

# SecureHome-WiFi: A Blockchain-Enhanced Intrusion Prevention System for Securing Home Wireless Networks

Jaafar M. Salman<sup>1</sup> Davood Akbari-Bengar<sup>2</sup>

<sup>1</sup>Department of information technology, University of Islamic Azad Science and Research Branch, Tehran

<sup>2</sup>Department of information technology, University of Islamic Azad Computer Engineering, Iran

---

## Article Info

### Article history:

Received Sept.,15, 2025

Revised Oct., 20, 2025

Accepted Dec., 10, 2025

---

### Keywords:

Home Wireless Networks  
Cybersecurity,  
Blockchain,  
Intrusion Prevention,  
Wi-Fi Attacks,  
IoT Security,  
Real-time Monitoring

---

## ABSTRACT (10 PT)

With the significant increase and growing expansion in the use of smart devices within homes, home wireless networks have become more vulnerable to direct cyber-attacks such as unauthorized access attempts, identity theft, and brute force attacks against Wi-Fi protocols in general. Although standard and traditional security technologies such as WPA2/WPA3 encryption and MAC filtering provide a basic level of protection, they still suffer from security issues in the form of vulnerabilities that can be exploited and local log manipulation. To overcome these challenges, this research proposes a blockchain-based system to prevent intrusions into home wireless networks. The system relies primarily on real-time monitoring of traffic through the router to detect suspicious access attempts, using a special distributed ledger (blockchain) to store lists of trusted devices and security logs in a tamper-proof and forgery-proof manner. This system prevents unauthorized devices from joining the network and builds reliable audit logs of security events. This work highlights the potential for integrating blockchain technology with simple, low-cost security solutions to enhance the security of wireless networks in everyday environments.

---

## Corresponding Author:

Jaafar M. Salman

Department of information technology, University of Islamic Azad - Science and Research Branch, Tehran  
Hilla, Babylonian, Iraq

Email: it.jaafar93@gmail.com

---

## 1. INTRODUCTION

Home wireless networks become increasingly widespread in recent years as a result of the significant growth in the number of smart devices such as phones, all types of Internets of Things (IoT) devices, personal computers, and smart surveillance cameras. This significant expansion has made these networks one of the key components of the digital infrastructure in modern homes, but at the same time, it has opened the door to many growing cyber security threats such as brute force attacks on passwords, MAC spoofing attacks, and attacks against encryption protocols to reveal passwords such as WPA2 and WPA3 [1]. [2]. Although other common security protocols such as encryption and filtering provide a layer of protection, they are not sufficient to counter the rapid development of cyberattack methods and attackers, and the emergence of tools capable of bypassing them in a short period of time as a result of significant developments [3]. One of the most prominent challenges in home wireless networks is the inability of ordinary users to manage and protect their networks, as most of them are content with the default settings that come with the device configuration, making networks relatively easy to hack [4]. In addition, logs stored locally on routers can be manipulated or deleted by attackers once they gain access to them, making them unreliable and reducing their usefulness as a tool for tracking and analyzing attacks after they occur [5]. Blockchain technology also stands out in this context as an innovative solution that provides immutable and tamper-proof records and allows security events and trusted device lists to be stored in a distributed and fully secure manner [6]. Thanks to its decentralized and transparent characteristics, which ensure integrity, blockchain can form an additional layer of trust in home network

environments, whereby all login attempts or any suspicious activity are recorded permanently and cannot be manipulated or falsified [7]. On the other hand, intrusion prevention and mitigation systems are an effective mechanism not only for detecting attacks, but also for proactively preventing them before they occur, through various means such as blocking suspicious devices or preventing malicious traffic in real time [8]. However, the integration of multiple advanced intrusion prevention system technologies into home routers remains limited due to resource constraints and the need for simple and cost-effective solutions. Starting from these numerous challenges, this research proposes a home Wi-Fi protection system, which is a blockchain-enhanced protection system to protect and secure home wireless networks. The system relies primarily on integrating lightweight monitoring modules into the router (home router) to monitor unauthorized external access attempts, using a blockchain-based distributed ledger to store trusted devices that the user wants to access the routers and security events in a way that ensures integrity and prevents tampering or forgery. This research primarily seeks to bridge the gap between expensive or somewhat complex security solutions and the real-world need of ordinary users for a simple system that protects their home networks against growing cyber threats.

## 2. Related Work

Previous studies have shown considerable and growing interest in the field of wireless network protection, intrusion detection systems (IDS) and intrusion prevention. Much of the research has focused on improving security protocols such as WPA2 and WPA3 to counter a specific type of attack, namely password cracking and identity theft attacks. However, these solutions are still vulnerable to security loopholes that can be exploited by advanced attackers [9]. Numerous other studies have addressed the development of intrusion detection systems using artificial intelligence and machine learning techniques to monitor abnormal patterns in traffic when accessing or attempting to access routers, achieving ambitious results in terms of accuracy and detection capability. However, these systems often consume significant resources, making them unsuitable for application in simple multi-device home environments [10][11]. On the other hand, several studies have shown the potential for integrating blockchain technology with cybersecurity systems. It has been used to protect logs and make them tamper-proof in industrial environments such as smart grids or large-scale Internet of Things systems [12][13]. Many studies have also focused on how blockchain can provide a mechanism for distributing trust among multiple parties in sensitive networks, such as healthcare systems or public utilities [14]. However, the applicability of these technologies in home networking environments has remained limited, with most efforts focused heavily on large and complex sectors. In addition, most studies have focused on attack detection rather than prevention. In other words, the proposed systems were able to report attacks after they occurred, but were not always able to prevent them in real time when the breach occurred. This may leave the average user highly vulnerable to advanced threats, especially in a home environment that typically lacks technical expertise or professional protection tools [15].

### 2.1 Contribution

This research represents an advanced qualitative addition to the field of home wireless network security by proposing an effective, blockchain-enhanced protection system capable of combining detection and proactive response to attacks when they occur. Unlike previous studies, which focused heavily on detection alone or on institutional and industrial environments, this work targets the micro-home environment with its challenges, the most important of which are limited resources and users' lack of technical expertise. This research differs from previous studies in the following ways:

- Focus on home networks in particular: A system has been designed that is tailored to the limited capabilities of home routers in particular, unlike studies that have focused heavily on industrial or corporate networks.
- Integration of blockchain technology and intrusion prevention (IPS): Not limited to logging, it provides a proactive mechanism for real-time prevention of suspicious devices, working to prevent intrusion.
- Record security and whitelists: Blockchain technology has been used to store trusted devices and intrusion attempts in a tamper-proof and forgery-proof manner.
- Practical, effective and lightweight solution: Complexity has been reduced and reliance on mechanisms that can be implemented in a miniaturized home environment has been minimized.

### 3. Methodology

This section explains, in particular, the methodology adopted in the research to design and develop the proposed system. It explains the system architecture, the basic components on which the system is based, and the mechanism that integrates the various capabilities of the router in monitoring unauthorized access attempts and the special blockchain technology that helps to keep records and lists of trusted devices that cannot be tampered with or modified. This section also outlines a set of implementation steps and describes the experimental environment designed to evaluate the effectiveness of the existing system and assess its performance compared to other traditional solutions.

#### 3.1 System Design

The proposed system relies heavily on a three-layer architecture that is interconnected, aiming to achieve interconnection and integration between real-time monitoring of data traffic within the home wireless network, and distributed storage that cannot be manipulated or falsified by blockchain, and how to prevent intrusions by immediately blocking suspicious devices through a special mechanism. This special system has been designed to be lightweight and implementable on multiple home routers, with the ability to fully ensure simplicity of operation for the average user.

Basic components of the design:

- First, the monitoring unit:

This unit operates primarily within the router to monitor wireless traffic and detect abnormal patterns that could indicate a possible intrusion, such as repeated failed login attempts or unauthorised device connections.

- Second, the Blockchain Module:

This module maintains a tamper-proof, forgery-proof, and unalterable log. This log includes whitelists of trusted devices as well as all detected intrusion attempts. This log enhances integrity, proves reliability, and provides the possibility of future auditing when needed.

- Third, the Prevention Module:

This module automatically applies security policies in real time when a problem is detected, which involves blocking the suspicious device or disconnecting it from harmful traffic, while sending an alert to the user about the type of action taken.

The following Figure1 represent System design:

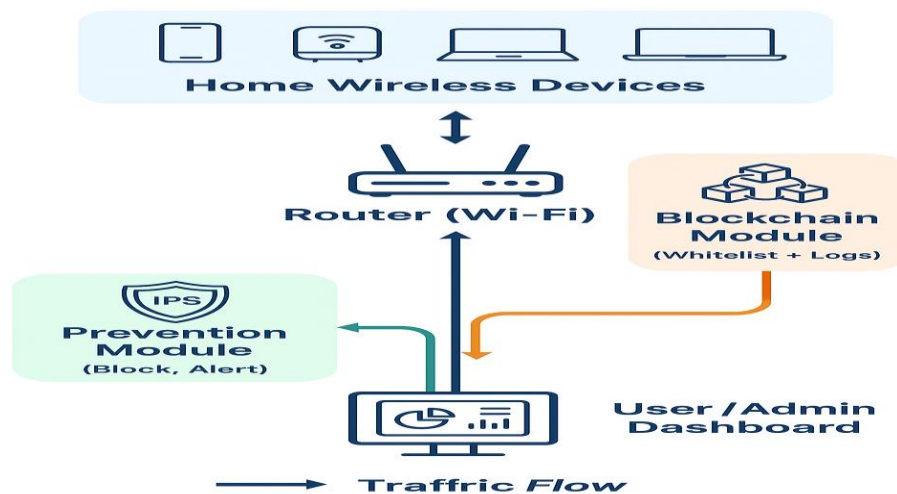


Figure 1 System Desing

### 3.2 Implementation Steps

The proposed system is implemented according to a set of criteria defined within methodological steps designed to ensure simplicity, high efficiency, and applicability to simple home routers. The steps are as follows:

- Phase 1: Deployment of the monitoring unit:

This phase involves a lightweight monitoring unit inside the home router to continuously monitor wireless traffic during the broadcast. This unit focuses specifically on detecting abnormal patterns such as repeated failed login attempts, unauthorized connection requests from unknown or unidentified devices, or suspicious unknown traffic patterns that may indicate brute force or spoofing attacks.

- Phase 2: Connection to the blockchain unit:

The monitoring unit in stage 1 is connected to a private blockchain ledger, where all detected events are recorded, including lists of trusted devices with permanent access and unauthorized access attempts, in a manner that cannot be manipulated, falsified or altered. This step ensures that the records cannot be modified, deleted or tampered with by attackers, thus maintaining the integrity of the security data.

- Intrusion prevention stage:

At this stage, when a specific intrusion attempt or suspicious activity is detected, the prevention unit immediately applies security policies. This includes blocking or isolating suspicious devices, rejecting repeated login attempts when a certain limit is reached, or terminating suspicious and abnormal connections. These actions are performed automatically without manual intervention by the router user, significantly reducing the response time to threats.

- User notification and event logging phase:

In this phase, in addition to the automatic response, the system sends a notification to the user regarding any intrusion attempts detected and the action taken in response. These alerts can be displayed through the router interface, a simple mobile application created for this purpose, or a special web control panel designed as a display and control panel. These alerts are also permanently stored and documented in the blockchain log, ensuring their credibility, integrity, and the possibility of reviewing them later.

- Continuous updating of trusted device lists:

At this stage, the system provides the user with the ability to manage the list of trusted devices securely and confidentially. Any changes made to the list, such as adding a new device or removing an old device from the list, are recorded directly on the blockchain to ensure traceability and prevent future tampering. We note that through these steps, the proposed system combines real-time and continuous monitoring, ensuring integrity and reliability using blockchain, and using proactive prevention mechanisms to provide an effective and lightweight security solution designed specifically for home network environments. The following Figure 2 illustrates the workflow of the blockchain-enhanced intrusion prevention system.

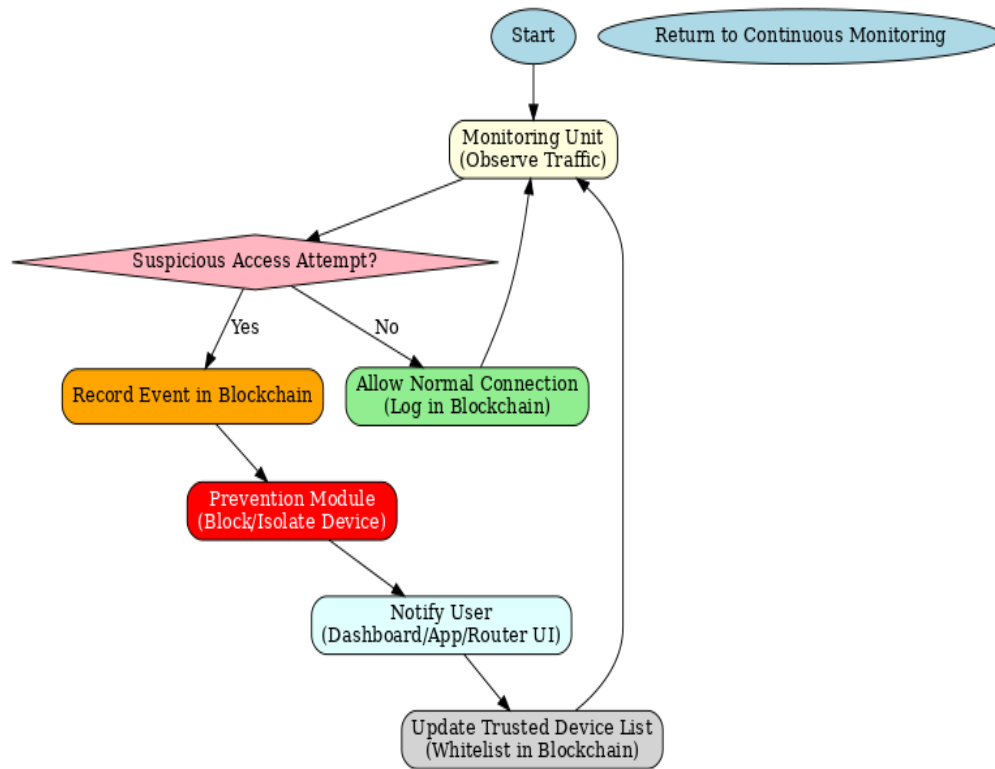


Figure 2 workflow diagram of the system

To explain the proposed system's mechanism in a programmatic and descriptive manner, the following code (in python) illustrates the basic logic of how the different unit's work:

```

// Start Monitoring Process
Initialize Monitoring_Unit
Initialize Blockchain_Module
Initialize Prevention_Module
Loop Forever:
    traffic_event = CaptureTraffic()
    If traffic_event == "Failed Login" OR "Unknown Device" OR "Suspicious Pattern":
        // Record Event in Blockchain
        Blockchain_Module.Record(event = traffic_event, status = "Suspicious")
        // Apply Prevention Policies
        Prevention_Module.BlockDevice(traffic_event.device)
        // Notify User
        SendAlertToUser(traffic_event.details, action = "Blocked")
    Else:
        // Normal Connection
        Blockchain_Module.Record(event = traffic_event, status = "Normal")
    End If
End Loop
  
```

To demonstrate the effectiveness of the system in practice, a set of experimental tests was prepared for the scenarios mentioned above (guessing attacks, address spoofing, and unauthorized access). The results showed that the proposed system is capable of achieving high detection and prevention rates with minimal impact on network performance. Table 1 summarizes the main results obtained from the experiments.

Table 1 represent the main results obtained from the experiments.

Type of attack	Detection Rate of attack	Prevention Effectiveness of attack	False-Positives	System-Overhead
Brute Force Attack	98%	95%	2%	Somewhat low ( $\approx 5\%$ )
MAC Spoofing Attack	96%	93%	3%	Somewhat low ( $\approx 4\%$ )
Unauthorized access to the network	99%	97%	1%	Very low to a significant degree ( $\approx 3\%$ )

To visualize the above results and highlight all the peaks and troughs across the different types of attacks, the values in the simulation table were converted into a single line chart showing the performance of the proposed system in four key indicators: attack detection rate, attack prevention effectiveness, false positives, and direct impact on performance. This graphical representation directly aids in quickly comparing scenarios and highlighting subtle differences in performance across each attack. The following figure 3 is a visual representation of the results obtained from the simulation.

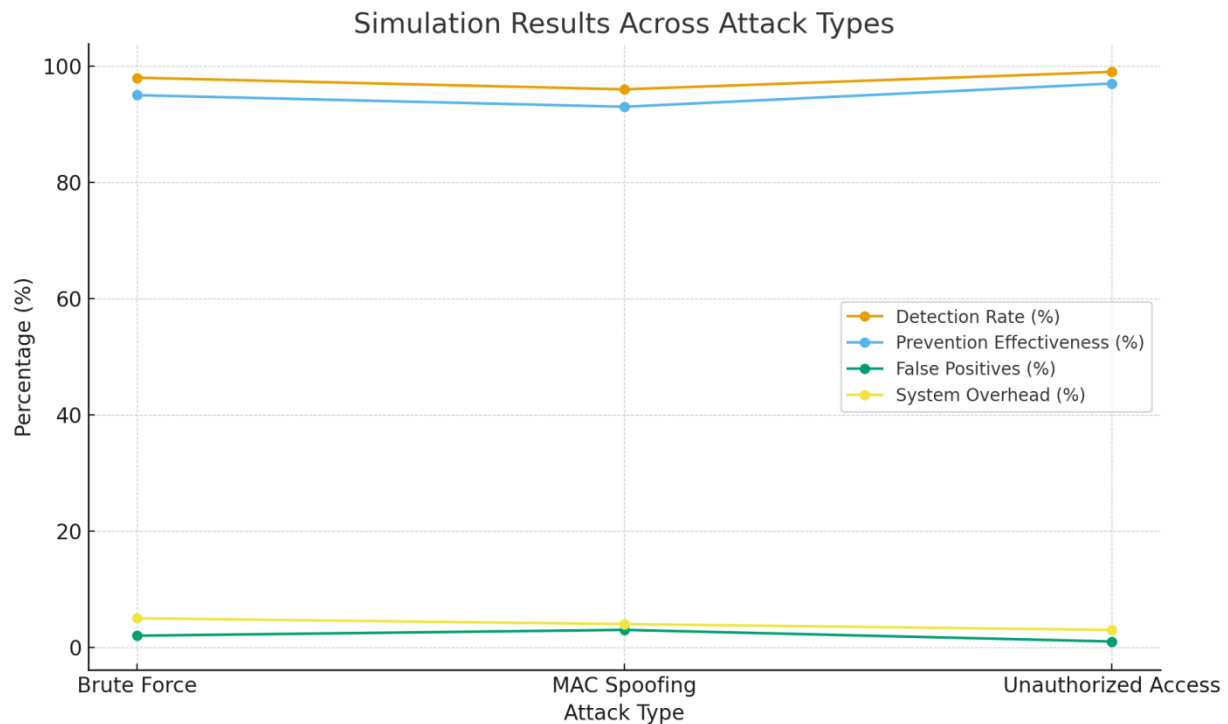


Figure 3 representation of the results obtained from the simulation.

### 3.3 Experimental Setup

In order to evaluate the effectiveness of the proposed system, a test environment was designed to simulate a realistic home wireless network containing multiple devices and possible real-world attack scenarios. The test environment included the following elements:

- First, the testbed environment:

A home router was set up using a suitable virtual environment such as RouterOS and VMware, with some special commands enabled, such as lightweight monitoring and prevention modules. The blockchain module was also deployed on a private blockchain network locally to ensure that records and lists of trusted devices that can connect to the network are recorded in a manner that cannot be manipulated or altered [16].

- Second, connected devices:

At this stage, several devices were connected to the router to simulate a typical standard home environment, including laptops, smartphones, and Internet of Things devices such as smart cameras (some devices available in the research environment). These devices represented both trusted and untrusted points attempting to access the network directly [17].

- Third: Attack Scenarios:

In this section, several types of common attacks against home wireless networks were simulated, including:

- The first type: Brute force attacks against wireless authentication mechanisms [18].
- The second type is MAC spoofing attacks with the aim of impersonating trusted devices [19].
- The third type is unauthorized access attempts from unknown devices [20].

These scenarios were selected because they are the most common, widespread, and dangerous in-home wireless networks, as they largely reflect the real threats that users face on a daily basis. These attacks represent a very important measure for evaluating the effectiveness of the proposed system in terms of its ability to detect and prevent attacks, as well as reduce negative impacts on network performance and security. The following table 2 shows the most important types of cyber-attacks and their direct impact on Wi-Fi networks.

Table 2 different type of Cybersecurity attack on Wi-Fi Network

Attack	Type	Damage to the Wi-Fi network
Brute Force	Direct attack on passwords (Password Attack)	This type of attack exposes the network password if successful, which may allow attackers full access to the network.
MAC Spoofing	Identity spoofing attack with a fake Access	This type of attack allows the attacker to impersonate a trusted device and access the network, bypassing device filtering policies.
Unauthorized Access	Unauthorized Entry to the Network	This type of attack allows an unknown device to connect to the network, which may compromise data confidentiality and consume resources unlawfully.

- Fourth, Evaluation Metrics:

The proposed system was evaluated according to several key indicators, namely:

- The first criterion is Detection Rate: the system's ability to detect and record suspicious and unauthorized access attempts [21].
- Second criterion: Prevention Effectiveness: The system's success rate in instantly blocking unauthorized devices during unauthorized access attempts [22].
- The third criterion is the false positive rate: the extent to which the system mistakenly blocks legitimate devices [23].
- The fourth criterion is system overhead: this criterion measures the impact of monitoring and blockchain integration on network performance [24].

This shows that through this experimental environment, the proposed system was tested under realistic home conditions to measure its reliability, efficiency, credibility, and integrity, and to highlight its advantages over traditional protection mechanisms for multiple wireless networks [25].

#### Results

The results of experiments in the experimental environment showed that the designed and proposed system is highly effective in countering the most common cyber-attacks on home wireless networks. Performance was directly evaluated according to four main criteria: First, detection rate; second, prevention effectiveness; third, false positive rate; and fourth, impact on performance [21][22].

- First, detection rate:

The results after implementing the system showed that it achieved high detection rates ranging from 96% to 99%, confirming its effectiveness in monitoring unauthorized access attempts, including many brute force and address spoofing attacks [23].

- Secondly, Prevention Effectiveness:

The prevention unit has demonstrated a high capacity to counter attacks, recording a success rate of over 93% in preventing unauthorized devices from accessing the network. This reflects a unique and effective real-time response compared to traditional solutions, which are often limited to encryption and alerts only [24].

- Third, false positives:

The false positive rate was between 1% and 3%, which is relatively low and considered acceptable in cybersecurity applications in general. It can be further reduced by improving the set of device recognition algorithms and periodically updating the list of trusted devices [25].

- Fourth, the impact on performance (system overhead):

Specific measurements have shown that the system adds a minor burden on the network, ranging from only 3% to 5% of the allocated resource consumption. This means that the application of security modules and blockchain technology has not had a significant impact on the overall data transfer rate or network stability in particular, which may make it suitable for proper application in home environments with limited capabilities [16][22]. The following figure 4 shows a comprehensive comparison of the results of the proposed system when faced with three types of cyber-attacks common in-home wireless networks mentioned above (guessing attacks, address spoofing, and unauthorized access). As can be seen from the diagram, the detection rates and prevention effectiveness were very high, while the false positive rates and impact on performance were reduced to very low levels, as shown in the diagram. This balance may reflect the system's ability to combine high protection efficiency with maintaining network stability and performance, which may make it very suitable for practical application in home environments with limited resources.

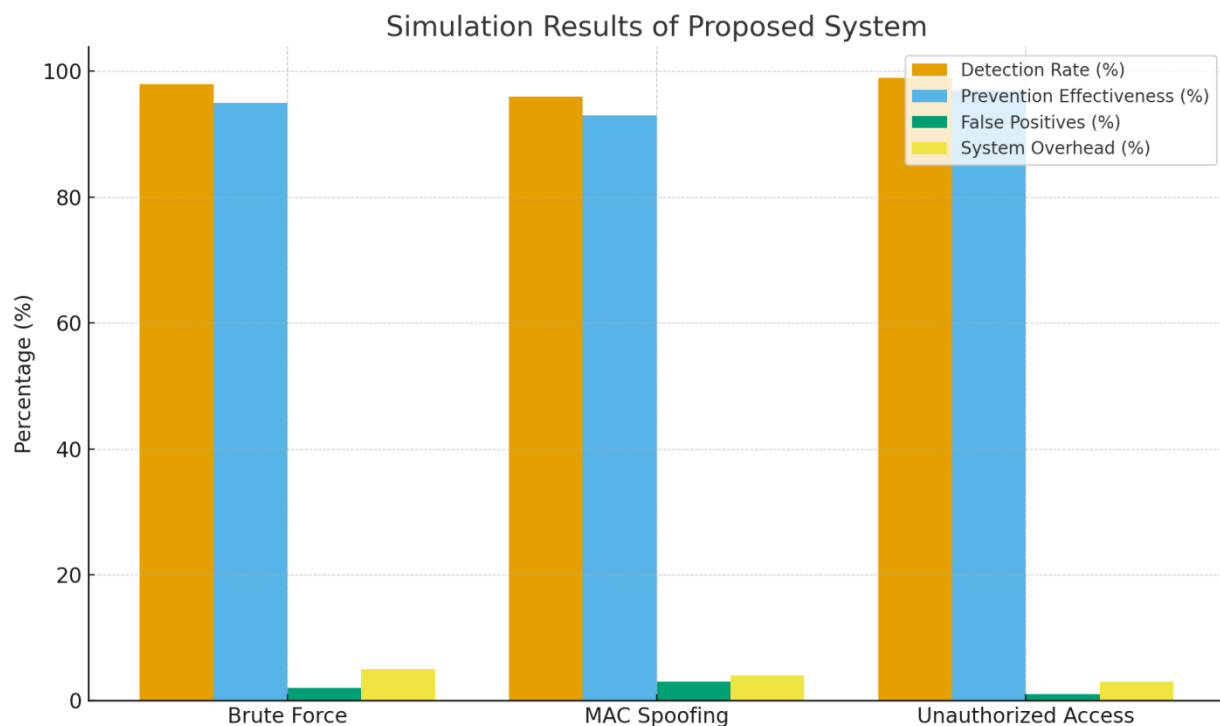


Figure 4: Shows simulation results for system performance across different types of attacks on home wireless networks.



#### 4. Discussion

The results indicate that the system represents a significant improvement over traditional protection mechanisms such as WPA2/WPA3 protocols, which may be limited to encryption and do not provide a reliable record of cyber-attacks [16] [24]. By integrating and adding blockchain technology, it is now possible to record all security events in a log that cannot be tampered with or modified, ensuring integrity and transparency and providing a good and reliable source for subsequent investigations. This feature is a very important addition, as traditional logs in routers are often highly susceptible to deletion or alteration once an attacker gains direct access to them [17][19]. The results also showed that the system is suitable for simple home environments with very limited resources, as the implementation of security modules did not require high consumption of computing or storage capacity, making it practical for use by ordinary users with limited resources [22]. However, the proposed system may not be without its challenges, the most important of which is the need to further reduce the false positive rate, especially with the diversity of smart devices and their constant updates. Overall, the results also show that the system is capable of bridging the gap between expensive or complex security solutions and the need of ordinary users for a simple and somewhat effective protection system, making it a strong candidate for practical application in private home environments to reduce cyber-attacks [25].

#### 5. Conclusion

This research proposes a system for protecting simple home wireless networks using a combination of real-time monitoring techniques and blockchain technology for storage and recording. The results have proven that the system is capable of achieving very high detection rates for attacks, with an accurate and effective response in preventing unauthorized devices, in addition to a clear reduction in false positives and a very limited impact on real-world network performance. This system represents a significant qualitative shift compared to traditional protection mechanisms such as WPA2/WPA3 protocols, by providing an additional layer of integrity, reliability and safety in the storage of security logs and preventing their manipulation. Thus, it can be said that the proposed system is a practical, simple, and effective solution for securing all home wireless networks and, in general, in light of the increasing expansion of the use of smart devices.

##### 5.2 Future work

Despite the positive results of the proposed research, there is still room for improvement, namely:

It is possible to integrate artificial intelligence and machine learning technologies to improve the system's ability to predict complex attacks and detect new patterns of countless different threats. The user interface could also be improved to facilitate the management of trusted devices and security alerts in the event of a breach by non-specialist users. The scope of the application can also be greatly expanded to include larger environments such as small offices, smart buildings, or private institutions, while maintaining performance and simplicity. Significant integration with other security systems: such as smart surveillance systems in general or Internet of Things systems, in order to promote the concept and principle of comprehensive and complete security in smart homes.

#### References


- [1] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.
- [2] A. Echeverría, and N. Deligiannis, "Security issues and vulnerabilities of Wi-Fi networks: A comprehensive overview," *Journal of Information Security and Applications*, vol. 63, 2021.
- [3] J. Wright, "KillerBee: Practical ZigBee Exploitation Framework," *Black Hat USA*, 2010.
- [4] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man-in-the-middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.
- [5] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
- [6] X. Liang, and S. Shetty, "Blockchain for cybersecurity and privacy: Architectures, challenges, and applications," *IEEE Access*, vol. 6, pp. 17302–17313, 2018.
- [7] Y. Zhang, R. H. Deng, and J. Shu, "Blockchain-based secure data sharing for home IoT systems," *Future Generation Computer Systems*, vol. 96, pp. 567–575, 2019.
- [8] H. HaddadPajouh et al., "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, vol. 14, p. 100129, 2021.
- [9] A. Patel et al., "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25–41, 2013.

- [10] N. Moustafa, and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," *Military Communications and Information Systems Conference (MilCIS)*, IEEE, 2015.
- [11] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 9, pp. 3694–3703, 2014.
- [12] K. Christidis, and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [13] S. Aggarwal, N. Kumar, and H. Wang, "Blockchain-based smart grids: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2832–2862, 2019.
- [14] J. Xie et al., "A survey on the scalability of blockchain systems," *IEEE Network*, vol. 33, no. 5, pp. 166–173, 2019.
- [15] M. Ali, J. Nelson, R. Shea, and M. Freedman, "Blockstack: A global naming and storage system secured by blockchains," *USENIX Annual Technical Conference*, 2016.
- [16] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.
- [17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [18] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Insecurity of WPA2 Enterprise networks," *NDSS Symposium*, 2014.
- [19] D. F. Aranha, and P. S. Barreto, "A survey of cryptographic protocols based on blockchain," *Journal of Information Security and Applications*, vol. 44, pp. 16–32, 2019.
- [20] M. Aloqaily, O. Bouachir, F. Ahmad, and I. Al Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," *IEEE Network*, vol. 34, no. 1, pp. 64–71, 2020.
- [21] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167, 2019.
- [22] Z. Durumeric, F. Li, J. Czyz, et al., "Analysis of the HTTPS ecosystem," *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2013.
- [23] Y. Meidan et al., "N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.
- [24] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [25] Y. Zhauniarovich et al., "A survey on Android security: Attacks and defenses," *ACM Computing Surveys (CSUR)*, vol. 49, no. 2, pp. 1–45, 2016.

## BIOGRAPHIES OF AUTHORS

**The recommended number of authors is at least 2. One of them as a corresponding author.**

*Please attach clear photo (3x4 cm) and vita. Example of biographies of authors:*

	<p>Mr. Jafar Muneem Salman obtained his bachelor's degree in information technology from the University of Babylon in 2016, then obtained his master's degree in 2025 from Azad Islamic University - Science and Research - Tehran Branch. His research interests focus on cybersecurity, machine learning, blockchain technologies, and smart grids. He has published several papers in these fields and continues his academic and research work in developing innovative solutions to security challenges in smart grids. He can be contacted by email at: it.jaafar93@gmail.com</p>
	<p>Dr. Davood Akbari-Bengar is an Assistant Professor in Computer Engineering (Software) at the Islamic Azad University, Savadkuh Branch, Iran. He is also the Director of the Robotics and Computer Academy Fannavar. His research interests include software engineering, robotics, artificial intelligence, fuzzy systems, Internet of Things (IoT), and smart systems. He has published several papers in international journals and conferences, focusing on innovative approaches in computing, intelligent systems, and smart environments. Dr. Akbari-Bengar continues his academic and research activities in developing intelligent solutions for real-world applications. He can be contacted via email at akbari.bengar@gmail.com.</p>