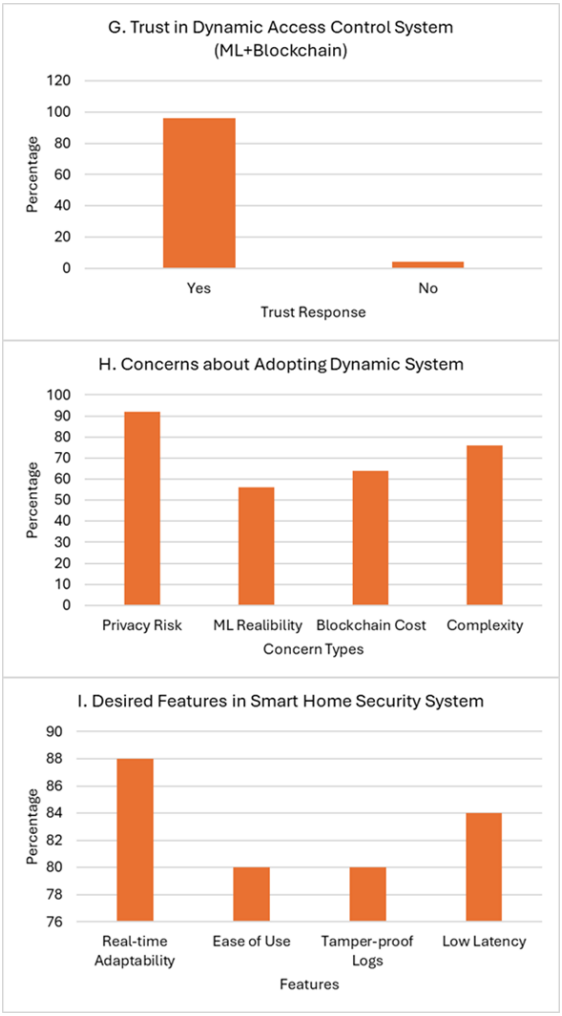


Fig. 6. (G-I) This Bar Chart Represent the Result from the Smart Home Iot Security-Limitations of Static Access Control Policies Survey

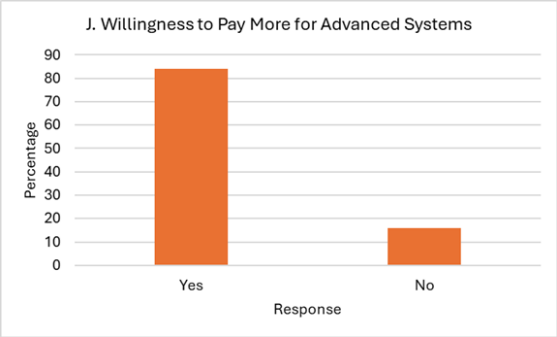


Fig. 7. (J) This Bar Chart Represent the Result from the Smart Home Iot Security-Limitations of Static Access Control Policies Survey

V. CONCLUSION

This study addressed the limitations of static access control in smart home IoT by proposing a dynamic framework that integrates blockchain and machine learning (ML). The literature review revealed that traditional Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models lack flexibility and scalability in multi-user environments. In contrast, blockchain provides transparency and tamper-proof logging, while ML enables adaptive, context-aware decision-making. Survey results confirmed that while smart home adoption is increasing, users remain concerned about the rigidity and vulnerabilities of static systems. Most respondents expressed trust in blockchain- and ML-based solutions, emphasizing features such as real-time adaptability, low latency, and auditability. However, issues of privacy, cost, and system complexity were also highlighted, underscoring the need for practical design considerations. The proposed architecture, illustrated in Fig. 3, demonstrates how IoT devices, ML algorithms, and blockchain can be integrated into a unified access control system. This hybrid approach enhances both security and user confidence by combining intelligent automation with decentralized trust. In conclusion, this work contributes to a robust model for securing multi-user smart homes. Future research should focus on reducing computational overhead, simplifying deployment, and strengthening privacy protections to support large-scale real-world adoption.

ACKNOWLEDGMENT

We would like to express our gratitude to all who have contributed to succeeding in this research. Special thanks to our instructor for the guidance along our journey in this research. Their unwavering commitment has greatly contributed to our advancement, enhancing our skills and deepening our understanding of enhancing network topologies, security challenges, and OSI model adaptation

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-security of embedded IoTs in smart homes: Challenges, requirements, countermeasures, and trends. *IEEE Open Journal of Vehicular Technology, 4*, 281–292.

[2] Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., & Yamin, M. (2021). Blockchain-based secured access control in an IoT system. *Applied Sciences, 11*(4), 1772.

[3] Ameer, S., Benson, J., & Sandhu, R. (2023). Hybrid approaches ABAC and RBAC toward secure access control in smart home IoT. *IEEE Transactions on Dependable and Secure Computing, 20*(5), 4032–4051.

[4] Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). A machine learning security framework for IoT systems. *IEEE Access, 8*, 114066–114077.

[5] Bhatt, S., Pham, T. K., Gupta, M., Benson, J., Park, J., & Sandhu, R. (2021). Attribute-based access control for AWS Internet of Things and secure industries of the future. *IEEE Access, 9*, 107200–107223.

[6] Boustia, N., & Mokhtari, A. (2012). A dynamic access control model. *Applied Intelligence, 36*(1), 190–207.

[7] Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access, 7*, 38431–38441.

[8] Di Francesco Maesa, D., Mori, P., & Ricci, L. (2017). Blockchain based access control. In L. Y. Chen & H. P. Reiser (Eds.), *Distributed Applications and Interoperable Systems* (Vol. 10320, pp. 206–220). Springer International Publishing.

[9] Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering, 28*(4), 2861–2879.

[10] Hashmi, I. F., Iqbal, Z., Munir, E., Kryvinska, N., Ivanochko, I., & Sampedro, G. A. (2024). SAAC secure access control management framework for multi-user smart home systems. *IEEE Access, 12*, 133339–133355.

[11] Houda, Z. A. E., Beaugeard, J., Sauvtre, Q., & Khoukhi, L. (2023). Towards a secure and scalable access control system using blockchain. In *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–8).

[12] Hussain, H. A., Mansor, Z., Shukur, Z., & Jafar, U. (2024). Cost-optimized dynamic access control policy using blockchain and machine learning for enhanced security in IoT smart homes. *ITM Web of Conferences, 63*, 01009.

[13] Alam, H., & Tomai, E. (2023). Security attacks and countermeasures in smart homes. *International Journal on Cybernetics & Informatics, 12*(2), 109–119.

[14] Lee, Y., Rathore, S., Park, J. H., & Park, J. H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. *Human-Centric Computing and Information Sciences, 10*(1), 9.

[15] Zhao, L., Liu, S., Li, J., & Xu, H. (2010). A dynamic access control model based on trust. In *2010 The 2nd Conference on Environmental Science and Information Application Technology* (pp. 548–551).

[16] Mahlous, A. R. (2023). Threat model and risk management for a smart home IoT system. *Informatica, 47*(1), 1–7.

[17] Mohammad, Z. N., Farha, F., Abuassba, A. O. M., Yang, S., & Zhou, F. (2021). Access control and authorization in smart homes: A survey. *Tsinghua Science and Technology, 26*(6), 906–917.

[18] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: A systematic review. *IEEE Access, 9*, 20717–20735.

[19] Nemec Zlatolas, L., Feher, N., & Hlbl, M. (2022). Security perception of IoT devices in smart homes. *Journal of Cybersecurity and Privacy, 2*(1), 65–73.

[20] Park, M., Oh, H., & Lee, K. (2019). Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors, 19*(9), 2148.

[21] Rajput, S., Talpur, N., Boudville, R., Abro, G. M. E., Talpur, B., & Zahid, F. (2024). Modernizing home protection: An IoT-driven approach with smart lock and Android application. In *2024 IEEE 14th International Conference on Control System, Computing and Engineering (ICCSCE)* (pp. 82–87).

[22] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access, 8*, 222310–222354.

[23] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191–1221.

[24] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: Challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing, 77*(12), 14053–14089.

[25] Uddin, M., Islam, S., & Al-Nemrat, A. (2019). A dynamic access control model using authorising workflow and task-role-based access control. *IEEE Access, 7*, 166676–166689.

[26] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. *Electronics, 13*(16), 3343.

[27] Vojković, G., Milenković, M., & Katulić, T. (2020). IoT and smart home data breach risks from the perspective of data protection and information security law. *Business Systems Research Journal, 11*(3), 167–185.

[28] Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express, 8*(3), 313–321.

[29] Yuan, B., Wan, J., Wu, Y.-H., Zou, D.-Q., & Jin, H. (2023). On the security of smart home systems: A survey. *Journal of Computer Science and Technology, 38*(2), 228–247.

[30] Ahmed, M. R., & Rahman, M. O. (2024). An enhanced secure user authentication and authorized scheme for smart home management. *International Journal of Advanced Computer Science and Applications, 15*(6), 58–67.