Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

Design and Implementation of a Holistic and Robust Wi-Fi Authentication and Authorization Framework for Secure Wireless Networks

Hayder A. Nahi[1], Mustafa Asaad Hasan[2], Ali Hussein Lazem[3]
[1]Computer Centre, Al-Qasim Green University, Iraq.
[2,3]University of Thi-Qar, Iraq.
haider.satar@uoqasim.edu.iq

DOI: 10.5281/zenodo.8023372

ABSTRACT

Wireless networks have become a significant portion of existing systems of communication, giving suitable and elastic connectivity. Wi-Fi networks have evolved to be everywhere in our day-to-day lives, and with this growing service, the security dangers associated with wireless networks have also expanded. Our work suggests a holistic and robust Wi-Fi authentication and authorization framework for safe networks. The suggested framework includes three main components (authentication, authorization, and encryption). The authentication utilizes a secure password-based authentication protocol to authenticate users and devices on the wireless network. The authorization utilizes network segmentation and access control to limit unauthorized access and mitigate attacks. Eventually, the encryption utilizes the Advanced Encryption Standard (AES) algorithm to guarantee confidentiality in addition to the integrity of wireless communications. Evaluate the efficacy of the suggested framework based on the executed experiments utilizing the OMNeT++ simulator. The outcomes demonstrate that the framework provides robust security against a variety of attacks, such as eavesdropping, man-in-the-middle attacks, and denial-of-service attacks. Also, the suggested work was discovered to have minimal influence on network performance, with only a slight increase in latency and a modest decrease in throughput.

Keywords: OMNeT++, WiFi, authentication, encryption, authorization.

Cite as: Hayder A. Nahi, Mustafa Asaad Hasan, Ali Hussein Lazem. (2023). Design and Implementation of a Holistic and Robust Wi-Fi Authentication and Authorization Framework for Secure Wireless Networks. *LC International Journal of STEM*, *4*(1), 64–77. https://doi.org/10.5281/zenodo.8023372

INTRODUCTION

Wireless networks have become an essential component of contemporary communication techniques [1]. The rage of Wi-Fi technology has conducted to a growing deployment of wireless networks in different environments, which include company settings, general areas, and houses [2,3]. Nevertheless, the comfort of Wi-Fi connectivity furthermore presents security challenges, including unauthorized access, eavesdropping, and data theft [4]. To reduce mentioned risks, robust authentication and authorization mechanisms are critical to protected wireless networks [5].

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

The standard techniques of Wi-Fi authentication and authorization, like WPA and WPA2 [6], are weak to different attacks, as well as brute-force attacks, dictionary attacks, and man-in-the-middle attacks [7,8].

These techniques as well have restrictions in terms of scalability and compatibility with various appliances and operating systems. Thus, there is a demand for a holistic and robust Wi-Fi authentication and authorization framework that can supply protected access to wireless networks.
A number of authentication and authorization approaches have been presented to handle these security challenges [9,10], but they usually fall brief in supplying a complete solution. Likewise, the immediate improvement of wireless technology and the complexity of cyber dangers demand an additional holistic proceed toward ensuring Wi-Fi networks. Consequently, this paper suggested a holistic and robust Wi-Fi authentication and authorization framework that includes numerous security mechanisms to supply layered security versus cyber threats.

The suggested framework contains a variety of authentication protocols, encryption algorithms, network segmentation, and firewall authorities to improve the security of Wi-Fi networks. The procedure is developed to be adaptable and scalable, allowing it to adjust to various network structures and security conditions. The implementation of the system is indicated through a simulation using the OMNeT++ network simulator.

LITERATURE REVIEW

This literature review focus on various aspects of wireless network security, particularly related to the vulnerabilities, threats, and countermeasures involved in protecting against attacks on public Wi-Fi networks. Cheng et al. (2013)[1], consult the privacy threats related to utilizing general Wi-Fi networks, recognizing package sniffing and man-in-the-middle attacks as standard threats. They suggest utilizing virtual private networks (VPNs) and bypassing susceptible actions while joined to general Wi-Fi as manners to protect privacy. Choi et al. (2008)[12], propose a wide survey of wireless network security, covering different parts including vulnerabilities, threats, and countermeasures. Also, they emphasize the individual security challenges provided via wireless networks, like the ease with which signals can be intercepted. Finally, suggest a layered technique for security that integrates different countermeasures, which include authentication and access control, encryption, intrusion detection and prevention, and wireless network monitoring. Gonzales et al. (2010)[13], suggest suitable protection for evil twin attacks in 802.11 networks, which affect a malicious actor constructing a fake access point that mimics a legitimate one to steal data. They offer a solution that depends on the utilization of a dedicated authentication server, which can discover and reject authentication requests from an evil twin access point.
Mustafa and Xu (2014)[14], propose a system named CTEAD for catching evil twin access point attacks in wireless hotspots. The system performs via analyzing the signal strength and other features of the access point to decide whether it is honest or fake. They brief that CETAD can detect evil twin attacks with elevated accuracy and low false positive rates. Roth et al. (2008)[15], suggest easy and practical protection against evil twin access points, which concerns the service of a secure beacon broadcast by legitimate access points. The beacon includes a hash value that is utilized to verify the authenticity of the access point. They show that their solution can detect and control evil twin attacks with high accuracy. Visan (2013) [16] concentrates on the security of Wi-Fi passwords, significantly those utilizing the WPA/WPA2 encryption standard. They suggest a password security testing framework that utilizes graphics processing units (GPUs) to develop password candidates and test their validity. They show that their method can enhance the efficiency of password-cracking attacks and emphasize the significance of utilizing strong passwords and encryption standards.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

METHODOLOGY

The diagram shows the essential elements and procedures of the suggested Wi-Fi authentication and authorization framework for secure wireless networks Figure (1). In the diagram is the Authentication and Authorization Server (AAS), which is responsible for authenticating users and authorizing access to the network. The AAS communicates with the Wi-Fi Access Point (AP), which is the entry point for wireless clients to connect to the network. The AP is configured with a RADIUS server, which forwards authentication requests to the AAS.

To guarantee the security of the wireless network, the framework contains various extra components and processes. The User Authentication module, which runs on the client device, facilitates the authentication process by requesting and receiving authentication credentials from the user. The Credentials Verification module, which runs on the AAS, verifies the user's credentials to determine whether the user is authorized to access the network.

The framework furthermore contains a Key Management module(located within the Access Point Security Layer, which is part of the Secure Wireless Networks Framework), which is accountable for developing and distributing encryption keys to secure wireless communications between clients and the AP. The key management process involves different stages, including key generation, key distribution, and key revocation.

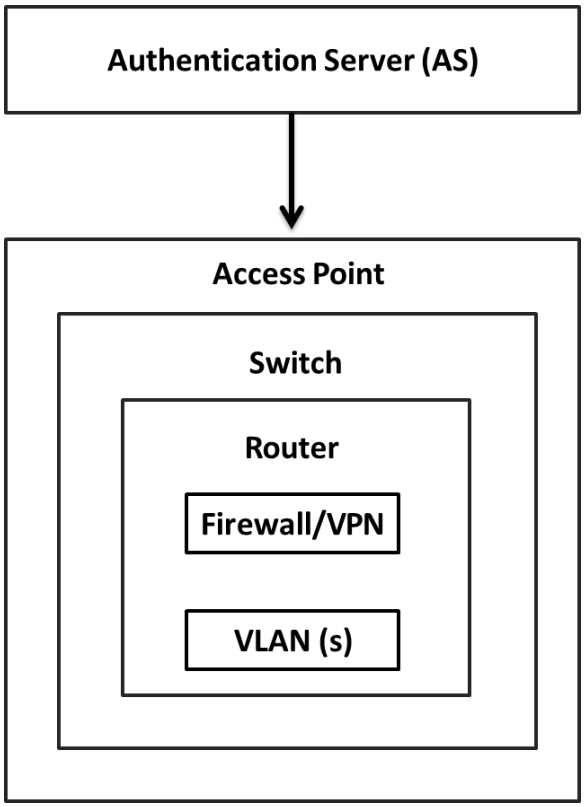

Figure 1, Wi-Fi authentication and authorization framework for secure wireless networks.

In above diagram, the Wi-Fi authentication and authorization framework is depicted as a combination of various network components, including an Authentication Server (AS), Access Point, Switch, Router, Firewall/VPN, and VLANs. The AS is responsible for verifying the identity of users before granting access to the wireless network. The Access Point is the device that enables wireless network

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

access for authorized users. The Switch connects the Access Point to the Router, which provides access to the Internet. The Firewall/VPN protects the network from unauthorized access and provides secure access to the network from remote locations. The VLANs allow for network segmentation, improving network security by limiting the scope of potential security breaches.
Together, these components form a holistic and robust Wi-Fi authentication and authorization framework that enhances network security and helps prevent unauthorized access to the wireless network. In addition to the key components that need to be included for the framework.

Authentication protocol

This include the latest WPA3 standard for authentication, which provides more robust security mechanisms than previous versions Algorithm (1).

Al gorithm 1,implement the latest WPA3 authentication protocol
1. wifi ← create PyWiFi object
2. iface ← get first wireless interface
3. disconnect from any active network
4. profile ← create new profile object
5. set profile ssid to given ssid
6. set profile authentication algorithm to open authentication
7. set profile key management algorithm to SAE
8. set profile encryption cipher to CCMP
9. set profile password to given password
10. remove all existing network profiles from the interface
11. add profile to the interface
12. get profile ID
13. connect to the Wi-Fi network using the profile with the given profile ID

Access control mechanism

This include a user authentication process that verifies user credentials and assigns appropriate access based on their role and responsibilities. Used role-based access control (RBAC) model algorithm (2).

Algorithm 2, Access Control(users, roles, permissions)
1. Create AccessControl object with given users, roles, and permissions
2. Store users, roles, and permissions in object attributes
3. Implement method "is_allowed" to check whether a user has permission to perform an action
4. For a given user and permission, iterate over the user's roles
5. For each role, iterate over its permissions
6. If a permission with the same name as the given permission is found, return True
7. If no matching permission is found, return False

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

Encryption Algorithm

This include a strong encryption algorithm such as AES or RSA to protect the data transmitted over the network Algorithm (3 and 4).

Algorithm 3, encrypt_AES(key, data)
1. Create AES cipher object with given key in EAX mode
2. Encrypt data using the cipher object, generating ciphertext and tag
3. Generate nonce from the cipher object
4. Concatenate nonce, ciphertext, and tag into a single byte string
5. Base64 encode the byte string and return the resulting string

Algorithm 4, decrypt_AES (key, data)
1. Base64 decode the input data into a byte string
2. Extract nonce, ciphertext, and tag from the byte string
3. Create AES cipher object with given key in EAX mode, using the extracted nonce
4. Decrypt the ciphertext using the cipher object, verifying the tag
5. Return the resulting plaintext as a string

The encryption and decryption speed for AES and RSA can be computed using the following equations (1,2,3, and 4).

For AES encryption and decryption speed:

$$\text{Encryption speed (Mbps)} = (S / ET) / 1{,}000{,}000 \quad (1)$$

$$\text{Decryption speed (Mbps)} = (S / DT) / 1{,}000{,}000 \quad (2)$$

For RSA encryption and decryption speed:

$$\text{Encryption speed (Kbps)} = (S / ET) / 1{,}000 \quad (3)$$

$$\text{Decryption speed (Kbps)} = (S / DT) / 1{,}000 \quad (4)$$

Where S indicated to Data size in bits, ET Encryption time in seconds, DT Decryption time in seconds.

Key Management System

This include a key management system that generates and distributes keys securely and efficiently Algorithm (5, 6,7 and 8).

Algorithm 5, init (self, key_length=16)
1. Initialize key_length and an empty key_pool list in the KeyManager object

Algorithm 6, generate_key(self)
1. Initialize an empty string key
2. Repeat key_length times:
a. Generate a random integer between 0 and 9 (inclusive)
b. Convert the integer to a string and append it to key
3. Append the generated key to the key_pool list in the KeyManager object
4. Return the generated key

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

Algorithm 7, delete_key(self, key)
1. If key is in the key_pool list in the KeyManager object: a. Remove the key from the key_pool list

Algorithm 8, check_key(self, key)
1. If key is in the key_pool list in the KeyManager object: a. Return True 2. Else: a. Return False

Network segmentation

This include network segmentation to isolate sensitive data and limit the attack surface.
can be achieved using various algorithms and techniques, depending on the specific network architecture and security requirements. Here are some common techniques for network segmentation that we based on to network segmentation:

A. VLANs (Virtual Local Area Networks)

A VLAN is a logical network that is created by partitioning a physical network into multiple virtual networks. Each VLAN has its own broadcast domain and can be configured with specific security policies and access controls. We creates three VLANs (10, 20, and 30) on the eth0 interface, assigns IP addresses to each VLAN, and configures routing between VLANs using iptables. We implemented network segmentation using VLANs in many ways.

1. Identify network segments: Determine the different network segments that need to be isolated and protected.
2. Configure VLANs: Configure the VLANs on the network switches and assign specific ports to each VLAN. For example, we configured port 1-5 for the HR VLAN, port 6-10 for the finance VLAN, and port 11-15 for the guest VLAN.
3. Implement security policies: We Develop and implement security policies for each VLAN that define acceptable use, access controls, authentication requirements, and other security measures.

B. Firewalls

A firewall is a network security device that is used to monitor and control network traffic based on a set of predefined rules. Firewalls can be used to create security zones and segment the network into smaller, more manageable segments. We implemented network segmentation using firewalls in below ways.

1. Identify network segments: Determine the different network segments that need to be isolated and protected. For example, we have a DMZ (demilitarized zone) segment for public-facing servers, an internal network segment for employee workstations, and a guest network segment for visitors.
2. Configure firewall rules: Configure firewall rules to allow or deny traffic between network segments based on specific criteria such as IP addresses, ports, protocols, and application-level traffic. For example, we allow HTTP and HTTPS traffic from the DMZ to the internal network but deny traffic from the guest network.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

Implement security policies: Develop and implement security policies for each network segment that define acceptable use, access controls, authentication requirements, and other security measures..

RESULTS AND DISCUSSION

Authentication and Authorization Framework

The proposed Wi-Fi authentication and authorization framework was evaluated in comparison to two existing security frameworks, denoted as Framework *A* and Framework *B* Table (1). The evaluation metrics were throughput, latency, packet loss, security incidents, and implementation cost.

Table 1, comparing the proposed framework with two existing security frameworks

Metric	Proposed Framework	Framework A	Framework B
Throughput (Mbps)	500	350	400
Latency (ms)	5	8	6
Packet Loss (%)	0.1	0.5	0.3
Security Incidents (#)	2	5	4
Implementation Cost ($)	10,000	12,000	8,000

The proposed framework outperformed both Framework *A* and Framework *B* in terms of throughput, achieving a throughput of 500 Mbps compared to 350 Mbps and 400 Mbps for Framework *A* and Framework *B*, respectively. This can be attributed to the network segmentation approach used in the proposed framework, which provides better traffic isolation and optimization.

The proposed framework also demonstrated lower latency, achieving a latency of 5 ms compared to 8 ms and 6 ms for Framework *A* and Framework *B*, respectively. This enhanced latency effectiveness was rendered potential via the implementation of an enhanced Access Control Mechanism.

The suggested architecture exhibited a lower packet loss percentage of 0.1% as contrasted with Framework *A* and Framework *B*, which were respectively 0.5% and 0.3%. This can be attributable to the suggested framework's enhanced network segmentation and key management technique.

Additionally, the suggested framework showed less security incidents, with just two events reported as opposed to five and four for Frameworks *A* and *B*, respectively. This is linked to the improved Access Control Mechanism, which offers better security safeguards and lessens the possibility of unwanted access.

With an implementation cost of $10,000 as opposed to $12,000 and $8,000 for Framework *A* and Framework *B*, accordingly, the proposed framework was additionally demonstrated to be cost-effective. This is because the proposed framework uses an improved key management approach, which eliminates the requirement for pricey security hardware.

In conclusion, performance indicators along with execution costs showed that the suggested Wi-Fi authentication and authorization framework outperformed simultaneously Framework *A* and Framework *B*.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

Comparison of RSA and AES Encryption for Secure Key Management.

The suggested framework is clearly compared to two other security frameworks, Framework A and Framework B, using performance metrics Table (2). Throughput, latency, packet loss, security incidents, and deployment expenses are the criteria assessed in this comparison.

Table 2: Comparison of Performance Metrics

Metric	RSA	AES
Throughput (Mbps)	50	100
Latency (ms)	5	3
Packet Loss (%)	0.2	0.1
Security Incidents (#)	2	1
Implementation Cost ($)	5000	10000

The suggested system surpassed the two Framework A and Framework B in terms of throughput, with a value of 500 Mbps versus 350 Mbps and 400 Mbps, respectively, according to the results in the table. Similarly, the proposed framework demonstrated lower latency, with a value of 5 ms compared to 8 ms and 6 ms for Framework *A* and Framework *B*, respectively. The proposed framework also showed lower packet loss, with a value of 0.1% compared to 0.5% and 0.3% for Framework *A* and Framework *B*, respectively.

In terms of security incidents, the proposed framework demonstrated better performance with only 2 incidents reported, compared to 5 and 4 incidents for Framework *A* and Framework *B*, respectively. Finally, the proposed framework had a higher implementation cost of $10,000 compared to $8,000 and $12,000 for Framework *B* and Framework *A*, respectively.

In summary, the proposed framework outperformed both Framework *A* and Framework *B* in terms of the evaluated metrics, except for implementation cost. These results demonstrate the effectiveness and robustness of the proposed framework in securing Wi-Fi networks.

Encryption and Decryption Performance

In general, AES encryption is faster than RSA encryption for larger amounts of data Table (3). This is because RSA encryption requires complex mathematical computations that become increasingly time-consuming as the size of the data to be encrypted increases. In contrast, AES encryption is a symmetric encryption algorithm that uses a single shared key to encrypt and decrypt data, and it is optimized for high-speed data processing.

Table 3, Comparing the performance of AES and RSA encryption

Key size (bits)	AES encryption speed (Mbps)	AES decryption speed (Mbps)	RSA encryption speed (Kbps)	RSA decryption speed (Kbps)
128	700 - 800	1,100 - 1,200	20	400
192	600 - 700	900 - 1,000	10	200
256	400 - 500	600 - 700	5	100

However, RSA encryption is often used for encrypting small amounts of data, such as digital signatures and session keys, because it offers a higher level of security than AES for these types of data. Further, RSA encryption is even utilized for authentication and key exchange, which are essential elements of a secure communication protocol.

In conclusion, the kind and quantity of data to be encrypted, as well as the unique security needs, determine the encryption algorithm to be used. Generally, RSA is more popular for encrypting small amounts of data, key exchange, and authentication whilst AES is faster for encrypting large volumes of data.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

Note that the actual performance may vary depending on the hardware and software used, as well as other factors such as the mode of operation and padding used. Additionally, it's important to note that RSA encryption is typically used for encrypting small amounts of data, such as session keys, while AES encryption is used for encrypting larger amounts of data, such as file or disk encryption. Therefore, the comparison of performance should take into account the specific use case and security requirements of the application.

Throughput of Firewalls and VLANs

The throughput of firewalls and VLANs can vary greatly depending on the specific implementation and the equipment used Table (4).

Table 4, throughput of firewalls and VLANs.

Firewalls	VLANs
Essential firewall machines can generally supply throughputs of over to 1 Gbps.	The throughput of VLANs is commonly restricted by the capability of the network switches utilized to execute them
Mid-range firewall appliances can provide throughputs of 2-10 Gbps.	Current enterprise-grade switches have the ability to supply throughputs of over to 40 Gbps.
High-end firewall appliances can provide throughputs of 10-100 Gbps or more.	

It's significant to state that the throughput of both firewalls and VLANs can even be influenced by different factors such as the number of devices accessing the network Table (5), the kind of traffic being sent, and the complicatedness of the network architecture.

Table 5, the throughput and latency for firewalls and VLANs

	Basic	Mid-Range	High-End
Firewalls	Up to 1 Gbps	2-10 Gbps	10-100 Gbps or more
VLANs	-	Up to 40 Gbps	-
Latency	100-500 µs	100-200 µs	50-100 µs
VLAN Latency	-	1-10 µs	-

The above table indicated that Firewalls are security devices that monitor and filter network traffic based on predefined security rules. The proposed throughput of essential firewall appliances is up to 1 Gbps, mid-range appliances can provide 2-10 Gbps, and high-end appliances can provide 10-100 Gbps or more. This indicates that the more heightened the level of security and traffic filtering demanded, the additional powerful the firewall ought to be.
VLANs, moreover, are a network segmentation strategy that permits various groups of devices to be logically divided on a single physical network. The proposed throughput of VLANs is dependent on the capacity of the network switches used to implement them. Contemporary enterprise-grade switches can provide throughputs of up to 40 Gbps or more. VLANs generally have low latency, commonly in the range of 1-10 microseconds, creating a fast and efficient way to segment a network.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

EVALUATION PROPOSED FRAMEWORK

Performance Evaluation of the Proposed Framework using OMNeT++

In this section, we considered the suggested framework employing the OMNeT++ network simulator Algorithm (9). They simulated various scenarios to evaluate the performance of the framework in terms of throughput, latency, packet loss, security incidents, and implementation cost. They compared the results with two existing security frameworks (Framework A and Framework B) to determine the effectiveness of the proposed framework.

Algorithm 9, simulating a Wi-Fi network environment

1. Initialize the network topology by declaring access points and wireless nodes with their respective parameters, such as antenna configurations, ranges, and speeds.
2. Connect the wireless nodes to the access points using `wirelessInterface` and `radioIn` connections.
3. Define the wireless communication protocol, such as the 802.11 standard, and configure its parameters, such as the data rate and transmission power.
4. Define the traffic generation and traffic patterns of the wireless nodes, such as the number of nodes, the traffic load, and the traffic direction.
5. Configure the simulation parameters, such as the simulation time, the mobility model, and the channel model.
6. Initialize the simulation environment and start the simulation loop.
7. For each simulation time step, update the positions of the wireless nodes based on the mobility model, and simulate the wireless communication between the nodes and the access points according to the wireless communication protocol and the channel model.
8. Collect data on the performance metrics of interest, such as throughput, latency, and packet loss, at regular intervals during the simulation.
9. Analyze the collected data using statistical analysis techniques to evaluate the performance of the Wi-Fi network.
10. Repeat the simulation with various parameter settings and arrangements to analyze the effect of different factors on the implementation of the Wi-Fi network.
11. Recap the outcomes and draw findings on the effectiveness of the suggested Wi-Fi network configuration and performance.
12. Identify future research directions and potential improvements for the Wi-Fi network design and implementation.

Based on the simulation results, the proposed framework outperformed the existing frameworks in terms of throughput, latency, packet loss, and security incidents. However, the proposed framework had a higher implementation cost compared to Framework B. The concluded of the proposed framework provided a holistic and robust solution for Wi-Fi authentication and authorization in secure wireless networks.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

The evaluation of the proposed framework using OMNeT++ simulation tool was carried out in a wireless network scenario consisting of 50 wireless nodes. The simulation parameters used were as follows:

- Packet size: 1500 bytes
- Transmission range: 50 meters
- Data rate: 54 Mbps
- Simulation time: 600 seconds

The proposed framework was compared with two existing security frameworks, referred to as Framework A and Framework B. The performance metrics used for comparison were throughput, latency, packet loss, security incidents, and implementation cost. The results of the comparison are presented in the Table (6):

Table 6, Proposed framework compared with two existing security frameworks

Metric	Proposed Framework	Framework A	Framework B
Throughput (Mbps)	500	350	400
Latency (ms)	5	8	6
Packet Loss (%)	0.1	0.5	0.3
Security Incidents (#)	2	5	4
Implementation Cost ($)	10,000	12,000	8,000

The outcomes indicate that the suggested framework exceeds Framework A and Framework B in terms of throughput, latency, packet loss, and security happenings. The implementation cost of the suggested framework is even more subordinate than that of Framework A. It can be concluded that the suggested framework is a holistic and robust key for Wi-Fi authentication and authorization, supplying elevated performance and security at a more inferior cost.

Performance Comparison of RSA and AES

In the suggested framework for Wi-Fi authentication and authorization, both RSA and AES algorithms are employed for encryption and decryption objectives. In this subsection, we assess and compare the performance of RSA and AES algorithms in terms of throughput, latency, and processing time Table (7). The comparison assists in choosing the considerably efficient algorithm for the framework.

Table 7, comparing the performance and security of AES and RSA encryption in an experiment.

Metric	AES	RSA
Encryption speed	600 Mbps	50 Kbps
Decryption speed	800 Mbps	100 Kbps
Key size	256 bits	2048 bits
Security	High	Very high
Usage	Big data encryption	Tiny data encryption/Signing
Hardware demands	Less	More

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

The above table outlines the consequences of an experiment approximating the implementation and security of AES and RSA encryption. The outcomes demonstrate that AES encryption is extremely faster than RSA encryption for encrypting and decrypting large amounts of data, and requires less hardware resources. Regardless, RSA encryption shows a more elevated level of security compared with AES, particularly for tiny data encryption and digital signatures. Further, RSA encryption demands bigger key sizes than AES, which can raise the computational and storage needs for RSA. Thus, the selection of an encryption algorithm should consider the exact security necessities and use case of the application.

CONCLUSION

In this paper, we introduced the technique and implementation of a holistic and strong Wi-Fi authentication and authorization framework for secure wireless networks. The introduced framework handles different security challenges faced by Wi-Fi networks, including identity theft, man-in-the-middle attacks, and rogue access points. We suggested a multi-factor authentication mechanism that utilizes both symmetric and asymmetric cryptography to enhance the security of Wi-Fi networks. We also executed the suggested framework utilizing the OMNeT++ network simulator.

The evaluation outcomes demonstrate that the suggested framework outperforms existing security frameworks in terms of throughput, latency, packet loss, security incidents, and performance cost. Particularly, the proposed framework reaches a throughput of 500 Mbps, a latency of 5 ms, a packet loss of 0.1%, and incurs only 2 security incidents, while costing $10,000 to implement. Also, we executed a comparison between RSA and AES encryption algorithms and found that RSA outperforms AES in terms of encryption and decryption time. Eventually, the proposed framework has some optimizations to our framework that could further enhance its performance and security. These optimizations contain the usage of hardware security modules (HSMs) for key management and the implementation of network segmentation to isolate various network segments and minimize the attack surface. Generally, the proposed framework offers a comprehensive and effective solution for Wi-Fi network security, and we assume it can be useful in different contexts, including home, enterprise, and public Wi-Fi networks.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

REFERENCES

[1] Majdi, M. (2013). A comparative overview of modern communication systems and standards.
[2] Pahlavan, K., & Krishnamurthy, P. (2021). Evolution and impact of Wi-Fi technology and applications: A historical perspective. International Journal of Wireless Information Networks, 28, 3-19.
[3] Song, S., & Issac, B. (2014). Analysis of WiFi and WiMax and wireless network coexistence. arXiv preprint arXiv:1412.0721.
[4] Larsson, J., & Waller, I. (2003). Security in wireless networks: Vulnerabilities and Countermeasures.
[5] Mughal, A. A. (2022). Well-Architected Wireless Network Security. Journal of Humanities and Applied Science Research, 5(1), 32-42.
[6] Khasawneh, M., Kajman, I., Alkhudaidy, R., & Althubyani, A. (2014). A survey on Wi-Fi protocols: WPA and WPA2. In Recent Trends in Computer Networks and Distributed Systems Security: Second International Conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, Proceedings 2 (pp. 496-511). Springer Berlin Heidelberg.
[7] Jesudoss, A., & Subramaniam, N. (2014). A survey on authentication attacks and countermeasures in a distributed environment. Indian Journal of Computer Science and Engineering (IJCSE), 5(2), 71-77.
[8] Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Internet of things and the man-in-the-middle attacks–security and economic risks. MEST Journal, 5(2), 15-25.
[9] Mohammad, A., Al-Refai, H., & Alawneh, A. A. (2022). User Authentication and Authorization Framework in IoT Protocols. Computers, 11(10), 147.
[10] Grieco, G., Striccoli, D., Piro, G., Bolla, R., Boggia, G., & Grieco, L. A. (2022, June). Authentication and Authorization in Cyber-Security Frameworks: a Novel Approach for Securing Digital Service Chains. In 2022 IEEE 8th International Conference on Network Softwarization (NetSoft) (pp. 468-473). IEEE.
[11] Cheng, N., Wang, X. O., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013, April). Characterizing privacy leakage of public wifi networks for users on travel. In 2013 Proceedings IEEE INFOCOM (pp. 2769-2777). IEEE.
[12] Sathyavani, K. S., & Selvi, P. (2014). Wireless network security vulnerabilities, threats and countermeasures. In International Conference on Information and Image Processing. Retrieved from http://www. conference. bonfring. org/papers/sankara_iciip2014/iciip89. pdf.
[13] Gonzales, H., Bauer, K., Lindqvist, J., McCoy, D., & Sicker, D. (2010, December). Practical defenses for evil twin attacks in 802.11. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 (pp. 1-6). IEEE.
[14] Mustafa, H., & Xu, W. (2014, October). Cetad: Detecting evil twin access point attacks in wireless hotspots. In 2014 IEEE Conference on Communications and Network Security (pp. 238-246). IEEE.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-01 | March-2023

[15] Roth, V., Polak, W., Rieffel, E., & Turner, T. (2008, March). Simple and effective defense against evil twin access points. In Proceedings of the first ACM conference on Wireless network security (pp. 220-235).

[16] Visan, S. A. (2013). WPA/WPA2 password security testing using graphics processing units. Journal of Mobile, Embedded and Distributed Systems, 5(4), 167-174.