Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2026.2151

Research Article

Blockchain-enabled virtual smart card authentication for IoT systems and applications

Abdulla J. Y. ALDARWISH[1,2,*], Kalyani PATEL[3], Aqeel A. YASEEN[1]

[1]*Department of Computer Sciences, Gujarat University, Ahmedabad, 380009, India*
[2]*Department of Computer Sciences, Education College for Pure Sciences, University of Basrah, 6100, Iraq*
[3]*K.S. School of Business Management and Information Technology, Gujarat University, Ahmedabad, 380009, India*

ARTICLE INFO

Article history
Received: 17 December 2024
Revised: 13 March 2025
Accepted: 15 June 2025

Keywords:
Authentication; Blockchain; Fog Computing; IoT; Multi-Factor Authentication; QR Codes; Scyther

ABSTRACT

Authentication on IoT devices has to work under tight limits on processing power, energy and response time, and many existing schemes either load the device too heavily or depend on one trusted server. This paper proposes a multi-factor authentication (MFA) framework for IoT that combines virtual smart cards (VSCs), QR-code login, fog computing and a permissioned blockchain. Heavy verification work is moved to fog nodes, and only the important events are written to the ledger, which keeps delays short and makes tampering detectable. We evaluated the design in a Python simulation. Authentication took 194.7 ms on average and registration 104.8 ms, and the system handled about 95.39 authentications per second. The cost on the user side stayed small, about 55 ms of device processing per login. We also checked the protocol with the Scyther tool; it found no attack on the stated secrecy and authentication claims, a model that covers replay, impersonation and man-in-the-middle attempts. Against recently published blockchain-based schemes, the latency is competitive and the feature set is wider, mainly because login is passwordless and user anonymity is kept. The results suggest that the framework is practical for real-time IoT services such as healthcare and smart cities, although tests on real hardware are still needed.

Cite this article as: Aldarwish AJY, Patel K, Yaseen AA. Blockchain-enabled virtual smart card authentication for IoT systems and applications. Sigma J Eng Nat Sci 2026;44(5):3195–3208.

INTRODUCTION

The Internet of Things (IoT) now links devices in homes, factories, transport systems and hospitals, and it has changed how many services reach people [1]. More links also mean more ways in. Unauthorized access and data breaches are the most obvious risks, and the usual defences are not keeping up: single-factor authentication (SFA) and even two-factor authentication (2FA) can be defeated by phishing, identity theft or device cloning [2, 3]. IoT data is also used more and more in everyday services, from recommendation systems built on smart devices to K-means based security monitoring [4, 5], so the question of who may access a device or its data matters a great deal. What is missing is authentication that is strong but still

***Corresponding author.**
*E-mail address: abdullajas@uobasrah.edu.iq

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey
© Author. This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

light enough for small devices. In practice this has several sides. The scheme must run on devices with little processing power and memory, it must cope with very large numbers of nodes, it should protect user privacy, and it has to answer quickly enough for real-time services. Most existing schemes handle one or two of these well; few handle all of them without heavy overhead or limited scalability. This gap is the starting point of our work.

Multi-factor authentication (MFA) combines two or more independent credentials and is clearly stronger than single-factor login [6]. Classic MFA, though, still leans on passwords or physical smart cards. Cards get lost or stolen, and passwords get phished [7]. Several recent works therefore replace the physical card with a virtual smart card (VSC), using hardware already built into the device, such as a Trusted Platform Module, together with software protection [6, 7]. A VSC keeps the cryptographic keys inside the device and performs authentication without a separate token, so the theft-and-loss problem largely disappears [8]. Other work points in a related direction: the framework in [9], for example, combines blockchain with edge computing to secure a smart IoT system.

Blockchain is attractive for IoT authentication because its ledger is decentralized and, once written, practically immutable [10]. Integrity, transparency and the absence of a single point of failure follow from these properties, whereas a central server is exactly such a point. Fog computing helps from a different side. It processes data near the source, which cuts latency and bandwidth use and takes work away from weak devices, instead of sending every request to a distant cloud server that adds delay and widens the attack surface. Putting the two together is the main idea of this work. A blockchain alone is often too slow and too heavy for IoT, and fog nodes can absorb much of that computational and latency cost [11, 12]. The need is especially clear in healthcare, where work on lightweight, anonymity-preserving authentication and broader surveys of IoT security and privacy both point to open problems [13, 14]. General IoT design methods, architectures and protocols, as described in [15], give the base on which such frameworks are built.

Earlier schemes have improved parts of the picture, but the trade-off between security, computational cost and privacy is usually left open [16, 17]. In this paper we propose a blockchain-enabled MFA framework for IoT that uses virtual smart cards and passwordless factors (a biometric sample and a QR code). The design goals are simple to state. Keep the work on the user device small. Resist the common attack types. Make login easy. To reach them, the framework pairs a distributed ledger for credential records with lightweight cryptographic operations, and it brings blockchain, fog computing, VSCs and MFA into one scheme instead of treating them separately. The following sections show that this improves security while performance and usability stay at an acceptable level.

To our knowledge, VSCs, blockchain, fog computing and passwordless MFA have not been combined and evaluated together in one framework before. Compared with earlier fog- and blockchain-based schemes [16, 17], our design adds passwordless VSC login and user anonymity while keeping latency in the same range. The protocol was also checked formally with Scyther, which found no attack on its secrecy and authentication claims; this covers replay, man-in-the-middle and device impersonation, the attacks most often discussed for IoT [16, 18]. Such properties matter in many IoT domains. Smart agriculture is one example where secure authentication has been shown to be necessary [19].

The paper therefore has two aims: to identify the limits of current IoT authentication approaches, and to propose a framework that works in healthcare and in other domains as well. We describe the system architecture and the authentication protocol, and then evaluate security and performance with measured data. The main advantages of the scheme can be put briefly. MFA and the blockchain together raise the level of security. Fog computing reduces latency and the load on devices. Passwordless VSC and QR-code login make things easier for the user. Taken together, these features secure modern IoT systems better than password- or card-based methods do.

The rest of the paper is organized as follows. The next section reviews related work on IoT authentication. We then describe the primitive tools the framework relies on: blockchain, fog computing, asymmetric cryptography, VSCs, QR codes and the Scyther verifier. The proposed scheme follows, with the system model and the registration, authentication and credential-update phases. After that comes the security analysis, first informal and then formal with Scyther, and then a comparison of security features and performance with related schemes. The last section concludes the paper, notes its limitations and outlines future work.

RELATED WORK

Work on IoT authentication is moving quickly, pushed by two needs that often pull against each other: strong security and low cost on constrained devices. We review the literature in four parts. First come the general challenges of IoT authentication, then the role of blockchain, then virtual smart cards, and finally integrated solutions that combine several of these technologies. The section ends with the gaps that motivate our work.

IoT Authentication: Challenges and Evolution

IoT devices are often placed in sensitive settings such as smart cities, hospitals and industrial control systems, and they have little computing power, memory or energy to spare [20]. Early systems usually protected them with a single factor, typically a password. This proved weak against phishing, brute-force guessing and device compromise [18]. Traditional frameworks also tend to be centralized and often

depend on a public key infrastructure (PKI). That creates single points of failure and scales poorly, which is a bad fit for distributed and heterogeneous IoT networks [16]. The survey of IoT security and privacy in [14] reaches a similar conclusion: centralized authentication has clear limits, and new defences must suit the dynamic, resource-constrained character of IoT.

MFA raises security by asking for several independent proofs of identity, which makes common attacks harder than with one factor [6]. Early MFA schemes, however, often relied on physical tokens or smart cards. These can be lost or stolen, and a careless implementation can still be broken by a determined attacker [7, 18]. The open problem is to find authentication methods that are light, decentralized and hard to break, and that fit very different IoT environments without overloading the devices. Design methods, architectures and protocols that support this goal are discussed in [15].

Blockchain Technology for Decentralized and Trustworthy IoT Authentication

Blockchain has received a lot of attention as a way to remove the trust and centralization problems of conventional IoT authentication [10, 16]. Its main properties (decentralization, immutability, transparency and cryptographic protection) allow a trustworthy authentication system to be built without a central authority. When device identities and credentials are kept on a distributed ledger, they are very hard to tamper with. There is also no single server whose failure or compromise, for example through phished administrator credentials, can bring the whole system down [3, 21]. Many studies use blockchain for device registration, identity checks and access control in IoT networks. In one example, the authors of [22] build a fast and secure emergency road healthcare service for smart cities on a blockchain, which shows the technology working in a critical application.

Using public blockchains such as Bitcoin or Ethereum, which have mostly relied on Proof-of-Work, directly in IoT is difficult. The computation, confirmation delay and storage they need are far beyond what most IoT devices can offer [9, 15]. Research has therefore turned to lighter designs: permissioned ledgers and faster consensus methods such as Proof-of-Authority or Proof-of-Elapsed-Time, tuned for IoT [11]. Fog and edge computing offer another way out. The heavy blockchain work moves from end devices to stronger intermediate nodes, so security does not have to be paid for with poor performance [11, 12]. The smart climate agriculture framework in [9] follows this pattern and combines blockchain with edge computing. On a broader level, [23] studies how blockchain can be adopted efficiently under risk and uncertainty, which shows how far its use has spread beyond the original setting.

VSCs and Advanced Credential Management

Virtual smart cards give the security of a hardware smart card without the physical token. They emulate the card in software and usually rely on security hardware already present in the device, such as a TPM or the secure element of a smartphone [6–8]. Keys are stored, and cryptographic operations run, inside a protected environment, so keys are less likely to be exposed even if other parts of the device are compromised. Safe credential handling in such dynamic systems also depends on the system staying observable and controllable, a question studied with control-theoretic sampling models in [24]. VSC authentication itself has advanced in recent years. In [25], a VSC on a mobile device is used within an MFA system to strengthen user authentication in healthcare. Another work [26] proposes a two-factor scheme for ad-hoc networks that joins a VSC mechanism with biometrics and reports resistance to a range of attacks.

VSC ideas are relevant to wider IoT security work too, even where virtual cards are not named. The security framework in [9] and the K-means based data security detection in [5] both operate in settings where credentials must be managed safely, and that is the core function of a VSC. The recommender system in [4], built on IoT smart devices, likewise depends on trusted interaction between users and devices. Finally, [18] and [19] describe healthcare and smart agriculture applications, two areas in which protected, and possibly virtualized, credential storage is important for security and privacy.

Integrated Solutions: Synergies of Blockchain, Fog/Edge Computing, and MFA for IoT

Because IoT systems are so varied, one technology is rarely enough, and recent studies increasingly combine blockchain, fog or edge computing and MFA. In [6], a two-layer MFA system uses blockchain and physically unclonable functions (PUFs) to authenticate both IoT devices and users. The architecture in [16] uses fog nodes to take computation off IoT end points, which raises throughput and lowers latency. A scalable, cluster-based blockchain protocol for IoT networks is developed in [27], while [28] proposes BUA, a blockchain-based unlinkable authentication scheme that protects privacy. The work in [29] links blockchain with the InterPlanetary File System (IPFS) to support continuous, adaptive authentication. Game theory has been applied as well; [30] combines game-theoretic and cryptographic models to study crypto-cloud computing, including its economic and financial side.

Other contributions deal with specific building blocks. Efficient message transmission over twisted Edwards curves [31] is relevant to the elliptic-curve operations used in such systems. The cooperative game model of crypto cloud computing in social networks [32] gives insight into how trust and computation can be shared, which also applies to decentralized IoT authentication. For latency-sensitive IoT applications, [33] proposes metaheuristic task scheduling in edge computing. And [34] introduces a coalition game for managing electronic health records on a blockchain, an

example from a sensitive domain where security has to be designed in from the start.

In a different field, the study in [35] shows how circular-economy principles and Industry 5.0 technologies, blockchain among them, can support supplier selection in complex supply chains. For IoT the lesson is that device interactions are becoming part of larger, sustainability-driven systems, and authentication frameworks need to be flexible enough for that.

Gaps in Existing Literature and Motivation for Proposed Work

Despite this progress, several gaps remain. Many solutions concentrate on one property, for example decentralization or the use of several factors, and do not offer a complete framework that balances security, computational cost, privacy and scalability as IoT requires. The overhead of some blockchain designs is still a concern. Managing VSCs safely in a highly distributed and possibly hostile environment needs careful design. And keeping a system interoperable and easy to use without lowering its security is a problem that does not go away.

Our work responds to these gaps with a framework that combines blockchain, fog computing, MFA, VSCs and QR codes. The aim is better security and privacy at a performance level that real-time IoT services can accept, with healthcare and smart environments as the main use cases. Each technology is used to cover the weak points of the others, so that the result is more resilient, more efficient and easier for users than existing approaches.

PRIMITIVE TOOLS

The framework is built from a small set of basic tools and technologies. Below we describe each one and what it contributes to security, efficiency and scalability in the authentication process.

Blockchain Technology

The blockchain is a central part of the system. It provides a decentralized ledger in which authentication records cannot be changed unnoticed, so their integrity and transparency are preserved. Control is shared among several nodes instead of one authority, and no single party can rewrite stored data. This makes tampering and many kinds of attack much harder. At the same time, authorized parties can check that the data are genuine without weakening their protection.

Recent studies show the value of blockchain in IoT, especially for sensitive records such as patient data. According to [36], decentralization helps most when many stakeholders are involved, because no single point of failure remains. Immutability means that authentication records stay exactly as they were written, which protects them against corruption and keeps the system consistent [37]. The ledger is also transparent: authentication steps can be verified without showing sensitive content to parties that should not see it. Figure 1 shows the main elements of a blockchain, namely the network nodes, the chain of linked blocks and the Merkle tree inside each block.

Fog Computing

Fog computing brings computing resources close to the IoT devices themselves. Data no longer has to travel to a remote data centre before anything can be done with it, and this is what makes fog useful for real-time work such as patient monitoring. Fog nodes are placed between the devices and the cloud. They process and authenticate sensitive data locally, and only after that is the data stored on the blockchain.

By moving computation toward the edge, fog computing makes IoT systems faster and supports quicker decisions [38]. Results from applied mathematics can help here as well. Homogenization techniques for periodic network structures [39] may be used to improve the performance and scalability of fog architectures, and robust optimization

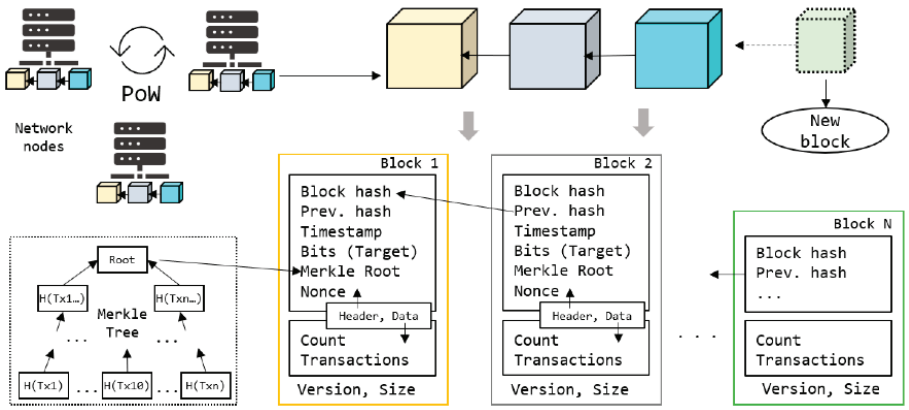


Figure 1. Structure of a blockchain: nodes, linked blocks and Merkle tree [1]. (Adapted from Tulkinbekov K, Kim DH. Data modifications in blockchain architecture for big-data processing. Sensors (Basel) 2023;23:8762).

under polyhedral uncertainty, developed for multi-model regulatory networks [40], offers a way to keep distributed systems reliable when their parameters are uncertain. The decentralized structure also scales, since more devices can join without a central bottleneck. As [41] points out, the ability of fog nodes to take over tasks from the cloud matters most where data must be processed in real time, as in healthcare and industrial IoT.

Asymmetric Cryptography

Asymmetric (public-key) cryptography is basic to secure communication in IoT networks. Each entity holds a public and a private key. In our architecture these key pairs protect the data exchanged between IoT devices, fog nodes and the blockchain. Only a holder of the right private key can decrypt a message, so the data stay confidential and out of reach of unauthorized parties.

Public-key cryptography is a standard requirement wherever distributed devices exchange data [42]. If a message is intercepted, its content still cannot be read without the private key. This is particularly important for biometric data. It is one of the key factors in the proposed system, and unlike a password it cannot be changed once it leaks.

Virtual Smart Cards

A VSC is a secure, passwordless replacement for a physical smart card. It stores sensitive authentication data, such as the biometric template and the cryptographic keys, in digital form. For IoT users this is both safer and more convenient than carrying a card. In the proposed framework the VSC is combined with biometric verification and a QR code, which gives an MFA process that is stronger without being harder to use.

With a VSC, users no longer depend on physical tokens, so theft and loss are much less of a risk [25]. Because it runs on the user's mobile device, no extra hardware is required. Passwordless authentication, studied for example in [43], also removes many weaknesses of password-based login and is easier for the user.

QR Codes

In the framework, QR codes act as authentication tokens that the user scans at login. Each user has a unique code. Together with the biometric sample and the per-session nonce, it ties every login to one user and one session, so a recorded session cannot simply be replayed.

Earlier work has shown that QR codes can serve as tamper-resistant identifiers that protect the integrity of the authentication process [44]. When the QR content is also encrypted, it adds another layer of protection in IoT settings, since access is granted only to authorized users.

Scyther Security Protocol Verification Tool

We use Scyther to check the security mechanisms of the framework. The tool models the message exchanges of the protocol and searches for attacks, including man-in-the-middle and replay attacks, by an adversary who controls the network. When Scyther finds no attack on a claim, the claim holds within the model. This is a much stronger assurance than informal reasoning alone.

Scyther is one of the most widely used tools for analysing security protocols [45]. It explores complex attack scenarios automatically, which makes it well suited to IoT authentication protocols. Formal tools of this kind help to find weaknesses early, before a protocol is deployed.

PROPOSED SCHEME

This section describes the proposed MFA framework for IoT systems, which combines VSCs, blockchain and fog computing. Our priorities were security, efficiency and convenience, and for this reason login is passwordless and relies on QR codes and biometric verification. The framework has three phases: registration, authentication, and password change (credential update). The parties involved are the user devices (UD_i), the fog nodes (FN_j) and a permissioned blockchain network (BCN). Table 1 lists the notation used in this section.

System Model

The architecture has three main entities:

- **User Devices (UD_i):** End-user devices, such as smartphones, that run the application used to manage credentials, communicate with the system and carry out the cryptographic operations.
- **Fog Nodes (FN_j):** Geographically distributed computing nodes placed between the user devices and the blockchain network. They verify authentication requests locally, which reduces latency and takes computation away from the user devices.
- **Blockchain Network (BCN):** A permissioned distributed ledger maintained by authorized fog nodes. It stores the essential credential information (in hashed or encrypted form) and the authentication logs, so that they cannot be altered without detection.

Registration Phase

In this phase a new user UD_i is enrolled through the mobile application, which talks to a designated fog node FN_j. When the phase ends, the user's virtual smart card (VSC_i) has been created and its information stored securely. The steps are:

1. **User Input:** The user UD_i starts registration in the mobile application by giving biometric data Bio_i and, if wanted, a password PW_i.
2. **VSC Generation:** The application generates a unique identifier UID_i, a unique QR code QR_i and a public/private key pair (PK_{Ui}, SK_{Ui}) for the user. Together with the biometric template Bio_i, these items form the virtual smart card VSC_i:

$$VSC_i = \{UID_i, Bio_i, QR_i, PK_{Ui}, SK_{Ui}\}$$

Table 1. Notations

Notation	Description
UD_i	The *i*-th User Device (e.g., smartphone, tablet)
FN_j	The *j*-th Fog Node
BCN	The permissioned Blockchain Network
Bio_i	Stored biometric data template of user *i*
Bio'_i	Freshly captured biometric data of user *i* during an authentication attempt
PW_i	Optional password chosen by user *i*
UID_i	Unique Identifier assigned to user *i*
QR_i	Unique QR code associated with user *i*
PK_{Ui}	Public Key of user *i*
SK_{Ui}	Private Key of user *i*
PK_{FN}	Public Key of the Fog Node FN_j
SK_{FN}	Private Key of the Fog Node FN_j
VSC_i	Virtual Smart Card for user *i*, containing $\{UID_i, Bio_i, QR_i, PK_{Ui}, SK_{Ui}\}$
VSC'_i	Updated Virtual Smart Card for user *i* after credential change
$E_{PK}(M)$	Asymmetric encryption of message *M* using public key *PK*
$D_{SK}(C)$	Asymmetric decryption of ciphertext *C* using private key *SK*
C	The random challenge generated by the Fog Node for mutual authentication
Token	Response token generated by the User Device during mutual authentication
SK	Symmetric Session Key established between UD_i and FN_j after successful authentication
$KeyExchange(P_1, P_2)$	Secure key exchange protocol run between parties P_1 and P_2 to establish a session key
Update(*Net, Data, ID*)	The operation to securely record or update *Data* associated with Identifier *ID* on the network *Net* (BCN)
$h(\cdot)$	A secure cryptographic one-way hash function (e.g., SHA-256)

3. **Credential Encryption:** To keep it confidential in transit, the application encrypts VSC_i with the public key PK_{FN} of the designated fog node FN_j:

$$C_{VSC} = E_{PK_{FN}}(VSC_i)$$

The ciphertext C_{VSC} is then sent to FN_j.

4. **Fog Node Verification:** On receiving C_{VSC}, the fog node FN_j decrypts it with its private key SK_{FN}:

$$VSC_i = D_{SK_{FN}}(C_{VSC})$$

FN_j then checks that the received VSC_i components are complete and valid.

5. **Blockchain Storage:** If the check succeeds, FN_j submits a transaction that records the registration on the blockchain network *BCN*. The transaction normally holds the user's UID_i and a hash (or an encrypted form) of the critical VSC_i elements, which then cannot be modified:

$$Transaction_{Reg} = \{UID_i, h(VSC_i), timestamp, ...\}$$
$$Record(BCN, Transaction_{Reg})$$

The mobile application keeps the required parts of VSC_i, including SK_{Ui}, in the secure local storage of the device.

Figure 2 shows the sequence of operations and the data flow in the registration phase.

Authentication Phase

This phase verifies the identity of a registered user UD_i who wants to access a service or resource. It involves the fog node FN_j and a check against the *BCN*. The steps are:

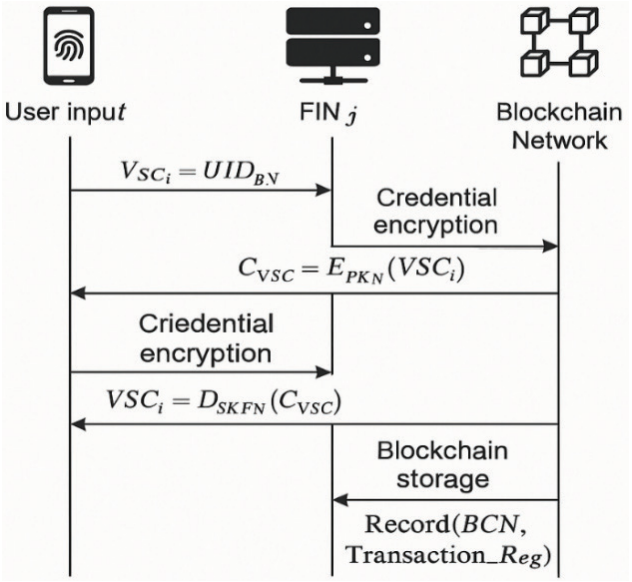


Figure 2. Registration process.

1. **Authentication Initiation:** The user UD_i scans the relevant QR_i and gives a fresh biometric sample Bio'_i through the mobile application.
2. **Credential Retrieval:** The application reads the required credentials (e.g., UID_i, SK_{Ui} and the stored Bio_i) from the locally protected VSC_i.
3. **Request Transmission:** The application builds an authentication request with UID_i, Bio'_i, the scanned QR_i data, a fresh nonce and a timestamp. The request is encrypted with PK_{FN} and sent to FN_j.
4. **Fog Node Validation:** FN_j decrypts the request with SK_{FN} and then runs the following checks:
   - **Biometric Comparison:** The fresh sample Bio'_i is compared with the stored template Bio_i, which is retrieved using UID_i from secure storage or, if needed, through a *BCN* lookup:

$$Result_{Bio} = Compare(Bio'_i, Bio_i)$$

   - **QR Code Verification:** The scanned QR_i data are validated.
   - **Identifier Extraction:** The UID_i is confirmed.
   - **Blockchain Verification:** FN_j queries the *BCN* with UID_i to confirm that the registration of the user is still active and to obtain any data needed for validation: $Status = Verify_{BCN}(UID_i)$
5. **Mutual Authentication:** To block impersonation and man-in-the-middle attacks, FN_j and UD_i authenticate each other. FN_j generates a random challenge C and sends it encrypted under the public key PK_{Ui} of UD_i:

$$C_{Chal} = E_{PKU_i}(C)$$

UD_i recovers the challenge with its private key SK_{Ui}:

$$C = D_{SKU_i}(C_{Chal})$$

UD_i computes a response *Token* from C (for example, by signing C, or by hashing C together with a nonce) and returns it encrypted with PK_{FN}:

$$C_{Resp} = E_{PKFN}(Token(C))$$

FN_j decrypts C_{Resp} with SK_{FN} and checks the *Token*. A valid response shows that the device really holds the private key of the user.

6. **Session Key Generation:** Once mutual authentication succeeds and all factors have been verified, UD_i and FN_j agree on a session key SK through a key exchange protocol:

$$SK = KeyExchange(UD_i, FN_j)$$

SK protects all further communication in that session.

Figure 3 gives the detailed flow of the login and authentication phase.

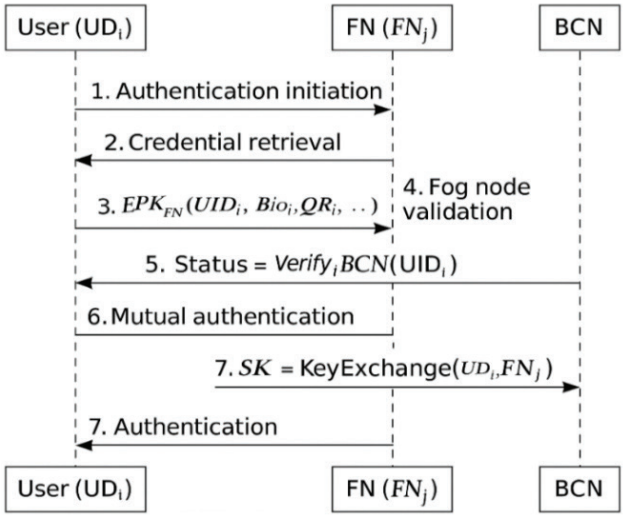


Figure 3. Login and authentication process.

Password Change Phase (Credential Update)

This phase lets a user UD_i update their credentials safely, for example to change the password PW_i (if one is used) or to re-enrol the biometric Bio_i.

1. **Initiation & Verification:** The user starts the update in the mobile application and must first authenticate with the existing credentials, exactly as in the authentication phase.
2. **New Credential Input:** The user enters the new credential (e.g., PW_i^{new} or a new Bio_i^{new}), and the application produces an updated card, VSC'_i.
3. **Encryption & Transmission:** The updated VSC'_i is encrypted with PK_{FN} and sent to FN_j:

$$C_{VSC'} = E_{PKFN}(VSC'_i)$$

4. **Fog Node Processing & Blockchain Update:** FN_j decrypts $C_{VSC'}$ with SK_{FN}, checks that the request is legitimate, and submits a transaction that updates the user's record on the *BCN*. The change is recorded under UID_i; the old credential is either revoked or kept as an earlier version:

$$Update(BCN, h(VSC'_i), timestamp, UID_i)$$

5. **Local Update:** When FN_j confirms that the update has been written to the blockchain, the mobile application replaces the locally stored VSC_i data.

SECURITY ANALYSIS

Informal Security Analysis

Here we examine how well the proposed VSC-based MFA framework resists common threats. For each property we give a short explanation and the corresponding cryptographic expression.

User anonymity

User anonymity means that the real identity of a user is known only to the user and the fog node. In our framework,

user data are encrypted before anything is written to the blockchain. The ledger holds only the encrypted VSC (or its hash), so an observer cannot link a record to a person, and credentials are checked without revealing identity details to any intermediate party:

$$\textbf{User Anonymity: } UID_i \xrightarrow{E_{PK_{FN}}(VSC_i)} FN \rightarrow Blockchain \ (anonymous\ storage)$$

Untraceability

Untraceability comes from using a fresh session key and nonce for every authentication attempt. An attacker who records the encrypted messages still cannot tell whether two sessions belong to the same user, because the session-specific values change every time:

$$\textbf{Untraceability: } SK_{session} = KeyExchange(UD_i, FN_j), \ where\ each\ session\ generates\ a\ unique\ SK_{session}$$

Resistance to common attacks

We consider the following threats:

- **Impersonation Attack:** An attacker cannot pose as a user without both the private key of the user user (SK_{Ui}) and the matching biometric data. Without the private key the challenge cannot be recovered, so no valid response token can be produced:

$$\textbf{Impersonation Resistance: } Token(C)\ accepted \Longrightarrow C = D_{SKUi})(C_{Chal}) \wedge Compare(Bio'_i, Bio_i) = 1$$

- **Replay Attack:** Each request carries a timestamp and a fresh, session-specific nonce (N_i). A recorded message therefore fails the freshness check if it is sent again:

$$\textbf{Replay Protection: } AuthRequest_i = \{UID_i, N_i, Timestamp\}$$

- **Man-in-the-Middle Attack:** The user device and the fog node authenticate each other through encrypted challenge–response messages. An attacker in the middle can relay these messages but cannot read or change them without the private keys, so the exchange cannot be taken over:

$$FN \xrightarrow{E_{PK_U}(C)} UD, \quad UD \xrightarrow{E_{PK_{FN}}(Token)} FN$$

- **Password Guessing Attack:** Online or offline guessing gives the attacker little. The password is optional and never enough on its own, because login also needs the biometric sample and the QR code, and the credentials kept on the blockchain are encrypted:

$$\textbf{Credential Security: } E_{PKFN}(Bio_i, QR_i) \rightarrow Stored\ securely\ on\ Blockchain$$

- **Stolen-Verifier Attack:** The verification data on the blockchain are stored in encrypted (or hashed) form. An attacker who copies them cannot use them to impersonate a user without the matching private key:

$$\textbf{Secure Storage: } D_{SKFN}(E_{PKFN}(VSC_i)) \text{ only possible with private key } SK_{FN}$$

Mutual authentication

Mutual authentication confirms the identity of both sides, the user and the fog node. The device proves that it holds the private key of the user by answering the challenge, and only the genuine fog node, which holds its own private key, can read that answer and complete the key exchange. An attacker in the middle therefore cannot replace either party:

$$FN \rightarrow UD: E_{PKU}(C),\ UD \rightarrow FN: E_{PKFN}(Token), \text{ ensuring mutual verification}$$

Formal Verification with Scyther

To complement the informal analysis, we verified the protocol formally with the Scyther tool. Scyther assumes an attacker who controls the network and searches systematically for attacks on each secrecy and authentication claim, including man-in-the-middle and replay attacks.

Figure 4 shows the result for a baseline version of the protocol without the proposed protections: three claims of the user role (Secret T, Alive and Weakagree) are falsified. Figure 5 shows the same analysis for the proposed protocol. Here every claim of both roles is verified and Scyther reports no attacks.

Figure 6 gives the output of the Scyther role characterization for the VSC and SERVER roles.

SECURITY AND PERFORMANCE COMPARISON

This section compares the proposed framework with authentication schemes from the related work, first by security features and then by performance. The features considered are MFA, blockchain and fog computing integration, the use of VSCs and QR codes, passwordless login, mutual authentication and user anonymity.

Comparison of Security Features

Table 2 lists the main security properties of our method next to those of recent schemes reviewed in the related work section.

As Table 2 shows, the proposed framework is the only one among the compared schemes that combines all of these features: an immutable blockchain record, low-latency fog processing, MFA, VSCs and QR codes. It also offers mutual authentication and user anonymity. On every listed criterion it matches or exceeds the other schemes. Note, though, that the table records whether a feature is present, not how strong it is.

Performance Evaluation and Comparison

We now report the performance of the framework, measured in a Python simulation, and compare it with recent peer-reviewed work. The simulation ran on a machine with

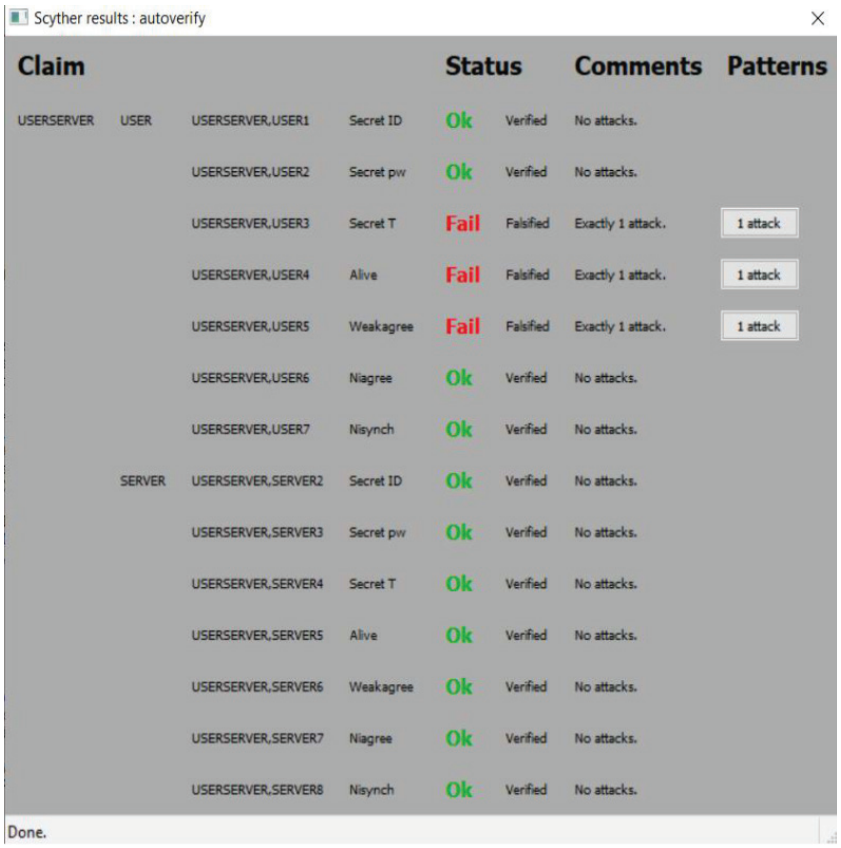


Figure 4. Scyther results for the baseline protocol, with the falsified claims.

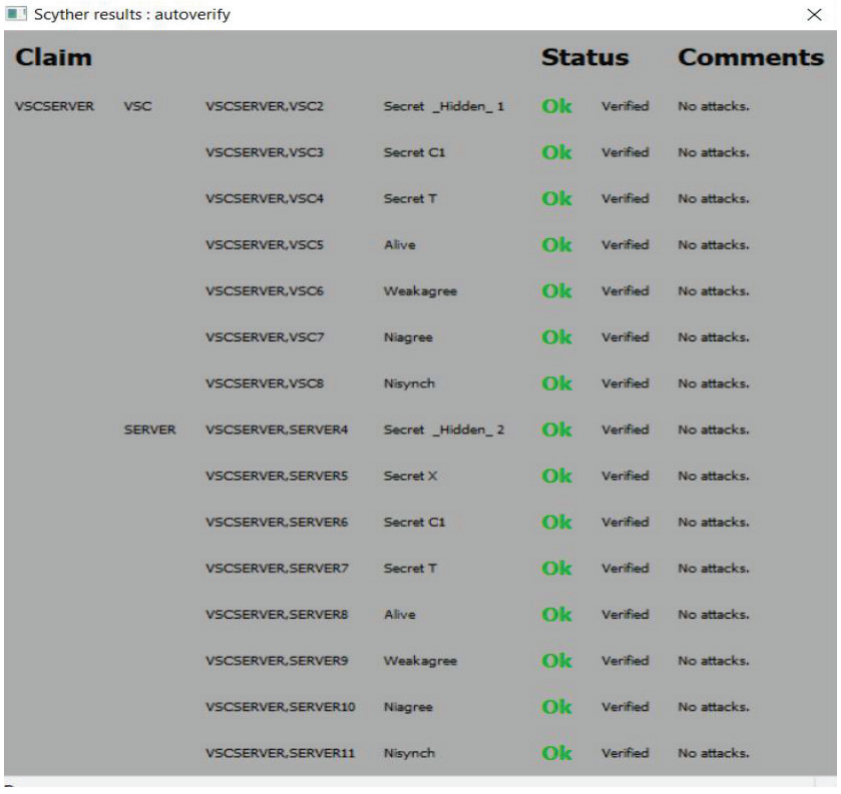


Figure 5. Scyther verification results for the proposed protocol.

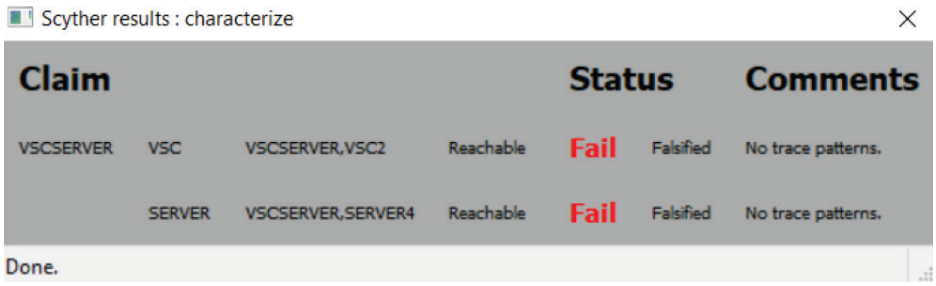


Figure 6. Scyther role characterization output.

Table 2. Security features of the proposed scheme and related schemes

Security Criteria	Proposed Scheme	[6]	[16]	[27]	[28]	[26]
Multi-factor Authentication	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*
Blockchain Integration	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*No*
Fog Computing Integration	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Virtual Smart Card	*Yes*	*No*	*No*	*No*	*No*	*Yes*
QR Code Utilization	*Yes*	*No*	*No*	*No*	*No*	*No*
Passwordless Authentication	*Yes*	*No*	*No*	*No*	*No*	*No*
Mutual Authentication	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
User Anonymity	*Yes*	*Partial*	*Partial*	*Yes*	*Yes*	*Partial*

an Intel Xeon processor at 2.00 GHz (4 logical cores) and 3.8 GB of RAM, under Ubuntu 22.04 and Python 3.11. It modelled the interactions between user devices (*UDs*), fog nodes (*FNs*) and a permissioned blockchain network.

The key performance indicators (*KPIs*) are registration latency, authentication latency, password change latency, blockchain transaction processing time and overall throughput. Table 3 gives the measured values.

On average, registration took about 104.8 ms and authentication about 194.7 ms (Table 3). A password change took 72.7 ms; this figure excludes the authentication step that precedes the update. Processing one blockchain transaction took 50.3 ms on average, and the system sustained about 95.39 authentications per second. We also looked at the parts of a single authentication. The user device spent about 55.2 ms on its operations, and the fog node needed about 22.0 ms without the blockchain interaction. The communication delay between device and fog node was fixed at 60.0 ms in the simulation. So distributed processing and network delay make up most of the latency, while the ledger operations themselves stay fast, as one would expect from a permissioned, Proof-of-Authority (PoA)-like chain.

Table 3. Performance metrics of the proposed system

Operation	Value
Registration Latency	*~104.8 ms*
Authentication Latency	*~194.7 ms*
Password Change Latency	*~72.7 ms*
Blockchain Processing Time	*~50.3 ms*
Authentication Throughput	*~95.39 auth/sec*

To put these numbers in context, we compared them with several recent blockchain-based authentication frameworks. Table 4 lists the authentication latency and throughput of each.

Table 4 shows the trade-offs between different blockchain designs. Some systems, such as [46] and [47], report very low latency or very high throughput. Their figures, however, come from settings that differ from a full MFA login: [46] uses PoA consensus, and [47] uses DPoS with sharding for high-volume data sharing, both of which give up some decentralization. Our framework also relies on a permissioned, PoA-like ledger and so accepts part of the same trade-off, which is reasonable here because the validators are the operator's own fog nodes. With an authentication latency of about 194.7 ms, the framework is faster than [48] (about 256.5 ms) and [49] (about 390 ms) and close to [50] (about 152.5 ms) and [48] (about 148.9 ms). Its throughput of about 95.39 authentications per second is modest. It is still enough for most IoT deployments, where a single fog node rarely sees very frequent authentication events. The cited figures were obtained on different hardware and workloads, so the comparison is indicative rather than exact. Overall, the

Table 4. Comparative latency and throughput of recent authentication frameworks

System	Auth Latency	Throughput	Consensus
Proposed Framework	*~194.7 ms*	*~95.39 auth/sec*	*Permissioned/PoA*
[48]	*~256.5 ms*	*~156.6 TPS*	*PBFT*
[50]	*~152.5 ms*	*~298.2 TPS*	*Hybrid*
[49]	*~148.9 ms*	–	*PoAh*
[46]	*~0.06 ms*	*~43 TPS*	*PoA*
[47]	*~390 ms*	*~30 TPS*	*Raft (Hyperledger)*
[51]	*<1 ms*	*~500–2000 TPS*	*DPoS + Sharding*

Table 5. Characteristics of blockchain consensus mechanisms

Consensus	Latency	Throughput	Security & Decentralization
PoW	Very High (~10 min block time)	Low (5–15 TPS)	High (Decentralized)
PoS	Moderate (~12 s)	Moderate	High
DPoS	Low (~0.5–1 s)	High (1000+ TPS)	Medium
PBFT	Low (<1 s)	High (100s TPS)	Medium-Low
PoA	Very Low (<<1 s)	High	Low (Centralized)

framework performs well enough for practical use and keeps the integrity benefits of a shared ledger.

The consensus mechanism has a large effect on blockchain performance. Table 5 summarizes the main properties of the consensus algorithms most relevant to IoT and MFA.

The proposed system moves the heavy authentication logic from constrained IoT devices to fog nodes and uses a lightweight permissioned blockchain that behaves like PoA, with fast transaction finality. This choice explains much of the observed performance and gives a reasonable balance between security and efficiency.

In summary, on modest hardware the proposed MFA framework reaches registration and authentication latencies of roughly 100–200 ms and a throughput of about 95.39 authentications per second. These results are in line with, and in some respects better than, several recent systems [46–51], especially when performance, security features and the practical needs of IoT deployment are considered together.

CONCLUSION

This study presented a blockchain-based MFA framework for IoT and assessed its security and performance through simulation and formal verification. The framework combines blockchain, fog computing, VSCs and passwordless QR-code login to give a decentralized, tamper-resistant authentication process that constrained devices can afford.

In the simulations, the system achieved low authentication latency, a manageable computational cost and acceptable throughput on modest hardware. Moving verification and blockchain interaction to fog nodes improves scalability and keeps the load on user devices small. The VSCs remove the need for physical tokens or static credentials, which helps both usability and security.

The informal analysis and the Scyther verification indicate that the protocol resists common attacks such as impersonation, replay and man-in-the-middle attacks. The permissioned blockchain gives fast transaction finality and protects record integrity, which suits time-sensitive applications in healthcare, smart homes and industrial automation.

The study has limitations. All results come from a simulated environment, and a real deployment may face changing network conditions, hardware limits and energy constraints. Management of the VSC life cycle, in particular revocation and recovery, also needs stronger mechanisms before field use.

In future work we plan to deploy the framework in real IoT settings, improve its scalability with optimized consensus mechanisms, and add advanced cryptographic tools for stronger privacy and long-term security.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence was not used in the preparation of the article.

REFERENCES

[1] Tulkinbekov K, Kim DH. Data modifications in blockchain architecture for big-data processing. Sensors (Basel) 2023;23:8762. [CrossRef]

[2] Khalil U, Malik OA, Uddin M, Chen CL. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. Sensors (Basel) 2022;22:5168. [CrossRef]

[3] Basit A, Zafar M, Liu X, Javed AR, Jalil Z, Kifayat K. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun Syst 2021;76:139–154. [CrossRef]

[4] Ahmed M, Ansari MD, Singh N, Gunjan VK. Rating-based recommender system based on textual reviews using IoT smart devices. Mob Inf Syst 2022;2022:2854741. [CrossRef]

[5] Zhu J, Huo L, Ansari MD, Ikbal MA. Research on data security detection algorithm in IoT based on K-means. Scalable Comput Pract Exp 2021;22:149–159. [CrossRef]

[6] Bamashmos S, Chilamkurti N, Shahraki AS. Two-layered multi-factor authentication using decentralized blockchain in an IoT environment. Sensors (Basel) 2024;24:3575. [CrossRef]

[7] Khan MA, Alhakami H, Alhakami W, Shvetsov AV, Ullah I. A smart card-based two-factor mutual authentication scheme for efficient deployment of an IoT-based telecare medical information system. Sensors (Basel) 2023;23:5419. [CrossRef]

[8] Ashraf Z, Mahmood Z, Iqbal M. Lightweight privacy-preserving remote user authentication and key agreement protocol for next-generation IoT-based smart healthcare. Future Internet 2023;15:386. [CrossRef]

[9] Ting L, Khan M, Sharma A, Ansari MD. A secure framework for IoT-based smart climate agriculture system: toward blockchain and edge computing. J Intell Syst 2022;31:221–236. [CrossRef]

[10] Chen F, Xiao Z, Xiang T, Fan J, Truong L. A full lifecycle authentication scheme for large-scale smart IoT applications. IEEE Trans Dependable Secure Comput 2022;20:2221–2237. [CrossRef]

[11] Li Y, Su DA, Mardani A. Digital twins and blockchain technology in the industrial Internet of Things (IIoT) using an extended decision support system model: Industry 4.0 barriers perspective. Technol Forecast Soc Change 2023;195:122794. [CrossRef]

[12] Sharma PC, Mahmood MR, Raja H, Yadav NS, Gupta BB, Arya V. Secure authentication and privacy-preserving blockchain for industrial internet of things. Comput Electr Eng 2023;108:108703. [CrossRef]

[13] Masud M, Gaba GS, Choudhary K, Hossain MS, Alhamid MF, Muhammad G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet Things J 2022;9:2649–2656. [CrossRef]

[14] Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. IoT privacy and security: challenges and solutions. Appl Sci (Basel) 2020;10:4102. [CrossRef]

[15] Pathak A, Tembhurne JV, Kalaiarasan C, Jain T. IoT design methodology: architectures and protocols. In: Gunjan VK, Ansari MD, Usman M, et al., editors. Modern approaches in IoT and machine learning for cyber security: latest trends in AI. Cham: Springer International Publishing; 2024. p. 1–20. [CrossRef]

[16] Umoren O, Singh R, Awan S, Perwez Z, Dahal K. Blockchain-based secure authentication with improved performance for fog computing. Sensors (Basel) 2022;22:8969. [CrossRef]

[17] Zhao J, Zhang Y, Jiang J. Blockchain-based distributed computing consistency verification for IoT mobile applications. Appl Sci (Basel) 2023;13:7762. [CrossRef]

[18] Suryanarayana G, Prakash KLNC, Ansari MD, Gunjan VK. IoT for healthcare. In: Gunjan VK, Ansari MD, Usman M, et al., editors. Modern approaches in IoT and machine learning for cyber security: latest trends in AI. Cham: Springer International Publishing; 2024. p. 201–218. [CrossRef]

[19] Vijayakrishna A, Gopichand G, Ansari MD, Suryanarayana G. IoT based smart agriculture using LiFi. In: 2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT); 2022. p. 1–7. [CrossRef]

[20] Chen CM, Liu S, Chaudhry SA, Khan MA. A lightweight and robust user authentication protocol with user anonymity for IoT-based healthcare. Comput Model Eng Sci 2022;131:307–329. [CrossRef]

[21] Tembhurne JV, Diwan T, Jain TK. IoT security and privacy. In: Gunjan VK, Ansari MD, Usman M, et al., editors. Modern approaches in IoT and machine learning for cyber security: latest trends in AI. Cham: Springer International Publishing; 2024. p. 45–61. [CrossRef]

[22] Ksibi A, Mhamdi H, Ayadi M, Almuqren L, Alqahtani MS, Ansari MD, et al. Secure and fast emergency road healthcare service based on blockchain technology for smart cities. Sustainability (Basel) 2023;15:5748. [CrossRef]
[23] Babaei A, Tirkolaee EB, Amjadian A. Crafting efficient blockchain adoption strategies under risk and uncertain environments. Alex Eng J 2024;103:137–147. [CrossRef]
[24] Hamidoğlu A, Mahmudov EN. On construction of sampling patterns for preserving observability/controllability of linear sampled-data systems. Int J Control 2022;95:206–217. [CrossRef]
[25] Aldarwish AJY, Patel K, Yassin AA, Yaseen AA. Virtual smartcards-based authentication in healthcare systems and applications. Int J Comput Inf Syst Ind Manag Appl 2023;15:9.
[26] Jolin JS, Theophilus A, Kathirvel A. Two-factor mutual authentication with fingerprint and MAC address validation. Int J Comput Netw Inf Secur 2024;16:56–68. [CrossRef]
[27] Al Ahmed MT, Hashim F, Hashim SJ, Abdullah A. Authentication-chains: blockchain-inspired lightweight authentication protocol for IoT networks. Electronics (Basel) 2023;12:867. [CrossRef]
[28] Wen Y, Liu M, Yang X, Yang T, Chang V. BUA: a blockchain-based unlinkable authentication scheme for mobile IoT. Enterp Inf Syst 2024;18:2243616. [CrossRef]
[29] Yao Y, Zhang X, Hu H, Liu H, Huang R, Wang Z. Blockchain-based multistage continuous authentication for smart devices. Appl Sci (Basel) 2023;13:12641. [CrossRef]
[30] Kırlar BB, Ergün S, Alparslan Gök SZ, Weber GW. A game-theoretical and cryptographical approach to crypto-cloud computing and its economical and financial aspects. Ann Oper Res 2018;260:217–231. [CrossRef]
[31] Kirlar BB. Efficient message transmission via twisted Edwards curves. Math Slovaca 2020;70:1511–1520. [CrossRef]
[32] Ergun S, Kirlar BB, Alparslan Gök SZ, Weber GW. An application of crypto cloud computing in social networks by cooperative game theory. J Ind Manag Optim 2020;16:1927–1941. [CrossRef]
[33] Satouf A, Hamidoğlu A, Gül ÖM, Kuusik A, Durak Ata L, Kadry S. Metaheuristic-based task scheduling for latency-sensitive IoT applications in edge computing. Cluster Comput 2024;28:143. [CrossRef]
[34] Hamidoğlu A, Altiti M, Jana C, Weber GW. A novel coalition game on management of electronic health records in blockchain technology. J Ambient Intell Humaniz Comput 2025. Epub ahead of print. [CrossRef]
[35] Nayeri S, Sazvar Z, Babaee Tirkolaee E. Viable supplier selection problem based on Industry 5.0 and circular economy aspects: a hybrid decision-making approach. Int J Syst Sci Oper Logist 2025;12:2469117. [CrossRef]
[36] Sohail MN, Anjum A, Saeed IA, Syed MH, Jantsch A, Rehman S. Optimizing industrial IoT data security through blockchain-enabled incentive-driven game theoretic approach for data sharing. IEEE Access 2024;12. [CrossRef]
[37] Aldarwish AJY, Patel K, Yaseen AA, Yassin AA, Abduljabbar ZA. Fog enabled private blockchain-based identity authentication scheme for oil and gas field monitoring. ICTACT J Commun Technol 2024;15:3236–3247. [CrossRef]
[38] Almadhoun R, Kadadha M, Alhemeiri M, Alshehhi M, Salah K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA); 2018. IEEE; 2018. p. 1–8. [CrossRef]
[39] Kropat E, Meyer-Nieberg S, Weber GW. Bridging the gap between variational homogenization results and two-scale asymptotic averaging techniques on periodic network structures. Numer Algebra Control Optim 2017;7:223–250. [CrossRef]
[40] Özmen A, Kropat E, Weber GW. Robust optimization in spline regression models for multi-model regulatory networks under polyhedral uncertainty. Optimization 2017;66:2135–2155. [CrossRef]
[41] Rahman G, Wen CC. Mutual authentication security scheme in fog computing. Int J Adv Comput Sci Appl 2019;10. [CrossRef]
[42] Lopez MI, Barsoum A. Traditional public-key cryptosystems and elliptic curve cryptography: a comparative study. Int J Cyber Res Educ 2022;4:1–14. [CrossRef]
[43] Praveen Kumar E, Priyanka S. A password less authentication protocol for multi-server environment using physical unclonable function. J Supercomput 2023;79:21474–21506. [CrossRef]
[44] Hasson M, Yassin AA, Yassin AJ, Rashid AM, Yaseen AA, Alasadi H. Password authentication scheme based on smart card and QR code. Indones J Electr Eng Comput Sci 2021;23:140–149. [CrossRef]
[45] Le TMC, Pham XT, Le VT. Advancing security protocol verification: a comparative study of Scyther, Tamarin. J Tech Educ Sci 2024;19:43–53. [CrossRef]
[46] Assiri B. A modified and effective blockchain model for e-healthcare systems. Appl Sci (Basel) 2023;13:12630. [CrossRef]
[47] Alzahrani RJ, Alzahrani FS. Blockchain for smart homes: blockchain low latency. J Comput Commun 2024;12:1–15. [CrossRef]
[48] Meshcheryakov Y, Melman A, Evsutin O, Morozov V, Koucheryavy Y. On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices. IEEE Access 2021;9:80559–80570. [CrossRef]

[49] Puthal D, Mohanty SP, Yanambaka VP, Kougianos E. PoAh: a novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks. arXiv [Preprint]. 2020. arXiv:2001.07297.

[50] Ali AA, Atiahallah AN. A hybrid blockchain-based approach for secure and efficient IoT identity management. Int J Comput Sci Netw Secur 24:11–25.

[51] Haque EU, Shah A, Iqbal J, Ullah SS, Alroobaea R, Hussain S. A scalable blockchain based framework for efficient IoT data management using lightweight consensus. Sci Rep 2024;14:7841. [CrossRef]