Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.037129
Article

Efficient Authentication Scheme for UAV-Assisted Mobile Edge Computing

Maryam Alhassan and Abdul Raouf Khan*

Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Alahssa, 31982, Kingdom of Saudi Arabia
*Corresponding Author: Abdul Raouf Khan. Email: raoufkhan@kfu.edu.sa
Received: 24 October 2022; Accepted: 06 January 2023

Abstract: Preserving privacy is imperative in the new unmanned aerial vehicle (UAV)-assisted mobile edge computing (MEC) architecture to ensure that sensitive information is protected and kept secure throughout the communication. Simultaneously, efficiency must be considered while developing such a privacy-preserving scheme because the devices involved in these architectures are resource constrained. This study proposes a lightweight and efficient authentication scheme for the UAV-assisted MEC environment. The proposed scheme is a hardware-based password-less authentication mechanism that is based on the fact that temporal and memory-related efficiency can be significantly improved while maintaining the data security by adopting a hardware-based solution with a simple implementation. The proposed scheme works in four stages: system initialization, EU registration, EU authentication, and session establishment. It is implemented as a single hardware chip comprising registers and XOR gates, and it can run the entire process in one clock cycle. Consequently, the proposed scheme has significantly higher efficiency in terms of runtime and memory consumption compared to other prevalent methods in the area. Simulations are conducted to evaluate the proposed authentication algorithm. The results show that the scheme has an average execution time of 0.986 ms and consumes average memory of 34 KB. The hardware execution time is approximately 0.39 ns, which is a significantly less than the prevalent schemes, whose execution times range in milliseconds. Furthermore, the security of the proposed scheme is examined, and it is resistant to brute-force attacks. Around 1.158×10^{77} trials are required to overcome the system's security, which is not feasible using fastest available processors.

Keywords: MEC; UAVs; drones; security; efficiency; authentication; hardware-based solution; password-less authentication

1 Introduction

The Internet of Things (IoT) technology has emerged in response to the ever-growing demand for smarter, faster, and more convenient ways of connecting and controlling large numbers of smart

devices. IoT applications are employed in various fields, such as healthcare, business, home appliances, and the military [1]. IoT technology involves multiple smart devices and sensors that are connected together that continuously collect massive amounts of data, which are sent to a processing unit to obtain meaningful information for the end users (EUs) [2]. The central processing unit may be a cloud server that can provide unlimited storage and processing capabilities. Cloud computing is a suitable technology that allows limited-capability devices in the IoT to offload their computational tasks to a more powerful server [3]. However, the presence of only one central server increases the potential for the development of bottlenecks such that the performance of the entire system is dependent on a single point: the cloud server. Moreover, commonly used applications of the IoT involve mobile devices, such as vehicles and smartphones connected together. Cloud computing is not the best choice for this type of IoT due to limitations such as location unawareness, high cost, unavailability of real-time services, and insufficient guarantee of data privacy [3]. These limitations have led to the advent of another technology: mobile edge computing (MEC).

MEC provides a decentralized structure wherein several mobile servers with high processing capabilities are employed to serve the end devices [3]. Advantageously, MEC enables the processing of data closer to their origin [4], avoiding the bottleneck that is encountered in cloud computing. This decentralization yields many advantages, such as reduction of network latency, increase of the security of services, and energy saving [5]. MEC works well for IoT devices with limited levels of mobility. However, for some IoT applications wherein the connected devices have high levels of mobility, the MEC architecture is inadequate. Therefore, more efficient methods are required to handle the mobility of IoT devices. One solution involves the utilization of unmanned aerial vehicles (UAVs) to support MEC in mobile IoT environments.

UAVs are a promising technology that have attracted considerable research interest as they can solve various networking-related problems, such as those related to mobility and coverage area [6]. They also have many advantages in terms of network communication, such as flexibility, scalability, adaptability, and stability [7]. UAV-assisted MEC systems consolidate the benefits of UAVs and MEC. Fig. 1 displays the general architecture of a UAV-assisted MEC system.

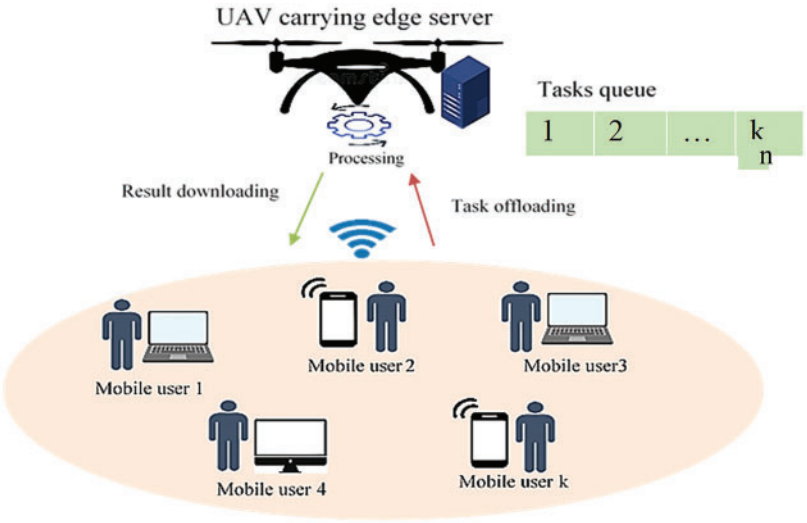

Figure 1: General architecture of the UAV-assisted MEC

UAV-assisted MEC systems are powerful systems that are capable of handling critical tasks requiring timely operations and intensive computations such as in some IoT applications [8]. They are considered to be context-aware systems because they involve location-related information [9]. UAV-assisted MEC systems have achieved notable success in civilian and military applications [10–13], including traffic monitoring [14], public safety [15], search and rescue missions [16], disaster management, and reconnaissance and recovery.

The implementation of UAV-assisted MEC systems has some challenges, such as limited onboard energy of the UAV [17], security of aerial data, security of the UAV, data privacy [18], and data management and storage. This study focuses on preserving privacy in UAV-assisted systems. Many studies have attempted to tackle privacy-related issues associated with UAV-assisted MEC systems. This study proposes an efficient authentication scheme for UAV-assisted MEC systems to preserve the data privacy while maximizing the efficiency and minimizing the computational overhead in terms of temporal and spatial requirements.

The remainder of this paper is organized as follows: Section 2 presents a review of past literature, Section 3 describes the proposed authentication scheme, and Section 4 presents the experimental setup used to assess the scheme as well as the results. Section 5 provides a detailed analysis of the proposed authentication algorithm, and Section 6 summarizes the conclusions.

2 Related Work

Each EU in the architecture of a UAV-assisted MEC system is connected to an edge server (ES) that is carried on a UAV. EUs can communicate and offload computational tasks to the ES that they are connected to. Authentication is required to verify the user identity before accepting their communication. Intruders may attempt to execute attacks on the system by pretending to be legitimate users. Moreover, issues related to the privacy of location-related data arise because the UAV-assisted MEC system is a location-aware system. This has drawn the attention of many researchers, and several solutions have been proposed for this problem. In this section, some state-of-the-art studies on privacy-preserving schemes for MEC systems as a general case and for UAV-assisted MEC as a specific case are discussed.

Zhang et al. [19] proposed a privacy-preserving authentication framework that combines 5G and edge computing technologies, and it is mainly designed for use in vehicular networks to securely transfer traffic-related information. They aimed to ensure secure communication in 5G-enabled vehicular networks. Moreover, Zhang et al. [19] proposed a signature scheme based on authentication that mainly functions in two parts. The first part comprises an authentication process that involves using a fuzzy logic model to select the vehicle for edge computing. The second part involves mutual authentication between the selected edge-computing vehicle and another regular vehicle. Furthermore, they considered allowing the sharing of information in groups while ensuring the privacy and traceability of vehicles. Zhang et al. [19] tested the scheme under the random oracle model and proved that it is secure. Their scheme allows for device-to-device (D2D) communication without the involvement of a base station when two communicating devices are within a short distance of each other. This significantly improves the spatial efficiency, energy efficiency, throughput, fairness, and latency of the scheme. Experimental results showed that their scheme takes 0.9116 ms to verify a single signature with an average communication overhead of 144 bytes.

Liao et al. [20] proposed a security-enhancing scheme for MEC systems that includes a physical authentication layer based on deep learning (DL). This scheme detects spoofing attacks on the network using channel state information. Furthermore, to ensure improved efficiency with decreases

computational overhead and energy consumption, Liao et al. [20] considered expediting the learning process in the deep neural network using three gradient descent algorithms: gradient descent with momentum, root mean-squared drop, and adaptive moment estimation. Experimental results showed that their proposed scheme can identify multiple edge nodes and can differentiate between legitimate and malicious nodes. The maximum rate of authentication of their method was 97.75% with the Adam optimizer. However, Liao et al. [20] focused more on the learning rate than the level of privacy of the data.

Rasheed et al. [21] proposed a privacy-preserving network protocol based on edge computing. It mainly aims to increase the security of vehicular networks. Their model is based on creating an improved certificate-less aggregation sign-cryption scheme (iCLASC) and integrating the protocol for information transmission into it to generate monitoring data on roads. The main components of the security protocol in the model are confidentiality, anonymity, privacy, integrity, and joint authentication. Rasheed et al. [21] improved on a previous model proposed by Basudan et al. [22]. Their main contributions include minimization of pairing operations using the efficient Weil/Tate pairing and quick reduction of elliptic curves. Rasheed et al. [21] compared their method with four other methods in terms of the times needed for pairing, multiplication, and exponentiation. The results showed that their method took the shortest time on average (15.1 ms) for both sign-cryption and unsign-cryption phases. However, they did not provide any analysis on the storage-related requirements and did not explain whether the public key was to be saved on mobile devices.

Gope et al. [23] proposed a privacy-aware authentication scheme for edge-assisted UAVs. Their solution is primarily based on inexpensive cryptographic methods: the physically unclonable function (PUF) and the one-way hash function. They aimed to provide an authenticated key agreement protocol. Their protocol is designed to be mainly used by service providers to verify the identity of EUs, specifically the identity of UAVs without compromising their privacy. Their scheme does not require a secret key to be stored in any device. This method incurs a low cost and provides good security-related features. Gope et al. [23] compared their method with three other methods proposed in literature in terms of communication-related and computational overheads as well as execution time. The comparison results showed that their method had a shorter computation time (4.96 ms) than the other methods considered (5173 ms). However, the PUF method used in this scheme is vulnerable to many attacks, such as machine-learning-based attacks. Gope et al. [23] did not adequately analyze the robustness of their method against security attacks, because of which it cannot be used to process critical information [24].

Rahman et al. [25] proposed an MEC framework that can serve crowded regions, such as the annual pilgrimage by Muslims to Mecca (the Hajj). Their framework aims to provide knowledge of each pilgrims' context, such as their geographical location at a given time of day, to help find them if they are lost and provide them information on important nearby locations, such as the nearest clinic or hospital, grocery store, and mosque. Their scheme uses a cloud on the server side and a fog computing terminal on the crowded edge side. The location of each mobile user is shared and secured according to a privacy scheme developed by Rahman et al. [25]. A mobile user's information is encrypted using the symmetric Advanced Encryption Standard (AES) algorithm with a 256-bit key. The key is changed for every new message shared between users. AES keys are locally stored in each pilgrim's phone and are secured with an extra layer of encryption that uses the passphrase method. To further enhance security, Rahman et al. [25] used two-way authentication based on the user's mobile number. They integrated D2D communication into the system for emergency situations to provide more efficient communication in crowded places. Additionally, they measured the response time of the server in their scheme for multiple types of applications. The results showed that the worst-case scenario involved a

response time of 2 min, and the switching to the D2D mode drastically reduced this time to the order of seconds. Disadvantageously, the encryption method adopted in their scheme, AES with a 256-bit key, requires considerable storage and intensive processing, which are not suitable for lightweight mobile devices.

Li et al. [26] considered the problem of ensuring privacy in edge computing and proposed an efficient edge-based privacy-preserving scheme for the energy Internet. Their scheme utilized both the ZSS short signature algorithm and Pilliar homographic cryptography to preserve privacy. Li et al. [26] conducted a security analysis of their scheme by considering its capabilities in privacy preservation, confidentiality, authentication, and integrity. Furthermore, they performed simulations to evaluate its computational complexity and communication overhead in comparison to three prevalent schemes. The results showed that the communication overhead of their scheme is $2448(N + 1)$ bits, where N represents the number of users ranging from zero to 2,000. The time complexity of the proposed scheme is $T = N * 2(2.528) + N * (0.111) + 2(114.628) + (N + 1) * TZSS$, where N is the number of users and TZSS is the time required for the ZSS signature by a user. The comparison results showed that the scheme of Li et al. [26] has lower time complexity and communication overhead than the other three models considered. However, the use of the Pilliar cryptosystem increases the time required to decrypt the data because the generated cipher text is longer than the corresponding plaintext. This also increases the storage-related requirements of the system.

The above literature review shows that various mechanisms can be employed to ensure privacy in the MEC environment. However, the abovementioned studies have not considered efficiency-related requirements for using UAVs in the MEC environment. UAVs have limited operation time and power and cannot be used to perform complicated tasks while ensuring data privacy. Thus, a new scheme is needed that can satisfy the requirements related to the use of UAVs in the MEC environment. To tackle this challenge, an authentication scheme is proposed in the next section.

3 Proposed Authentication Scheme

The proposed scheme is a hardware-based password-less authentication scheme based on the concept of public key cryptography. This section briefly explains the overall mechanism of the authentication process along with the required interactions between the users of the system.

The proposed authentication mechanism comprises four main stages: system initialization, EU registration, EU authentication, and session establishment.

3.1 System Initialization

At the outset, the UAV initializes the system parameters and makes them available to all parties involved in the system. The system parameters are as follows:

- domain of numbers (finite field);
- privacy policy, including the personal information needed in the system and the manner in which it is maintained, processed, and kept private;
- mechanism of random number generation; and
- session duration (MAX_TIME).

3.2 EU Registration

This stage is intended to provide the UAV with the identity of all EUs that belong to its area of coverage. It is executed for each EU in the system only once before it starts authenticating itself and communicating with the UAV. Fig. 2 illustrates the flow of the registration stage.

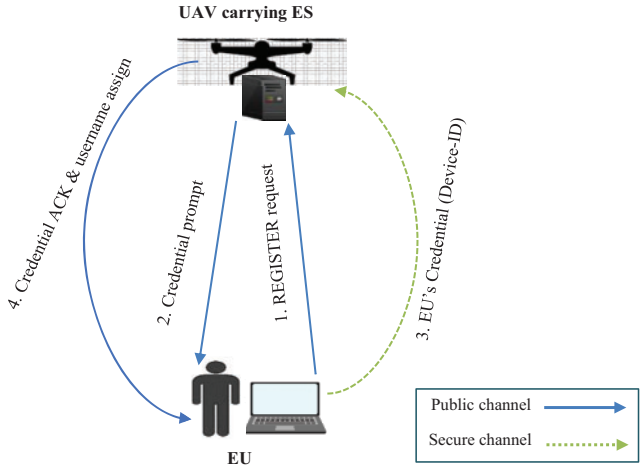

Figure 2: EU registration stage

Fig. 2 shows the following:

- The registration stage starts when the UAV receives a registration request from an EU.
- The UAV then prompts the EU to send their credential, which is the device ID, through a secure channel.
- The EU subsequently sends the credentials to the UAV through a secure channel.
- Upon receiving the credential, the UAV sends an acknowledgement message along with an assigned username to the EU. The registration process ends here.

When all users have been registered, the ES compiles a list (usernames, IDs) for all EUs belonging to its area of coverage. The ID of a user is never shared over the network.

3.3 EU Authentication

This stage is executed when an EU wants to communicate with a UAV or when an established session expires while the EU has still not finished communicating with UAV. It is fundamental to the proposed scheme. Fig. 3 provides an overall picture of the EU authentication mechanism.

Fig. 3 shows the following:

- The authentication stage starts when an EU sends their username as an authentication request to the UAV.
- Upon receiving the username, the UAV searches for the credentials associated with it. If the credentials do not exist, the UAV sends an "invalid user error" to the EU and the process stops.
- If the credentials exist, the UAV generates a random number (Rn) using the linear-feedback shift register (LFSR) algorithm (described in Section 3.3.1), and feeds it along with the found ID into the authentication algorithm (described in Section 3.3.2) to calculate a certain value, called X, that should only be kept on the UAV side.
- The UAV sends Rn to the EU over the network.

- The EU uses Rn along with its own device ID to generate the value X∗ similar to the way in which X is generated on the UAV side.
- The EU sends X∗ to the UAV.
- The UAV subsequently compares the received value with X; if X∗ = X, the authentication succeeds; otherwise, the authentication fails and the system aborts.
- The UAV sends an "Authentication Success" message to the EU, which indicates the end of the authentication process and the beginning of the session establishment stage.

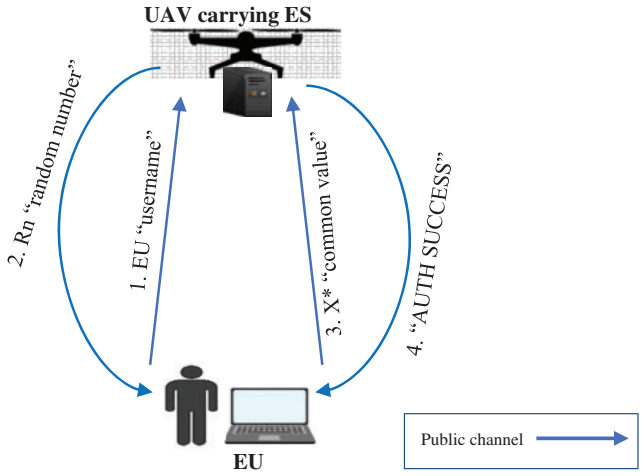

Figure 3: One-way authentication of the EU

3.3.1 Random Number Generation

The random numbers used in our proposed scheme are all 256 bits long. To generate such a sequence of numbers, a 256-bit LFSR is used. The following function [27] is used to ensure a long period (maximum possible sequence of numbers before any of them is repeated), where the symbol ⊙ represents the XNOR function:

$$b_{168} = (b_{168} \odot b_{166}) \odot (b_{153} \odot b_{151}) \tag{1}$$

Using Eq. (1), the LFSR obtains a 168-period length. This denotes that the number generated at any time is between 1 and $2^{256} \approx 1.158 \times 10^{77}$ and is different from at least the 168 numbers previously generated.

3.3.2 Authentication Algorithm

The proposed authentication algorithm is denoted in the pseudo-code as Algorithm 1.

Algorithm 1: AUTHENTICATION (ID, Rn)

Inputs: ID: 256-bit user ID (secret value)
Rn: 256-bit random number (public value)
Output: Res: the response of authentication based on the shared Rn and the secret ID
1. *userID* ← *Integer Array* [0 . . . 255]
2. *rand* ← *Integer Array* [0 . . . 255]

(Continued)

Algorithm 1: Continued

```
3.  Res ← Integer Array [0 . . . 255]
4.  userID = ID
5.  rand = Rn
6.  j = 192
7.  for i = 0 to 63 //calculating block-1 of Response by XORing block-1 of rand with block-4 of userID
8.      Res[i] = rand[i] ⊕ userID[j]
9.      j = j + 1
10. End for
11. j = 128
12. for i = 64 to 127 //calculating block-2 of Response by XORing block-2 of rand with block-3 of
    userID
13.     Res[i] = rand[i] ⊕ userID[j]
14.     j = j + 1
15. End for
16. j = 64
17. for i = 128 to 191 //calculating block-3 of Response by XORing block-3 of rand with block-2 of
    userID
18.     Res[i] = rand[i] ⊕ userID[j]
19.     j = j + 1
20. End for
21. j = 0
22. for i = 192 to 255 //calculating block-4 of Response by XORing block-4 of rand with block-1 of
    userID
23.     Res[i] = rand[i] ⊕ userID[j]
24.     j = j + 1
25. End for
26. Return Res
```

Fig. 4 displays the logic diagram of the hardware. The hardware unit takes a unique identification number (Device ID) as one input and a random number as another input to yield an output. The process is implemented both on the server and the client. The server receives the output (response) from the client and compares it with the output at its end. The results of the two have to be identical for successful authentication.

Fig. 5 presents a simplified example of the way to calculate the response, where the size of both the inputs and output is set to 64 bits instead of the actual size of 256 bits used in our system. Each input/output is divided into four blocks and each block is 16 bits long. The inputs are assumed to be as follows:

ID = 1110110001111010101111100001000011111010101010101010101111110000

Rn = 0011001001010101010110011001101001111111111110000111100001101010

The steps shown in Fig. 5 are performed to calculate the output (response), that is,

Res = 1001010000010000110000011110100010100011001100001001100110100101

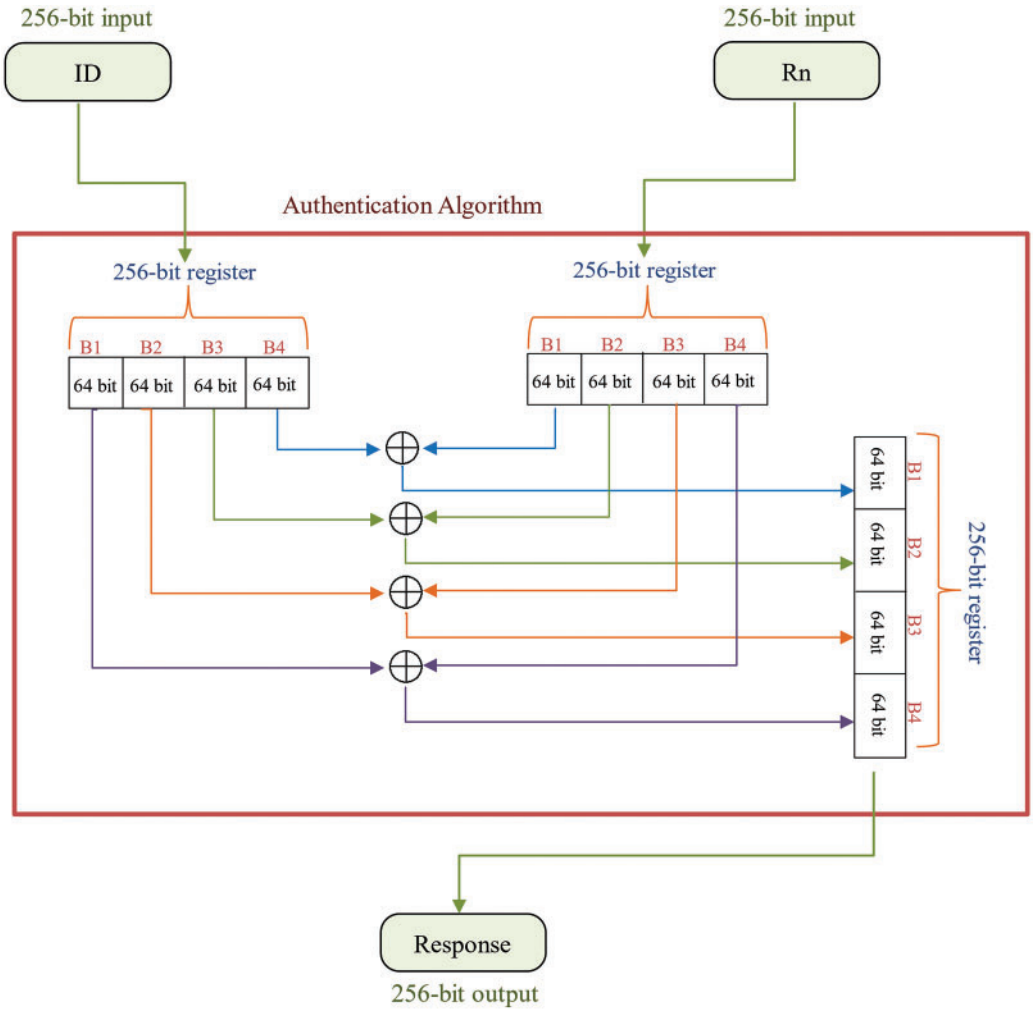

Figure 4: Hardware logic diagram of the proposed authentication algorithm

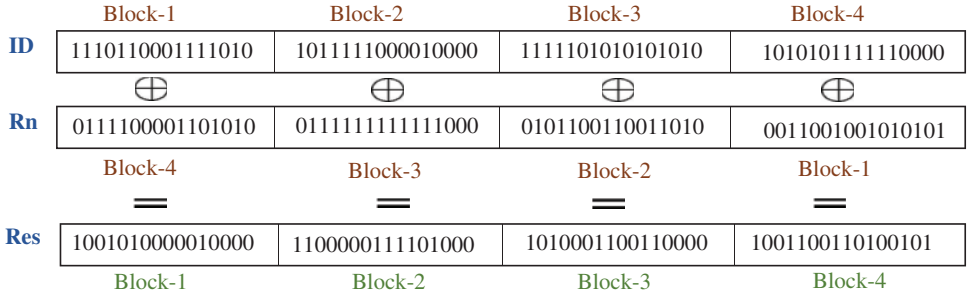

Figure 5: Example of the authentication response calculation

An adversary cannot obtain the Device ID from the random number (Rn) and the derived Response (Res) because the numbers are not XORed bit by bit. Instead, for example, the least significant block of the random number is XORed with the most significant block of the response,

as shown in Fig. 4. This arrangement is one of the numerous possible ways and the actual choice remains private.

3.4 Session Establishment

After successful EU authentication, the session establishment stage commences. In this stage, the EU can share data with the corresponding UAV for a specified period. Fig. 6 briefly illustrates the session establishment stage.

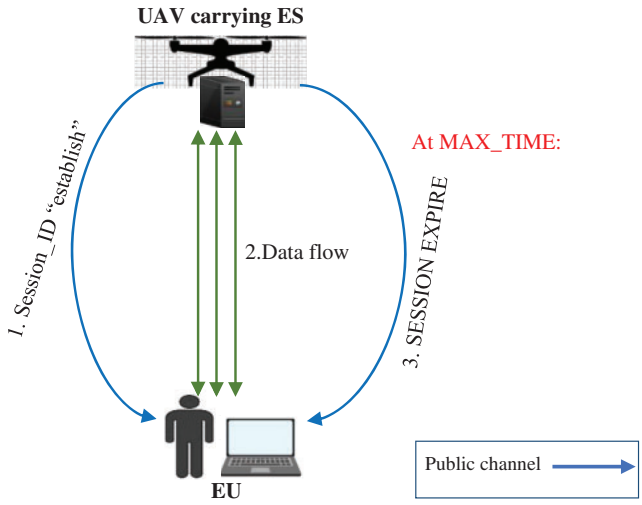

Figure 6: Session establishment stage

Fig. 6 shows the following:

- Upon successful authentication, the UAV generates a session ID and sends it to the corresponding EU to signify the establishment of a session.
- The UAV starts a timer for the session.
- Upon receiving the session ID, the EU starts sending its data to the UAV, and vice versa.
- When the timer reaches a predefined maximum session duration (MAX_TIME), the session expires, a session expiry message "SESSION EXPIRED" is sent to the EU, and re-authentication is required to continue the communication.

4 Simulations

To assess the performance of our proposed authentication scheme, simulations are conducted to analyze its running time and memory consumption. The program is coded on the MATLAB R2022a platform. An Intel(R) Core(TM) i7 processor with a clock speed of 2.59 GHz and 12 GB of RAM is used.

4.1 Software Simulation

The authentication algorithm and the method of random number generation (LFSR) are coded in separate functions and are linked in a single program. This allows the precise and separate measurement of the performance of each method.

Due to the effects of uncontrolled factors on the execution time and memory consumption of the program (e.g., processes running in the background and caching of memory), different executions of the same code yield different execution times and amount of memory consumed. The average running time and memory consumption over 20 executions are calculated. Fig. 7 displays the execution times for the proposed scheme in these 20 runs.

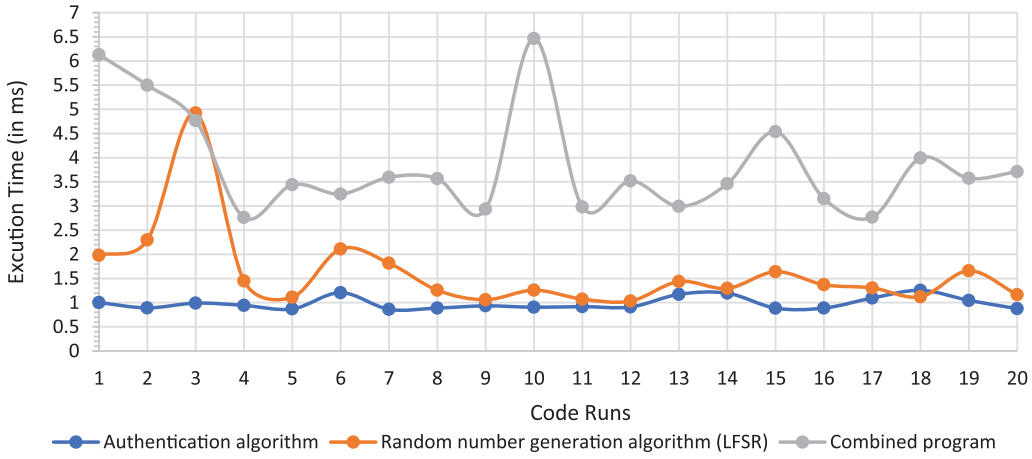

Figure 7: Execution time of different runs of the proposed system

The data shown in Fig. 7 are used to calculate the average execution time of the authentication algorithm, LFSR, and the combined program, which are 0.986, 1.618, and 3.854 ms, respectively.

Similarly, to obtain the average memory consumption of the proposed method, the average of 20 runs is calculated and plotted in Fig. 8. The average memory consumed by the authentication algorithm, LFSR, and the combined program are 34, 34.8, and 40.2 KB, respectively.

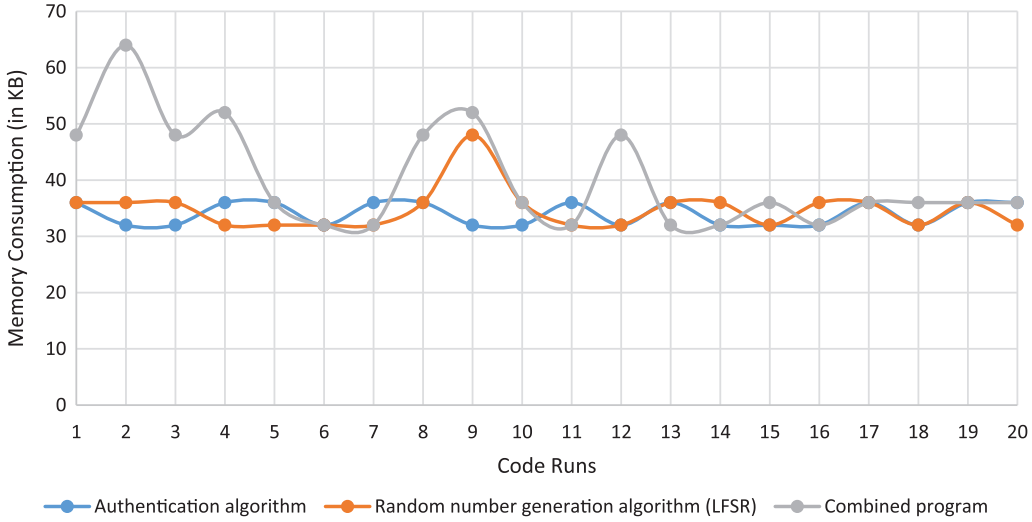

Figure 8: Memory consumption in different runs of the proposed system

4.2 Results

Table 1 summarizes the average running time of each method of the proposed system along with the average memory consumed.

Table 1: Time and memory requirements of the proposed scheme

Method	Authentication algorithm	LFSR	Combined program
Average software execution time	0.986 ms	1.618 ms	3.854 ms
Average memory consumption	34 KB	34.8 KB	40.2 KB

The above results only present the results of the software simulation of the proposed scheme. However, as mentioned above, the proposed scheme is to be implemented as a hardware-based system, and only one hardware clock cycle is required to compute the output because all the XOR operations are performed in a single clock period.

In this implementation scenario, the employed computer has a clock speed of 2.59 GHz. Consequently, the clock time is

$$\text{Clock time } = \frac{1}{clock\ speed} = \frac{1}{2.59\ \times 10^{9}} \approx 0.386\ \times\ 10^{-9}\ \text{s} \approx 0.39\ \text{ns} \tag{2}$$

Therefore, the hardware execution time of the proposed authentication algorithm is approximately 0.39 ns.

5 Analysis of Proposed Authentication Algorithm

The above results show that the proposed authentication algorithm has a very short execution time, which satisfies the requirements of the temporal efficiency of the UAV-assisted MEC environment.

The performance comparison of the proposed algorithm with the methods discussed in Section 2 shows that the shortest execution time among the previous methods [19] is 0.91 ms, while that of the proposed scheme is 0.39 ns as depicted in Eq. (3). Thus, the scheme has a significantly shorter execution time than prevalent methods in the area. Particularly, the runtime was reduced from the order of milliseconds to that of nanoseconds using the hardware-based implementation of the proposed algorithm.

The average memory consumption of the proposed authentication algorithm is 34 KB, which is significantly less than that of the methods described in Section 2.

For an attacker to overcome the proposed scheme, they need to first break the authentication algorithm and then guess the private parameter and/or the random number. However, both the numbers are 256-bit long. For an attacker to guess these numbers, the number of required trials ($T_{brute-force}$) is given by

$$T_{brute-force} = 2^{256} \approx 1.158 \times 10^{77}\ trials \tag{3}$$

This is extremely huge and accordingly Eq. (3) proves that the proposed scheme is resistant to brute-force attacks.

6 Conclusion

UAV-assisted MEC is a powerful architecture that utilizes the flexibility of UAVs to improve the performance of the MEC architecture by providing better coverage, higher security, and optimized adjustments to the location of ESs based on the changing locations of the end devices involved. However, concerns have recently been raised regarding the energy consumption, storage-related requirements, time constraints, and the privacy of people's data in terms of the use of UAV-assisted MEC. This study investigated prevalent authentication schemes applicable to UAV-assisted MEC systems and proposed an effective and efficient authentication scheme for UAV-assisted MEC that reduces the computational overhead and minimizes the processing delays while ensuring a high level of privacy of the data.

The proposed scheme uses a hardware-based password-less method of authentication that comprises four main stages: system initialization, EU registration, EU authentication, and session establishment. The efficiency and security of the proposed scheme were tested in terms of the time taken and its memory-related requirements. The experimental results showed that it consumes an average of 34 KB of memory and can execute one clock cycle in 0.39 ns. Moreover, it has a shorter run time than all prevalent schemes in the area. The scheme may be extended to develop a complete authentication and encryption system based on a hardware chip that can be embedded in MEC devices.

Funding Statement: This work was funded by the Deanship of Scientific Research of King Faisal University through research project (Grant Number GRANT228).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the publication of this study.

References

[1] V. Stephanie, M. A. P. Chamikara, I. Khalil and M. Atiquzzaman, "Privacy-preserving location data stream clustering on mobile edge computing and cloud," *Information Systems*, vol. 107, pp. 101728, 2021.

[2] Q. Wu, K. He and X. Chen, "Personalized federated learning for intelligent IOT applications: A cloud-edge based framework," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 35–44, 2020.

[3] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu *et al.,* "Edge computing security: State of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.

[4] Y. Yazid, I. Ez-Zazi, A. Guerrero-González, A. El Oualkadi and M. Arioua, "UAV-enabled mobile edge-computing for IOT based on AI: A comprehensive review," *Drones*, vol. 5, no. 4, pp. 148, 2021.

[5] Z. Ali, S. Khaf, Z. Haq Abbas, G. Abbas, L. Jiao *et al.,* "A comprehensive utility function for resource allocation in mobile edge computing," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1461–1477, 2021.

[6] G. Avellar, G. Pereira, L. Pimenta and P. Iscold, "Multi-uav routing for area coverage and remote sensing with minimum time," *Sensors*, vol. 15, no. 11, pp. 27783–27803, 2015.

[7] T. Wang, R. Qin, Y. Chen, H. Snoussi and C. Choi, "A reinforcement learning approach for UAV target searching and tracking," *Multimedia Tools and Applications*, vol. 78, no. 4, pp. 4347–4364, 2018.

[8] Y. Xu, T. Zhang, Y. Liu, D. Yang, I. Xiao *et al.,* "UAV-assisted MEC networks with aerial and ground cooperation," *IEEE Transactions on Wireless Communications*, vol. 20, no. 12, pp. 7712–7727, 2021.

[9] S. van Engelenburg, M. Janssen and B. Klievink, "Designing context-aware systems: A method for understanding and analysing context in practice," *Journal of Logical and Algebraic Methods in Programming*, vol. 103, pp. 79–104, 2019.

[10] L. Gupta, R. Jain and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.

[11] M. J. Neely, "Intelligent packet dropping for optimal energy-delay tradeoffs in wireless downlinks," *IEEE Transactions on Automatic Control*, vol. 54, no. 3, pp. 565–579, 2009.
[12] H. Yu and M. J. Neely, "A new backpressure algorithm for joint rate control and routing with vanishing utility optimality gaps and finite queue lengths," *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1605–1618, 2018.
[13] G. Sharma, R. Mazumdar and N. Shroff, "Delay and capacity trade-offs in mobile ad hoc networks: A global perspective," in *Proc. IEEE INFOCOM 2006–25th IEEE Int. Conf. on Computer Communications*, Barcelona, Spain, 2006.
[14] M. Zhoujia, C. E. Koksal and N. B. Shroff, "Near optimal power and rate control of multi-hop sensor networks with energy replenishment: Basic limitations with finite energy and data storage," *IEEE Transactions on Automatic Control*, vol. 57, no. 4, pp. 815–829, 2012.
[15] Y. Wang, Z. -Y. Ru, K. Wang and P. -Q. Huang, "Joint deployment and task scheduling optimization for large-scale mobile users in multi-UAV-enabled mobile edge computing," *IEEE Transactions on Cybernetics*, vol. 50, no. 9, pp. 3984–3997, 2020.
[16] J. Yang, J. Chen and Z. Yang, "Energy-efficient UAV communication with trajectory optimization," in *2021 2nd Int. Conf. on Big Data and Artificial Intelligence and Software Engineering (ICBASE)*, Zhuhai, China, pp. 508–514, 2021.
[17] Z. Zhang, F. Xu, Z. Qin and Y. Xie, "Resource allocation in UAV assisted air ground intelligent inspection system," *Cognitive Robotics*, vol. 2, pp. 1–12, 2022.
[18] X. Wang, X. She, L. Bai, Y. Qing and F. Jiang, "A novel anonymous authentication scheme based on edge computing in internet of vehicles," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3349–3361, 2021.
[19] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu *et al.,* "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7940–7954, 2020.
[20] R. -F. Liao, H. Wen, J. Wu, F. Pan, A. Xu *et al.,* "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116390–116401, 2019.
[21] I. Rasheed, L. Zhang and F. Hu, "A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing," *Computer Networks*, vol. 176, pp. 107283, 2020.
[22] S. Basudan, X. Lin and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, 2017.
[23] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13621–13630, 2020.
[24] A. Babaei and G. Schiele, "Physical unclonable functions in the internet of things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, pp. 3208, 2019.
[25] A. Rahman, E. Hassanain and M. S. Hossain, "Towards a secure mobile edge computing framework for Hajj," *IEEE Access*, vol. 5, pp. 11768–11781, 2017.
[26] K. Li, X. Han, Y. Yang, S. Wang, R. Shi *et al.,* "A novel edge computing offloading and privacy-preserving scheme for energy internet," in *2021 IEEE 5th Int. Conf. on Cryptography, Security and Privacy (CSP)*, Zhuhai, China, pp. 79–83, 2021.
[27] P. Alfke, *Efficient shift registers, LFSR counters, and long pseudo-random sequence generators*. XAPP052 July 7, 1996. [Online]. https://docs.xilinx.com/v/u/en-US/xapp052