21. Yüzyılda Fen ve Teknik Dergisi

ISSN: 2587-0327
Research Article / Araştırma Makalesi

2023, Cilt/Volume: 10, Sayı/Issue: 19, 9-17
Geliş Tarihi / Received: 23.05.2023
Kabul Tarihi /Accepted: 27.06.2023

A New Blockchain-Based Authentication Infrastructure For Wireless Networks: BCAUTH

Remzi Gürfidan[1*], **Enes Açıkgözoğlu**[2]

Abstract: Authentication in wireless networks is the process of verifying the identity of users to authorize them to access the wireless network. This process is critical to ensure network security and prevent unauthorized access. Access to wireless networks carries the risk of unauthorized persons interfering with the network, accessing sensitive data, or engaging in malicious activities on the network. Authentication ensures that only authorized users can access the network and helps prevent security vulnerabilities. The inability of unauthorized access to the network prevents data traffic from being monitored and malicious actors from stealing data. Authentication helps manage network resources effectively. Unauthorized users accessing the network can degrade network performance and lead to inefficient use of resources. Authentication increases network efficiency by ensuring that only authorized users can access network resources. The fact that blockchain technology has proven itself in data security is quite suitable for combining it with such a critical area as authentication. In this study, an authentication system with the help of smart contracts is connected to a blockchain infrastructure and executed. The performance tests of the proposed model are rigorously performed and discussed.

Keywords: Blockchain, wireless network authentication, secure authentication, smart contract authentication.

[1]**Address:** Isparta University of Applied Science, Yalvac Technical Sciences Vocational School, Isparta, Türkiye.
[2]**Address:** Isparta University of Applied Science, Keçiborlu Vocational School, Isparta, Türkiye

***Corresponding author**: remzigurfidan@isparta.edu.tr

Citation: Gürfidan, R., Açıkgözoğlu, E. (2023). A New Blockchain-Based Authentication Infrastructure for Wireless Networks: BCAUTH. 21. Yüzyılda Fen ve Teknik Dergisi, 10(19):9-17.

1.INTRODUCTION

Wireless networks are one of the most popular methods of providing internet connectivity. Wireless networks communicate and exchange information between computers, phones, and other devices. However, vulnerabilities can occur during this communication and can lead to data theft and other cyber-attacks by malicious users. The widespread use of wireless networks with rapidly developing technologies has revealed the need to authenticate the identity of devices connected to the network. Authentication is the most important and challenging way to secure wireless networks in organizations. With authentication, devices that want to connect to the network are taken into the wireless network environment through a series of processes and their access status to network services is decided. In this way, a more secure and sustainable network is created (Henry and Luo, 2002; Dantu, Clothier and Atri, 2007).

Authentication is a process used to verify the credentials (such as username and password) of a user who wants to connect to a wireless network. Authentication protects against data theft and other cyber-attacks by preventing unauthorized access to wireless networks. Authentication alone is not enough to secure wireless networks. Additional security measures, such as encryption and firewalls, can help make wireless networks more secure. However, authentication plays a fundamental role and is an important step in securing wireless networks. Authentication is when users pass an audit and prove their authenticity before joining a network. The user's identity data (username, password, etc.) is stored in a database. The data transfer between the information provided by the user to join the network and the server to verify the data must also be encrypted for data security. Authorization determines which operations users can perform on the network they join after successful authentication (Yildirim *et al.*, 2021).

The WEP protocol was first developed to ensure the security of wireless networks. Identity control cannot be provided with the WEP protocol, which can be easily broken and has security weaknesses. After the WEP protocol, the WPA protocol was developed to eliminate all the weaknesses of the Web. When the TKIP encryption used with the WPA protocol also became crackable by attackers, the WPA2 protocol was developed. WPA2 uses CCMP-AES as a security protocol and CBC-MAC to ensure data integrity (*(PDF) Securing UMaT Wireless Network Using pfSense Captive Portal with Radius Authentication*, no date). IEEE 802.1.x provides a port-based mechanism that provides authentication and authorization mechanisms for connecting devices to a wireless network (Chen and Wang, 2005). Figure 1 shows an authentication messaging used for 802.1x.

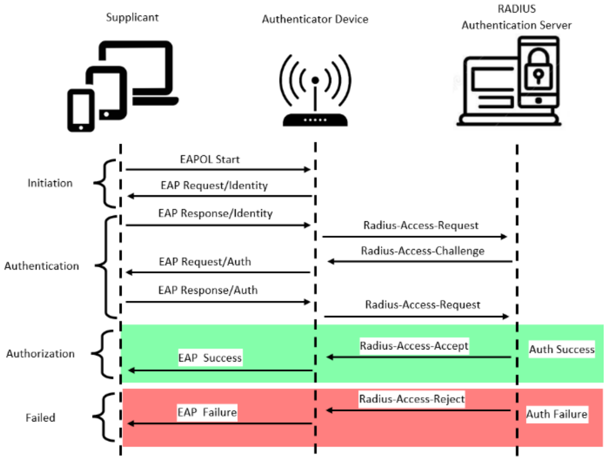


Figure 1. 802.1x user authentication steps

Table 1. Wireless network authentication protocols (*Kablosuz Ağlarda Şifreleme, Kimlik Doğrulama ve Güvenlik Önlemleri*)

802.11 Standard	**Auth.**	**Encryption**	**Encryption Algorithm**	**Key Generation Method**
WEP	Open/Shared Key	WEP	RC4 (24 Bit)	Static
WPA	PSK	TKIP	RC4 (48 Bit)	Dynamic
WPA2	PSK	CCMP	AES	Dynamic
WPA	802.1x	TKIP	RC4 (24 Bit)	Dynamic
WPA2	802.1x	CCMP	AES	Dynamic

Authentication of users is one of the basic procedures used to ensure secure communication over an insecure wireless network. To secure wireless network systems, it is necessary to use effective and simple authentication methods. Authentication methods using usernames and passwords provide the basic components to prevent unauthorized access and ensure network security (Liao and Lee, 2010). AAA is used as an acronym for authentication, authorization, and accounting. Authentication is the process of controlling a user's access to a network with valid credentials. Authorization controls access for each user after the user has been authenticated and controls the privileges, services and commands that belong to the user. Accounting monitors network traffic passing through the firewall and provides a record of the user's activities (Alabady, 2008). The TACACS+ protocol is a Cisco proprietary protocol that provides access control for network routers, network access servers, and other network computing devices through one or more centralized servers. TACACS+ provides AAA services for Authentication, Authorization, and Accountability, respectively. Authentication is the process of determining who the user (or agent) is and checking that the agent is the correct agent to access the network. Most computer systems use a username and a fixed password authentication mechanism, TACACS+ also uses the same approach for authentication. However, fixed passwords have several security threats and drawbacks (Pradeep *et al.*, 2019). Kerberos is a distributed authentication service that allows a client to verify its identity from a server or application server without sending data over the network. Kerberos provides optional integrity and confidentiality of data sent and received between client and server. Developed in mid-1980 as part of the Ahtena Project, Kerberos is now in its 5th version, supported by new usage models and policies as its use has expanded. Version 5 of the Kerberos authentication service is considered the standard Kerberos (Neuman and Ts'o, 1994). 802.1X provides a secure and flexible authentication mechanism that facilitates dynamic virtual private network (VLAN) assignment to users. Dynamic network assignment provides security, performance and mobility through the division of the network into multiple broadcast domains. 802.1X consists of three elements, the purpose of which is to restrict unauthorized devices from accessing the network (Benzekki, El Fergougui and El Belrhiti El Alaoui, 2016).

- Client: It is the device that wants to access the wired or wireless network by sending its credentials to the authenticator. The data between the client and the authentication mechanism is held and encapsulated by EAP.

- Authenticator: Devices located between the client and the authentication server. It is usually a switching device or a wireless access point. The main role of this component is to receive credentials from the requester and transmit them to the Authentication Server. It is usually based on the RADIUS protocol.

- Authentication Server: A server that serves to authenticate one or more clients based on the credentials provided to it. It needs a local database to check and verify credentials.

Authentication systems in wireless networks are potentially vulnerable to cyber-attacks. Malicious actors use various methods to access authentication systems and connect to the wireless network without authorization. Therefore, authentication systems used in wireless networks must be designed to be secure and protected against cyber-attacks. Some types of cyber-attacks are direct attacks on authentication systems. For example, brute-force attacks are when an attacker uses an automated program to try username and password combinations. This type of attack is used to obtain a user's credentials. Another type of cyber-attack is sniffing attacks, where an attacker listens and records traffic on a wireless network. This type of attack means that an attacker listens to traffic on a wireless network and captures sensitive information such as usernames and passwords. Some attacks can target vulnerabilities in authentication systems. For example, an attacker may find a vulnerability in a protocol used to connect to a wireless network and use this vulnerability to bypass the authentication system.

We would like to explain our motivation for this study in bullet points. In this way, we hope that the purpose and goals of our work will be better understood.

- The reason for using blockchain for authentication on the network is to provide a secure and decentralized authentication process. Blockchain technology is distributed, and each transaction is recorded in a block with other transactions. Each of these blocks is linked with other blocks to increase security and form a whole. Therefore, blockchain technology can provide a secure and decentralized authentication process that is difficult to manipulate.

- Blockchain technology can be used to securely manage the authentication process. This technology can provide users with a unique identity that will help them protect their personal information and prove the authenticity of their identity. Using these identities, users can interact with other users on the network without the need for any centralized authority.

- Blockchain technology also provides greater security by recording the authentication process along with other transactions on the network. Authentication transactions are recorded on the blockchain and cannot be modified retrospectively. Therefore, because it is recorded along with other transactions on the network, any authentication fraud is detected, and transactions can be reversed.

- As a result, blockchain technology provides a decentralized authentication process and provides greater security by recording it along with other transactions on the network. Therefore, authentication on the network with blockchain is an important step to create a more secure network environment.

The second section of the paper describes how authentication methods are provided, how they have been integrated into new technologies over time, and the need for new approaches in this area. The third section describes the technical infrastructure used in the new authentication model proposed in this paper, the smart contract details, and pseudo codes. The fourth section evaluates the proposed model in terms of performance criteria and discusses the results obtained. In the last section of the paper, all the data are evaluated together, and the experience gained from this study and the future vision of this study are described.

2. RELATED WORKS

Network authentication has become one of the most critical and widespread areas of study with the widespread use of Internet services. User authentication methods have been developed for many different purposes and concepts and have been enhanced and improved with new technologies over time. The next enhanced method shows how it overcomes the shortcomings of previous works or hints at vulnerabilities. Researchers have made comparisons on securing an enterprise wireless network using WPA2 based PEAP MS-CHAP and Captive portal. They separated the employee and visitor networks to increase the security level on the corporate wireless network. As a result of the study, they showed that the wireless network can be cracked using attack tools such as airodump, aireply and aircrack (Soewito and Hirzi, 2014). When the causes of these vulnerabilities are analysed in detail, it has been shown that they are due to the incorrect or incomplete application of the methods put forward over time. To overcome this problem, researchers have focused on informational studies. For example, documents and articles were prepared to explain how to use Active Directory, Captive Portal applications and pfSense firewall to manage the authentication process of users on a university's wireless network (*(PDF) Securing UMaT Wireless Network Using pfSense Captive Portal with Radius Authentication*, no date).

The increase in the number of portals using the Internet and the increase in the technical needs of the users naturally creates serious problems. To solve this problem, research has been carried out on the technical and basic requirements for meeting the broadband needs of users that will arise from the use of wireless networks in public areas after home and work environments, and solution approaches have been discussed (Henry and Luo, 2002). Researchers have further explored real-time approaches that simulate situations in outdoor and indoor networks. In a case study, taking a campus network as an example, a portal application running at OSI Layer 2 within the campus area was developed. The developed application was subjected to different tests in the Eve-Ng virtualization environment and simulated user registration, user authorization and internet access(Yildirim *et al.*, 2021)].

With personal data protection rights, GDPR laws, and the legal determination of user responsibilities in internet services provided to the masses, authentication methods have become more important in the use of wired and wireless internet services and studies in these areas have gained popularity. The researchers examined the widely used Extensible Authentication Protocol (EAP) protocols. They have also presented a literature review of authentication protocols. They examined the most widely used protocols of the EAP framework and the advantages and disadvantages of these protocols (Kumar and Gambhir, 2014). By characterizing the information on authentication systems as sensitive data, a new wireless network authentication protocol that provides user anonymity is proposed. In the study, symmetric encryption and decryption operations are performed for mobile users with hash function and smart cards. The most important feature of the work is the use of a one-time key between the user and the wireless network (Zhu and Ma, 2004). They identified the weakness of PairHand authentication phases and showed that the session key can be compromised under certain conditions. They proposed simple modifications to solve the security problems they identified without losing the security and efficiency of PairHand. They experimentally tested their implementation and showed that it can be used in real applications (He *et al.*, 2012). By classifying and comparing existing authentication techniques, the researchers aimed to make it easier for system designers to determine the appropriate technique for their computational, communication, and application requirements (Grover and Lim, 2015).

Mohsin et al. (2019) created a research environment with authentication using blockchain technology over the network and different authentication systems of various platforms using blockchain technology. With the research environment they created, they provided classified and useful information on how blockchain technology and various authentication systems can be combined. With the study, they emphasized the capabilities, importance, and challenges of blockchain technology used in various fields with different applications (Mohsin *et al.*, 2019). Hammi et al. (2018) proposed a decentralized system for verifying and identifying IoT devices called trust bubbles. The proposed system utilizes the security advantages of blockchain technology to protect data integrity and data availability. They developed a real implementation of the system using the Ethereum blockchain and C++ language (Hammi *et al.*, 2018). Lau et al. (2019) utilized blockchain technology to authenticate any device that will be included in the network in IoT networks. Using the features of the blockchain, they created digital identities of IoT devices and used these identities for the device authentication process. In this process, they proposed the Authenticated Devices Configuration Protocol (ADCP). They demonstrated all the results of the solution with a working application (Lau, Alan and Yan, 2019).

We briefly mentioned recent studies on authentication in wired and wireless networks in different methods and techniques. As the security, privacy, and immutability features of blockchain technology have become popular, it has contributed to alternative solutions to the authentication mechanisms implemented in previous years. Verification and access systems have been strengthened by contributing to the work done in previous years in various dimensions. Blockchain-based solutions have been proposed and implemented to carry out authentication and authorization processes in smart cities. The advantages of this method include the detection of malicious behavior and the removal of potential security violators from the infrastructure service (Esposito, Ficco and Gupta, 2021). Research on authentication and security in IoT (Internet of Thing) systems, which are frequently used in smart city infrastructures, is also becoming widespread. In these studies, Hyperledger Fabric infrastructure, which stands out with its powerful structure, was utilized. Among the advantages of the studies, simplicity and openness are emphasized compared to other studies (D. Li *et al.*, 2018). Another study for IoT networks presents the preliminary and initial conceptual design of a blockchain-based distributed IoT data network around urban transportation. It is believed that a vehicular network such as B-DRIVE powered by VANET can address some of the ongoing problems of current urban transportation and overcome security concerns (Zia, 2021).

Blockchain-based verification models carried out in the field of Wireless Sensor Network (WSN) have been evaluated in terms of security and performance criteria and introduced to the literature (Cui *et al.*, 2020). The security aspects and potential vulnerabilities of Vehicular Ad-hoc Networks (VANETs) technology, which is one of the current parallel comprehensive fields, have been realized in other researches and efforts have been made to provide solutions with blockchain-based authentication methods (Abbas *et al.*, 2021). The gap in this area has been identified by researchers and a new blockchain scheme based on a permissioned blockchain has been developed for secure road traffic data management (Diallo, Dib and Al Agha, 2022).

On 18.05.2023, 593 results were reached in the research conducted by selecting "topics" with the keyword "Authentication" and "Blockchain". According to the years, 468 articles, 47 papers, 2 book chapters and 78 review studies were reached from different disciplines and fields, with the oldest 2018 and the newest 2023. The data were analysed through author-citation-journal-journal-country-institution-keyword and abstract analysis. The content indexed in Web of Science was taken as a database. The keyword map in the research conducted in the literature is shown in Figure 2.

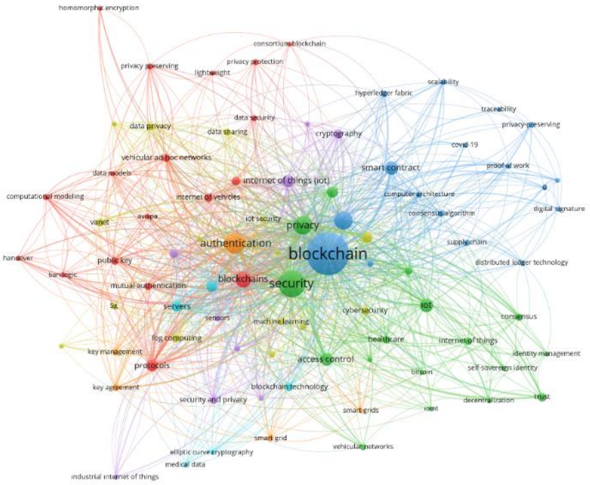


Figure 2. Authentication Literature Tree

A literature tree was obtained by examining the studies identified in the results of the literature search by adding the keywords "Architecture", "Architecture", "Method", "System", "Model", "Approaches", "Scheme", "Algorithm", provided that the keyword "Authentication" remains constant, and by grouping the studies carried out under these headings. This tree is shown in Figure 3. In the grouping made in the light of the scan findings, Smart Phone (Sahu *et al.*, 2018), Financial Sector (Ramya *et al.*, 2022), Smart City (Esposito, Ficco and Gupta, 2021; Ferreira *et al.*, 2021) leaves in the "New Architecture" branch, Commercial Online (Okada *et al.*, 2019), Telecommunication (Pan *et al.*, 2017; Muhammad and Safdar, 2018) leaves in the "New Method" branch, Broadcast (Yavuz, 2014) leaf in the "New System" branch, Internet of Energy (Kim, Yoo and Yoo, 2015; X. Li *et al.*, 2018), Telemedicine(Mir and Nikooghadam, 2015) leaves in "New Model" branch, AI (Liang *et al.*, 2020; Zhang *et al.*, 2022) leaves in "New Approaches" branch, Telemedicine (Guo *et al.*, 2019)] leaves in "New Scheme" branch, Social networks(Li *et al.*, 2017; Yu *et al.*, 2017) leaves in "New Algorithm" branch were identified.

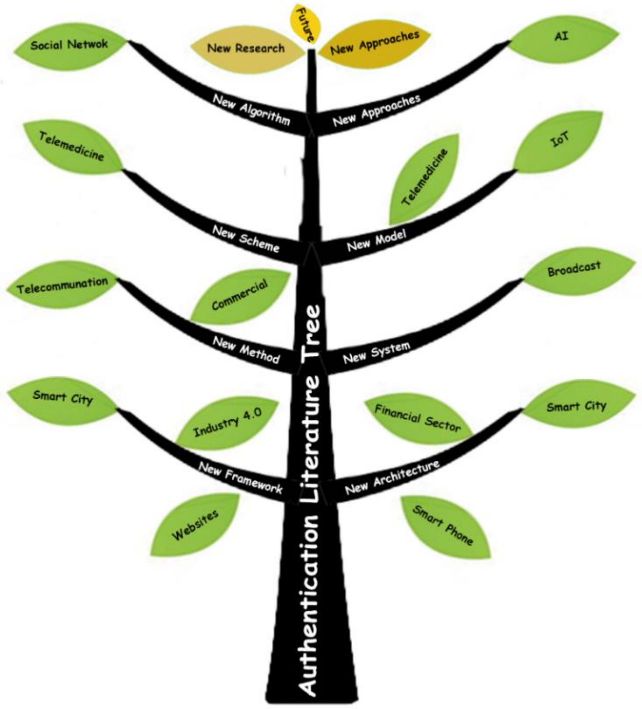


Figure 3. Authentication Literature Tree

3. PROPOSED MODEL

In this section, we will introduce a new infrastructure proposal that will change the functioning of the process that starts with the login panel used to log in to the systems in user interfaces. Let's examine the functioning of the system in stages. First, the user who wants to log in to the system must provide login information such as username, password, registration number, etc. to the interface with which they will interact. The type of hardware logged in can be a cell phone, tablet, laptop, or desktop computer. This device sends this information to the connected modem, server, or an internal firewall by applying its own security procedures. These security measures are usually realized with AES, TKIP or CCMP encryption methods. After this process, the upper service provider that receives the user information initiates the verification process by activating its own verification mechanisms. As a result of this verification process, rejection or approval information is returned. In addition, if the feedback is positive, the user authorization status can be determined on the system and added to the response. This verification mechanism works differently from standard systems. The main reason for this is that instead of a linear method such as a Radius-like verification mechanism, a blockchain-based system is proposed. This chain structure is a mechanism built on Hyperledger Fabric infrastructure and executed with smart contracts methods. Figure 4 shows the working mechanism of the proposed infrastructure.

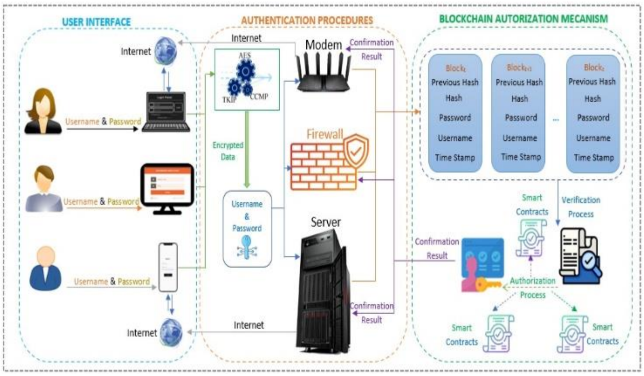


Figure 4. Blockchain-based authentication infrastructure architecture

The block chain structure consists of interrelated information rings that contain summary information of the previous block and are loyal to the distributed ledger technology. The input information received from the service provider is written into the previously issued smart contracts. First, verification is performed within the chain by means of smart contracts containing critical information. If the verification result is positive, the authorization protocol is activated again with smart contracts. The authorization information received from this unit is sent to the service provider with input confirmation. The service provider activates the necessary authorization arrangements and transfers information to the user hardware and the login process is completed.

With the realization of this infrastructure, manipulation processes that may occur in the verification server are prevented due to the nature of the blockchain, and eavesdropping attacks are eliminated due to the nature of smart contracts.

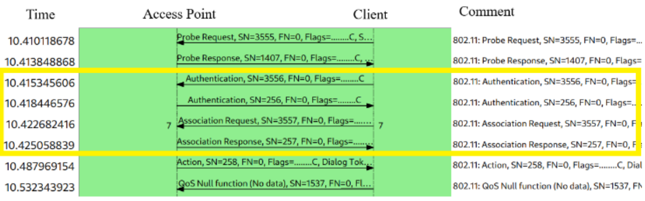
Algorithm 1 Smart Contract Pseudo Code

```
function initIdBook ()
    config IdBookStandarts ()
function CreateBookMember (cbm, params) ←obj
   if exist (cbm) = = true then
      return error
  else
      return (obj ⊃ [params])
function GetIdBook (cbm, id)
  const allData = []
  while! result. done then
    allData.Push → Key: result.value.key, Record:
    record
    result ← await. iterator. next ()
    return allData. AuthorityId
end
```

In the prepared smart contract, the initIdBook method is executed to perform the initial settings that need to be done at the beginning of the distributed ledger settings. Before writing new data into the distributed ledger, it is checked whether there is data with the same Id. When a positive answer is received, a new object is created and the process of registering to the distributed ledger is started and the new record is returned at the end of the process. The GetIdBook method can be executed to read the records. After checking the necessary permissions, the data stored in the distributed ledger can be read and listed with the help of an iterator. Algorithm 1 shows the pseudo code of the smart contract.

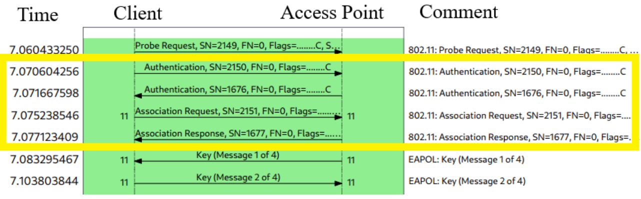
4. FINDINGS AND RESULTS

Authentication times of RADIUS, WPA2, WEP, Open Access and BCAUTH wireless authentication systems were measured in the test environment. In order to measure the authentication times, the wireless network packets in the environment were sniffed with the wireshark program installed on a computer with Kali Linux operating system. The connection steps of the sniffed packets and authentication types are given in Figure 5, Figure 6, Figure 7 and Figure 8.



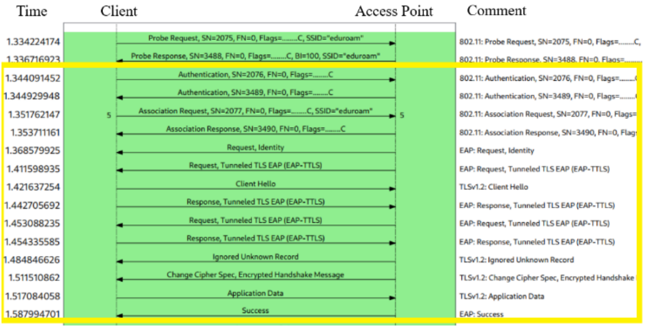
```
Time          Access Point                                                   Client   Comment
10.410118678     Probe Request, SN=3555, FN=0, Flags=........C, S...                  802.11: Probe Request, SN=3555, FN=0, Flags=...
10.413848868     Probe Response, SN=1407, FN=0, Flags=........C, ...                  802.11: Probe Response, SN=1407, FN=0, Flags=
10.415345606     Authentication, SN=3556, FN=0, Flags=........C                       802.11: Authentication, SN=3556, FN=0, Flags=
10.418446576     Authentication, SN=256, FN=0, Flags=........C                        802.11: Authentication, SN=256, FN=0, Flags=..
10.422682416  7  Association Request, SN=3557, FN=0, Flags=.......              7     802.11: Association Request, SN=3557, FN=0, F
10.425058839     Association Response, SN=257, FN=0, Flags=.......                    802.11: Association Response, SN=257, FN=0, F
10.487969154     Action, SN=258, FN=0, Flags=........C, Dialog Tok...                 802.11: Action, SN=258, FN=0, Flags=........C, Dial
10.532343923     QoS Null function (No data), SN=1537, FN=0, Fl...                    802.11: QoS Null function (No data), SN=1537, FN
```

Figure 5. Open Access Authentication connection process



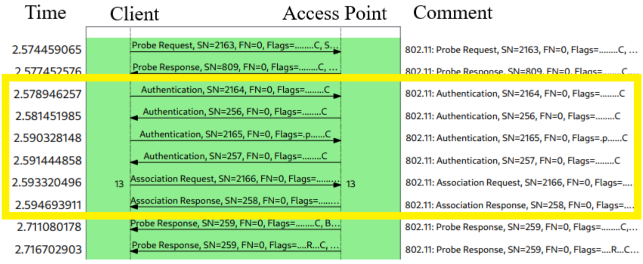
```
Time         Client                                                    Access Point   Comment
7.060433250      Probe Request, SN=2149, FN=0, Flags=........C, S...                  802.11: Probe Request, SN=2149, FN=0, Flags=........C, ...
7.070604256      Authentication, SN=2150, FN=0, Flags=........C                       802.11: Authentication, SN=2150, FN=0, Flags=........C
7.071667598      Authentication, SN=1676, FN=0, Flags=........C                       802.11: Authentication, SN=1676, FN=0, Flags=........C
7.075238546  11  Association Request, SN=2151, FN=0, Flags=.......           11       802.11: Association Request, SN=2151, FN=0, Flags=....
7.077123409      Association Response, SN=1677, FN=0, Flags=......                    802.11: Association Response, SN=1677, FN=0, Flags=.
7.083295467  11  Key (Message 1 of 4)                                        11       EAPOL: Key (Message 1 of 4)
7.103803844  11  Key (Message 2 of 4)                                        11       EAPOL: Key (Message 2 of 4)
```

Figure 6. WPA2 Authentication Connection Process



```
Time         Client                                                              Access Point   Comment
1.334224174     Probe Request, SN=2075, FN=0, Flags=........C, SSID="eduroam"                   802.11: Probe Request, SN=2075, FN=0, Flags=........C,
1.336716923     Probe Response, SN=3488, FN=0, Flags=........C, BI=100, SSID="eduroam"          802.11: Probe Response, SN=3488, FN=0, Flags=........
1.344091452     Authentication, SN=2076, FN=0, Flags=........C                                  802.11: Authentication, SN=2076, FN=0, Flags=........
1.344929948     Authentication, SN=3489, FN=0, Flags=........C                                  802.11: Authentication, SN=3489, FN=0, Flags=........
1.351762147  5  Association Request, SN=2077, FN=0, Flags=........C, SSID="eduroam"    5        802.11: Association Request, SN=2077, FN=0, Flags=
1.353711161     Association Response, SN=3490, FN=0, Flags=........C                            802.11: Association Response, SN=3490, FN=0, Flag
1.368579925     Request, Identity                                                               EAP: Request, Identity
1.411598935     Request, Tunneled TLS EAP (EAP-TTLS)                                            EAP: Request, Tunneled TLS EAP (EAP-TTLS)
1.421637254     Client Hello                                                                    TLSv1.2: Client Hello
1.442705692     Response, Tunneled TLS EAP (EAP-TTLS)                                           EAP: Response, Tunneled TLS EAP (EAP-TTLS)
1.453088235     Request, Tunneled TLS EAP (EAP-TTLS)                                            EAP: Request, Tunneled TLS EAP (EAP-TTLS)
1.454335585     Response, Tunneled TLS EAP (EAP-TTLS)                                           EAP: Response, Tunneled TLS EAP (EAP-TTLS)
1.484846626     Ignored Unknown Record                                                          TLSv1.2: Ignored Unknown Record
1.511510862     Change Cipher Spec, Encrypted Handshake Message                                 TLSv1.2: Change Cipher Spec, Encrypted Handshake
1.517084058     Application Data                                                                TLSv1.2: Application Data
1.587994701     Success                                                                         EAP: Success
```

Figure 7. Radius Authentication Connection process



```
Time         Client                                                    Access Point   Comment
2.574459065      Probe Request, SN=2163, FN=0, Flags=........C, S...                  802.11: Probe Request, SN=2163, FN=0, Flags=........C, ...
2.577452576      Probe Response, SN=809, FN=0, Flags=........C, ...                   802.11: Probe Response, SN=809, FN=0, Flags=........C...
2.578946257      Authentication, SN=2164, FN=0, Flags=........C                       802.11: Authentication, SN=2164, FN=0, Flags=........C
2.581451985      Authentication, SN=256, FN=0, Flags=........C                        802.11: Authentication, SN=256, FN=0, Flags=........C
2.590328148      Authentication, SN=2165, FN=0, Flags=.p......C                       802.11: Authentication, SN=2165, FN=0, Flags=.p......C
2.591444858      Authentication, SN=257, FN=0, Flags=........C                        802.11: Authentication, SN=257, FN=0, Flags=........C
2.593320496  13  Association Request, SN=2166, FN=0, Flags=.......           13       802.11: Association Request, SN=2166, FN=0, Flags=....
2.594693911      Association Response, SN=258, FN=0, Flags=.......                    802.11: Association Response, SN=258, FN=0, Flags=....
2.711080178      Probe Response, SN=259, FN=0, Flags=........C, B...                  802.11: Probe Response, SN=259, FN=0, Flags=........C,...
2.716702903      Probe Response, SN=259, FN=0, Flags=....R...C, ...                   802.11: Probe Response, SN=259, FN=0, Flags=....R...C...
```

Figure 8. WEP Authentication Connection Process

Apache jMeter application was used to perform performance tests of the authentication system on the blockchain. JMeter simulates resource requests (web requests) made by real users to servers while using a web application, as if real users were requesting these resources. The user scenarios simulated with JMeter (the way users use the web application) can be constructed as if multiple users are running the same scenario at the same time by differentiating the inputs requested by the web application and a load of the desired size can be created in the system.

Authentication times were calculated based on the difference between the time when the authentication process started and the time when the authentication process was successful. The calculated times in milliseconds are given in Table 2.

Table 2. Authentication time

Auth. Type	Radius	WPA2	WEP	Open Access	BCAUTH
Auth. Time (ms)	243.903	6.519	15.747	97.132	240.375

RADIUS authentication takes more time than other authentication types because after the authentication process with radius is successful, the user must be authorized and communicated with to establish the connection. WPA2 was found to be the fastest of the authentication types tested. According to the findings, the main reasons for the delay of the blockchain structure are the time spent for the formation of the genesis block, which is automatically generated at the start of the chain, the verification time applied to test the reliability of the chain, and the transaction processes realized through smart contracts. Considering all the conditions, the performance of the BCAUTH infrastructure proposed in this study is acceptable from the perspective of security measures and technological innovation.

5. CONCLUSIONS

Authentication and blockchain technology can be combined to create secure and decentralized systems for authentication and access control. As a distributed and immutable ledger, blockchain provides transparency, immutability, and resistance to tampering, making it suitable for authentication purposes. For user registration, when a user wants to create an account or register on a platform, they provide their personal information and create a digital identity. This identity is then hashed, encrypted, and stored on the blockchain network. The user is given a unique cryptographic key pair consisting of a private key (known only to the user) and a public key. When the user wants to verify their identity on the platform, they start the process by providing their public key or digital ID. The platform verifies the authenticity of the user by checking the blockchain records. Since the blockchain is immutable, any changes or tampering attempts can be detected. Smart contracts, which are self-executing contracts with predefined rules encoded in the blockchain, are used for access control. Access to certain resources or services is regulated through smart contracts that enforce certain conditions or permissions based on the identity of the user. This enables decentralized and automated access management without the need for intermediaries. Blockchain-based authentication systems increase privacy by enabling users to control their personal data. Instead of sharing sensitive information with each individual service provider, users can selectively disclose the information required for authentication purposes without revealing their entire identity. This reduces the risk of data breaches and identity theft. Another advantage of combining authentication with blockchain is the ability to audit and track user activity. The transparent nature of blockchain allows for the creation of an immutable audit trail that provides a comprehensive record of authentication events and related transactions. This is useful for compliance, regulatory purposes, or dispute resolution. It is important to note that while blockchain provides security and decentralization, it can also bring challenges related to scalability, performance, and energy consumption. Numerical results have been obtained that support this view. Therefore, the suitability of combining authentication and blockchain should be evaluated based on specific use cases and requirements. In future studies, it is aimed to implement authentication systems as well as authorization processes and move them to the smart contracts base.

Ethics Committee Approval
N/A

Peer-review
Externally peer-reviewed.

Conflict of Interest
The authors have no conflicts of interest to declare.

Funding
The authors declared that this study has received no financial support.

REFERENCES

Abbas, S. et al. (2021) 'Blockchain-Based Authentication in Internet of Vehicles: A Survey', Sensors 2021, Vol. 21, Page 7927, 21(23), p. 7927. Available at: https://doi.org/10.3390/S21237927.

Alabady, S.A.J. (2008) 'Design and implementation of a network security model using static VLAN and AAA server', 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA [Preprint]. Available at: https://doi.org/10.1109/ICTTA.2008.4530276.

Benzekki, K., El Fergougui, A. and El Belrhiti El Alaoui, A. (2016) 'Devolving IEEE 802.1X authentication capability to data plane in software-defined networking (SDN) architecture', Security and Communication Networks, 9(17), pp. 4369–4377. Available at: https://doi.org/10.1002/SEC.1613.

Chen, J.C. and Wang, Y.P. (2005) 'Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience', IEEE Communications Magazine, 43(12), pp. S26–S32. Available at: https://doi.org/10.1109/MCOM.2005.1561920.

Cui, Z. et al. (2020) 'A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN', IEEE Transactions on Services Computing, 13(2), pp. 241–251. Available at: https://doi.org/10.1109/TSC.2020.2964537.

Dantu, R., Clothier, G. and Atri, A. (2007) 'EAP methods for wireless networks', Computer Standards & Interfaces, 29(3), pp. 289–301. Available at: https://doi.org/10.1016/J.CSI.2006.04.001.

Diallo, E. hacen, Dib, O. and Al Agha, K. (2022) 'A scalable blockchain-based scheme for traffic-related data sharing in VANETs', Blockchain: Research and Applications, 3(3), p. 100087. Available at: https://doi.org/10.1016/J.BCRA.2022.100087.

Esposito, C., Ficco, M. and Gupta, B.B. (2021) 'Blockchain-based authentication and authorization for smart city applications', Information Processing & Management, 58(2), p. 102468. Available at: https://doi.org/10.1016/J.IPM.2020.102468.

Ferreira, C.M.S. et al. (2021) 'IoT Registration and Authentication in Smart City Applications with Blockchain', Sensors 2021, Vol. 21, Page 1323, 21(4), p. 1323. Available at: https://doi.org/10.3390/S21041323.

Grover, K. and Lim, A. (2015) 'A survey of broadcast authentication schemes for wireless networks', Ad Hoc Networks, 24(PA), pp. 288–316. Available at: https://doi.org/10.1016/J.ADHOC.2014.06.008.

Guo, R. et al. (2019) 'Flexible and Efficient Blockchain-Based ABE Scheme with Multi-Authority for Medical on Demand in Telemedicine System', IEEE Access, 7, pp. 88012–88025. Available at: https://doi.org/10.1109/ACCESS.2019.2925625.

Hammi, M.T. et al. (2018) 'Bubbles of Trust: A decentralized blockchain-based authentication system for IoT', Computers & Security, 78, pp. 126–142. Available at: https://doi.org/10.1016/J.COSE.2018.06.004.

He, D. et al. (2012) 'Analysis and improvement of a secure and efficient handover authentication for wireless networks', IEEE Communications Letters, 16(8), pp. 1270–1273. Available at: https://doi.org/10.1109/LCOMM.2012.061912.120941.

Henry, P.S. and Luo, H. (2002) 'WiFi: What's next?', IEEE Communications Magazine, 40(12), pp. 66–72. Available at: https://doi.org/10.1109/MCOM.2002.1106162.

Kablosuz Ağlarda Şifreleme, Kimlik Doğrulama ve Güvenlik Önlemleri (no date). Available at: https://yazilimcigenclik.com.tr/kablosuz-aglarda-sifreleme-kimlik-dogrulama-ve-guvenlik-onlemleri/ (Accessed: 18 March 2023).

Kim, Y.P., Yoo, S. and Yoo, C. (2015) 'DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things', 2015 IEEE International Conference on Consumer Electronics, ICCE 2015, pp. 196–197. Available at: https://doi.org/10.1109/ICCE.2015.7066378.

Kumar, U. and Gambhir, S. (2014) 'A Literature Review of Security Threats to Wireless Networks', International Journal of Future Generation Communication and

Networking, 7(4), pp. 25–34. Available at: https://doi.org/10.14257/IJFGCN.2014.7.4.03.

Lau, C.H., Alan, K.H.Y. and Yan, F. (2019) 'Blockchain-Based Authentication in IoT Networks', DSC 2018 - 2018 IEEE Conference on Dependable and Secure Computing [Preprint]. Available at: https://doi.org/10.1109/DESEC.2018.8625141.

Li, D. et al. (2018) 'A blockchain-based authentication and security mechanism for IoT', Proceedings - International Conference on Computer Communications and Networks, ICCCN, 2018-July. Available at: https://doi.org/10.1109/ICCCN.2018.8487449.

Li, J.S. et al. (2017) 'A comparison of classifiers and features for authorship authentication of social networking messages', Concurrency and Computation: Practice and Experience, 29(14), p. e3918. Available at: https://doi.org/10.1002/CPE.3918.

Li, X. et al. (2018) 'A robust and energy efficient authentication protocol for industrial internet of things', IEEE Internet of Things Journal, 5(3), pp. 1606–1615. Available at: https://doi.org/10.1109/JIOT.2017.2787800.

Liang, Y. et al. (2020) 'Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective', IEEE Internet of Things Journal, 7(9), pp. 9128–9143. Available at: https://doi.org/10.1109/JIOT.2020.3004077.

Liao, K.-C. and Lee, W.-H. (2010) 'A Novel User Authentication Scheme Based on QR-Code', Journal of Networks, 5(8). Available at: https://doi.org/10.4304/jnw.5.8.937-941.

Mir, O. and Nikooghadam, M. (2015) 'A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services', Wireless Personal Communications, 83(4), pp. 2439–2461. Available at: https://doi.org/10.1007/S11277-015-2538-4/TABLES/2.

Mohsin, A.H. et al. (2019) 'Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions', Computer Standards & Interfaces, 64, pp. 41–60. Available at: https://doi.org/10.1016/J.CSI.2018.12.002.

Muhammad, M. and Safdar, G.A. (2018) 'Survey on existing authentication issues for cellular-assisted V2X communication', Vehicular Communications, 12, pp. 50–65. Available at: https://doi.org/10.1016/J.VEHCOM.2018.01.008.

Neuman, C.B. and Ts'o, T. (1994) 'Kerberos: An Authentication Service for Computer Networks', IEEE Communications Magazine, 32(9), pp. 33–38. Available at: https://doi.org/10.1109/35.312841.

Okada, A. et al. (2019) 'e-Authentication for online assessment: A mixed-method study', British Journal of Educational Technology, 50(2), pp. 861–875. Available at: https://doi.org/10.1111/BJET.12608.

Pan, F. et al. (2017) 'Physical layer authentication based on channel information and machine learning', 2017 IEEE Conference on Communications and Network Security, CNS 2017, 2017-January, pp. 364–365. Available at: https://doi.org/10.1109/CNS.2017.8228660.

(PDF) Securing UMaT Wireless Network Using pfSense Captive Portal with Radius Authentication (no date). Available at: https://www.researchgate.net/publication/306056068_Securing_UMaT_Wireless_Network_Using_pfSense_Captive_Portal_with_Radius_Authentication (Accessed: 18 March 2023).

Pradeep, R. et al. (2019) 'Formal Verification of Authentication and Confidentiality for TACACS+ Security Protocol using Scyther', 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019 [Preprint]. Available at: https://doi.org/10.1109/ICCCNT45670.2019.8944623.

Ramya, S. et al. (2022) 'Face Biometric Authentication System for ATM using Deep Learning', Proceedings - 2022 6th International Conference on Intelligent Computing and Control Systems, ICICCS 2022, pp. 1446–1451. Available at: https://doi.org/10.1109/ICICCS53718.2022.9788310.

Sahu, A.K. et al. (2018) 'Secure Authentication Protocol for IoT Architecture', Proceedings - 2017 International Conference on Information Technology, ICIT 2017, pp. 220–224. Available at: https://doi.org/10.1109/ICIT.2017.21.

Soewito, B. and Hirzi (2014) 'Building secure wireless access point based on certificate authentication and firewall captive portal', EPJ Web of Conferences, 68, p. 00029. Available at: https://doi.org/10.1051/EPJCONF/20146800029.

Yavuz, A.A. (2014) 'An efficient real-time broadcast authentication scheme for command and control messages', IEEE Transactions on Information Forensics and Security, 9(10), pp. 1733–1742. Available at: https://doi.org/10.1109/TIFS.2014.2351255.

Yildirim, S. et al. (2021) 'Kampüs Ağlarında İnternet Erişimi İçin Bağlantı Katmanı Kimlik Doğrulama Uygulaması', Computer Science, (Special), pp. 82–92. Available at: https://doi.org/10.53070/BBD.990930.

Yu, R. et al. (2017) 'Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network', IEEE Access, 5, pp. 24944–24951. Available at: https://doi.org/10.1109/ACCESS.2017.2767285.

Zhang, Z. et al. (2022) 'Artificial intelligence in physiological characteristics recognition for internet of things authentication', Digital Communications and Networks [Preprint]. Available at: https://doi.org/10.1016/J.DCAN.2022.10.006.

Zhu, J. and Ma, J. (2004) 'A new authentication scheme with anonymity for wireless environments', IEEE Transactions on Consumer Electronics, 50(1), pp. 231–235. Available at: https://doi.org/10.1109/TCE.2004.1277867.

Zia, M. (2021) 'B-DRIVE: A blockchain based distributed IoT network for smart urban transportation', Blockchain: Research and Applications, 2(4), p. 100033. Available at: https://doi.org/10.1016/J.BCRA.2021.100033.

Xu, Z., Smyth, C. E., Lemprière, T. C., Rampley, G. J., & Kurz, W. A. (2018). Climate change mitigation strategies in the forest sector: biophysical impacts and economic implications in British Columbia, Canada. *Mitigation and adaptation strategies for global change*, *23*(2), 257-290.