FOG ENABLED PRIVATE BLOCKCHAIN-BASED IDENTITY AUTHENTICATION SCHEME FOR OIL AND GAS FIELD MONITORING

Abdulla J. Y. Aldarwish[1], Kalyani Patel[2], Aqeel A. Yaseen[3], Ali A. Yassin[4] and Zaid Ameen Abduljabbar[5]
[1,3,]*Department of Computer Science, Gujarat University, India*
[2]*Department of Computer Application and Information Technology, K.S. School of Business Management and Information Technology, India*
[4,5]*Department of Computer Sciences, College of Education for Pure Sciences, University of Basrah, Iraq*

Abstract

The oil and gas industry remains critical to the global economy, as it contributes to the provision of energy and raw materials. Nonetheless, this sector continued to face clear challenges in operational effectiveness, risk and security. Regular tracking methods are limited to latency issues; they are not secure, and data may face integrity issues. To this end, this paper lays out an efficient fog-enabled private blockchain-based identity authentication approach for oil and gas field monitoring. By integrating IoT devices to blockchain, , decentralized control systems are created that enhance security, transparency, and efficient execution of transactions. In this scheme, by making full use of the decentralized structure of blockchain technology and applying the computational power of fog nodes, a secure and efficient identity authentication framework is designed. Fog nodes are an intermediary between IoT devices and blockchain technology, providing lower latency in communication, and therefore more efficient. The main contributions of this paper include: developing a decentralized authentication system based on private blockchains and fog nodes to overcome the drawbacks of centralized models. Create a network model using a private blockchain that dramatically improves feasibility by incorporating strict admission and authorization procedures. Hence, this leads to simultaneous registrations with minimal network time consensus Authentication that incorporating fuzzy extractor to connect the privacy-centric approach and to improve the security analysis and performance evaluation proving that the proposed solution provides better. According to the previous security analysis, it is clear that the scheme conflicts with different types of threats including DoS, MITM attacks, replay, Sybil, and message substitution attacks. The performance evaluation also shows low computational and communication costs, high compatibility, and real-time operation, which indicates that the proposed scheme is effective and can be implemented as a real-time oil and gas field monitoring system.

Keywords:

Fog Computing, Blockchain, IIoT, Authentication, Oil and Gas Industry

1. INTRODUCTION

The oil and gas industry is a cornerstone of the global economy, providing essential energy and raw materials. However, this sector faces significant challenges in automation and industrial control. Conventional automation systems in use in the oil and gas sector have several drawbacks, including outdated technology, poor integration, and susceptibility to cyber risks. These systems are inefficient and costly to operate. Failures and disruptions can cause serious safety hazards and financial losses.

Furthermore, the industry is exposed to cyber threats and hacking incidents more than ever. These attacks affect the monitoring and control systems hence opening up the system to unauthorized access, data leak and manipulation of operations. Cyber security threats are a major concern and can lead to significant operational loss and even environmental damage [1], [2]. Such breaches emphasize that there is an intensive need for effective measures to be taken to secure the ICSs within the oil and gas industry. Thus, it is important to provide a high level of cybersecurity to minimize the negative impact on the operation and prevent possible disastrous consequences.

Failures and weaknesses in security systems are often due to authentication mechanisms that are not suitable for the Internet of Things (IoT) [3]-[4]. Traditional authentication systems are centralized, making them vulnerable to single points of failure and scalability issues. In an IoT environment, where numerous devices need to communicate securely, centralized systems cannot handle the load efficiently. This results in slow response times and increased vulnerability to attacks. The centralized nature of these systems also makes them an attractive target for cyber attackers, who can compromise the entire network by attacking a single point [5]-[6]. Therefore, there is a critical need for decentralized and scalable authentication mechanisms to ensure robust security in IoT-based industrial environments like the oil and gas industry.

Decentralization in the application of protection for automation and monitoring systems addresses many issues associated with centralized systems. Decentralized systems distribute control across multiple nodes, reducing the risk of a single point of failure. This enhances the resilience of the system and improves its ability to handle large-scale operations typical of the IoT environment. By distributing the workload, decentralized systems can manage higher volumes of data and ensure more reliable and efficient operations [7]-[9].

Blockchain technology is employed to cover some of the drawbacks of centralization problems. Blockchain provides a decentralized ledger that records transactions in a secure and transparent manner. This technology ensures data integrity and prevents unauthorized tampering. In the context of the industry, blockchain can be used to secure communication between IoT devices and ensure that all transactions are verified and immutable. This reduces the risk of data breaches and enhances the overall security of the system.

However, decentralization also suffers from failures and problems. One significant issue is the complexity of managing a decentralized network [9]. Ensuring consistent data synchronization across all nodes can be challenging. Additionally, decentralized systems may face higher latency due to the need for consensus mechanisms to validate transactions [10]. This can impact the speed of operations, especially in time-sensitive environments like oil and gas field monitoring. Another problem is the potential for scalability issues as the number of nodes increases. Ensuring that all nodes can communicate effectively and maintain security protocols can become increasingly difficult as the network grows.

In order to address the gaps and issues of decentralization, the proposed method suggests the integration of fog computing and private blockchain. Fog computing enables the processing of data at the network edge, thereby enhancing the system throughput and response time. In this way, the data is processed at the fog nodes, and it helps to make quick decisions for real time events and minimize the load on the cloud servers. This is especially useful in the oil and gas industry where data analysis should be done as soon as possible.

Private blockchain further enhances the system by providing a controlled and secure environment for transactions. Unlike public blockchains, private blockchains restrict access to authorized participants, ensuring higher security and privacy [11] [12]. This control mechanism helps in managing scalability and maintaining efficient communication among nodes. Combining fog computing with private blockchain allows for a more scalable, secure, and efficient decentralized system, addressing the weaknesses of traditional centralized and purely decentralized models.

The main contributions of this article are as follows:

- Proposing the decentralized authentication scheme based on private blockchain technology with fog nodes for monitoring the oil and gas field. the proposed scheme covered the limitations of centralized schemes.
- Implement a private blockchain by constructing our network model as an example. As opposed to public Blockchains, P2P Blockchains do not have an outbound time, which can greatly increase efficiency due to intense member Joining checks and authorization. Hence, the consensus time in this type of network is nearly insignificant.
- Providing a privacy-focused approach by introducing a fuzzy extractor in the proposed scheme.
- Presenting a security analysis and performance evaluation of the proposed solution, with findings showing that, indeed, our solution offers optimal balance in security implementation and system performance.

The rest of the paper is organized as follows: Section 2 provides a discussion on the related works in the domain of IoT, blockchain, and their presence and usage in the oil and gas sector. We now discuss the architecture and elements of the new fog-integrated blockchain authentication scheme in Section 3. The implementation and the precise experimental setting used to assess the scheme's functionality are explained. Section 4. The efficacy of the scheme is explained in detail regarding security. Section 5 discusses the proposed scheme. Section 6 illustrates how the scheme resists multiple types of attacks. also discussing the results of the proposed scheme analysis and their comparison to the initial parameters, concerning communication overhead and computational expenses. Finally, Section 7 Conclusion.

2. RELATED WORK

There is a vast literature on the application of blockchain technology and IoT in different areas such as smart homes, agriculture, and industries. This section offers a brief literature analysis of current frameworks that deal with the implementation of IoT using blockchain technology with an emphasis on its impact on security and performance.

Regarding smart homes, there are numerous papers that have aimed at designing distributed authentication mechanisms based on blockchain technology. For instance, in their article, Ghadimi N., et al [13]. discussed the application of blockchain technology in smart homes IoT devices; they pointed out that IoT devices should be controlled and managed decentralized to provide better security. In the same manner, Zhao et al. [14] proposed a novel, lightweight framework for implementing smart home IoT nodes within a blockchain-based platform to minimize computation load while ensuring top-tier security. Such in-depth analysis stresses the applicability of blockchain in mitigating the security threats of smart home IoT systems.

Blockchain technology implementation in agriculture has also been noticed to have a high level of interest in its adoption. Zeng et al. [15] presented a smart agriculture framework based on IoT and blockchain where data integrity of IoT devices is preserved using blockchain and data is shared securely with other stakeholders. In their work, they proved efficacy and efficiency of applying block chain in the records of the various activities in agricultural. Another study by Bosona [16] described another proposal of traceability for agricultural products using blockchain to provide information such as origin and quality of the products which in turn improves food safety and the supply chain.

Blockchain and IoT has been applied and implemented in different sectors with an aim of enhancing efficacy and security in manufacturing operations. For example, Sharma et al. [17] proposed blockchain for the industrial IoT that facilitates secure communication and data integrity in the manufacturing sector. Likewise, the work by Toma and Popa [18] examined the feasibility of IoT in industry 4. They pointed to the applicability of blockchain in the context of IoT applications in industry 4. 0, thereby signifying that it may bring improvement in trust and reduced operational expense as compared to the conventional control strategy through the application of non-centralized means.

In the case of the oil & gas sector, the adoption of IoT and the application of blockchain more generally has been considered in relation to the minimization of certain threats, and the enhancement of certain aspects of the industry's functioning. Zuo and Qi [19]put forward a blockchain for IoT solution for remote oil field observance and control, which also strengthens data security as well as the feature of remote control. This framework elucidates the relevance of the blockchain in guaranteeing the protection of information exchange and Authorizations in the Oil and Gas industry. Furthermore, Senthil and Suganthi [20] proposed an advanced approach to the intelligent detecting and alerting of industrial gas leakage utilizing the IoT and blockchain-based foundation which assists in the enhancing the safety and effectiveness of the gas monitoring systems.

Previous studies have successfully integrated decentralization and blockchain technologies into various fields of the Internet of Things (IoT). However, these solutions still face significant challenges. Synchronizing consistent data across all blockchain nodes is complex and difficult, and the consensus mechanisms required to verify transactions can slow down operations, especially in time-sensitive environments. Additionally, as the number of nodes increases, managing and scaling the system becomes more challenging. To address these issues, our proposed method integrates fog computing with proprietary blockchain technology. Fog computing enables data processing at the edge of the network, improving system throughput and response time. By processing data in fog nodes, the system can make quick decisions for real-time events and reduce the load on cloud servers. This approach enhances the overall performance of IoT applications by providing faster and more efficient data handling while maintaining the security benefits of blockchain technology.

3. PRELIMINARIES

In this section, we introduce the fundamental concepts and technologies used in the proposed fog-integrated blockchain authentication scheme for enhanced security in oil and gas field monitoring. that include the Internet of Things (IoT), blockchain technology, fog computing, and the cryptographic techniques employed in our scheme.

3.1 INTERNET OF THINGS (IOT)

Internet of Things (IoT) entails devices which are connected and form a network in such a way that data is shared among them. These devices are as diverse in their functions as they are in levels of complexity; they can be basic sensors or an industrial equipment. Within the context of the oil and gas business, IoT nodes are used to measure and transmit values and conditions such as temperature, pressure, and equipment live readings. This sort of data compiled by such devices is useful for making alterations in the working system, anticipating possible device failures, or for augmenting safety measures.

IoT has impacted uber industries since it has made monitoring and controlling of so many industries possible through smart technology. For instance, in smart agriculture, IoT devices assist in measuring levels of moisture in the soil, climatic conditions and crops' general wellbeing, thereby enhancing productivity while reducing resource wastage [21] . According to [13] other IoT applications in smart homes include energy management and monitoring, intelligent security systems, and home automation. In the oil and gas sector infrastructure, IoT makes it possible to gather data concurrently, which is critical for optimizing the processes and their safety [20].

3.2 BLOCKCHAIN TECHNOLOGY

Blockchain is an innovative and decentralised technology for documenting contractual processes that include some specific security features. If we take a block, there is a list of transactions and in the same block, these cannot be altered once the block gets connected with the chain. This makes it direct, informative, and honest, in a way that preserves its genuineness as information. Blockchain is suitable where there is a need to provide assurance on the information being shared with the Third Party and to guarantee credibility [22] - [25].

Apart from being used as a form of payment, in the referral to IoT, it offers a secure solution to the sharing of data and device identification. The use of blockchain technology makes it easy to record all the activities between the devices to ensure that no other person interferes with the activities or changes what has been recorded [26]. For instance, in the supply chain, blockchain can help in tracking food products from producers to customers in a more transparent way hence minimizing fraudulent activities [16]. Likewise, in the field of medicine, blockchain can safely store medical records and the data may be easily and effectively exchanged without compromising the privacy and accuracy of the information [27]. Fig.1 presents the general structure of a blockchain, highlighting that it is an entity of blocks connected through reverse pointers

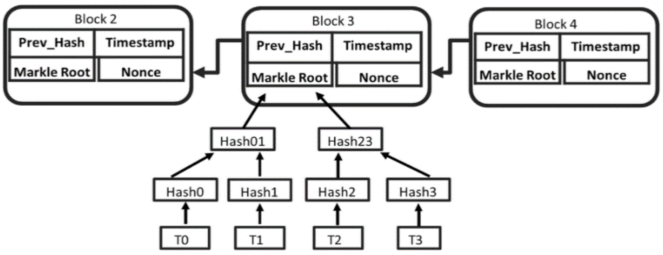

Fig.1. Blockchain model.

3.3 FOG COMPUTING

Fog computing, also referred to as edge computing, is a distributed extension of cloud computing that takes place at the edge points of the network. Fog is significant as it enables computation, storage and networking capabilities to be closer to the data source, the IoT devices. Fog computing can be said to cut down on latency and bandwidth as it enables the data to be processed at the edge of a network instead of relying on the central server.

Fog computing is particularly important in critical, real-time processing scenarios. For instance, in smart cities, the traffic nodes can analyze data collected from sensors that detect traffic and cameras in order to address traffic congestion [24], [28]. In industrial automation, the fog computing helps in continuous and random monitoring and controlling the operation of the machinery, thereby increasing utilization efficiency with less possibility of machinery failure [29]. The proposed architecture also categorized the IoT device to operate under the fog layer which offers localized authentication and data processing before sending it to the blockchain [28].

3.4 CRYPTOGRAPHIC TECHNIQUES

The proposed authentication scheme employs several cryptographic techniques to ensure security and privacy. These include public key cryptography, digital signatures, and fuzzy extractors.

3.4.1 Public Key Cryptography:

Public key cryptography involves a pair of keys - a public key and a private key. The public key is used for encryption, while the private key is used for decryption. This ensures that only the intended recipient can decrypt the message. In our scheme, public key cryptography is used to encrypt authentication requests and responses [30].

3.4.2 Digital Signatures:

Digital signatures provide a way to verify the authenticity and integrity of a message. A digital signature is generated using the sender's private key and can be verified using the sender's public key. This ensures that the message has not been tampered with and is indeed from the claimed sender. Digital signatures are used in our scheme to authenticate messages between devices and fog nodes [31].

3.4.3 *Fuzzy Extractors:*

Most systems use passwords to ensure that only the right individuals access particular applications, services, or other utilities, however, passwords cannot be said to have adequate security and privacy. To solve these problems, we employ the biometric Fuzzy extractor [32] which is a feature extraction algorithm. The fuzzy extractor consists of two algorithms: Gener and reproduction.

- Gen(BiO) = (σ,ρ): This function comes with a biometric sample term used as input (BiO) and gives out a high entropy secret string term (σ) as well as an auxiliary string term (ρ). This is the idea of saying that the Hamming distance between two strings is less than some predefined value (ε).
- Rep(BiO′, ρ) = σ: Here, it is using the new BiO and thereby recreating the sigma string using ρ string as long as the distance between BiO and BiO' is less than or equal to τ.

If BiO and BiO′ are belonging to the same user, then it is more likely for the distance to be small while, if from two different users, it will be closer to being larger [33].

3.4.4 *One-way hash function:*

A one-way hash function is a very important security function that can be used to support the integrity of data to be secured. It transforms an input or 'message' to a string with a specified length of bytes, which is usually a hash string and may seem random. The one way hash functions have several characteristics which include: One pre-image attack which does not allow an adversary to find the input that yields a specific output; Second pre-image attack whereby an attacker cannot find another input that yields the same hash; and most important of all; Collision attack is very difficult or almost impossible. These properties make one-way hash functions very useful in different security processes, for instance in digital signatures, message authentication code, and in the determination of the integrity of a given data. They are employed for assuring confidentiality, where data or information is not exposed to any unauthorized person, integrity where data has not been changed and authenticity where the source of the data is trusted. Some of the most used one-way hash functions are SHA full form is new Secure Hash Algorithm and its type used in latest cryptographic rush these are SHA-256 and SHA-3 [32], [33].

4. BACKGROUND AND SYSTEM MODEL

The oil and gas industry needs secure and intensive programs of monitoring to obtain efficiently and safely the resources. With monitoring systems that have been developed historically, there are certain issues that hinder their utilization, for instance, delay, data authenticity and security questions. What the previously mentioned challenges indicate is that, integrating of fog computing and blockchain could offer the much-needed solution to these challenges. Fog computing forwards data computation and processing to the edge of the network and allows for localized processing, thereby leading to decreased latency and requisite bandwidths. Blockchain, on the other hand, creates decentralized and extrapolated digital records of data that cannot be modified, ensuring the completeness, transparency, and security of records. In the subsequent sections, the discussion includes the network model that will support a fog-enabled private blockchain-based identity authentication scheme suitable for the oil and gas field monitoring: The threat model is also outlined in this section.

4.1 NETWORK MODEL

The network architecture comprises several key components, each playing a critical role in ensuring the secure and efficient operation of the monitoring system. These components include the Trusted Authority (TA), end-users, smart contracts, fog nodes, and smart devices. the proposed network working model is shown in Fig.2.

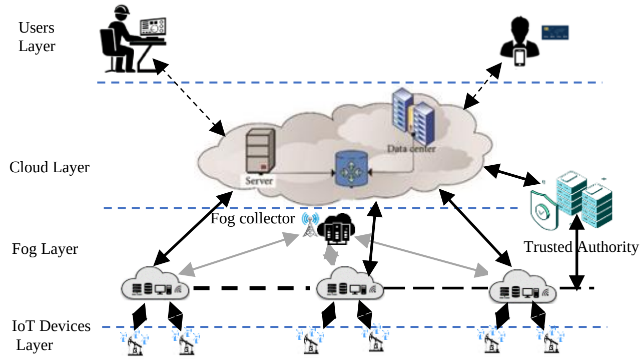

Fig.2. Network model**.**

- **Trusted Authority (TA):** The Trusted Authority (TA) of the framework can be regarded as the root of trust, being in charge of registering and authenticating all nodes in the network during the initialization phase. The TA is also responsible for generating and handling cryptographic keys needed for secure communication and authentication of various messages. Thus, the TA has to store only the confirmed identities of the network members, which eliminates the risk of the system being hacked, which makes the work of the network more reliable and safer [29].
- **End-user:** The most probable end user/clients of the oil and gas monitoring system are the operators/administrators who may require the data from field sensors or may need to control and manage the end devices in near real time. In end-users authentication, there is the combination of using password token and fingerprint as a way of enhancing the security. This makes it possible to restrict access to only those individuals who are supposed to have some level of access to such information and procedures [28].
- **Smart Contract:** Smart Contract: Smart contracts are contracts where all the conditions of fulfillment are processed and embedded with code interfaces. These contracts are developed to be implemented in the blockchain environment to work as automations, and they may include data permissions, device settings, and notifications. It is safer to execute those actions or deposits and returns only when certain conditions have been met because smart contracts mitigate dangers of unauthorized access [27], [34].
- **Fog Node:** Fog nodes serve as intermediaries between the end-users and the cloud, providing localized processing, storage, and decision-making capabilities. They handle real-time data processing from smart devices, reducing latency

and bandwidth usage. Fog nodes also play a crucial role in the authentication process by validating transactions and managing the local ledger before synchronizing with the main blockchain in the cloud. This distributed approach enhances the system's scalability and reliability [24], [31].

- **Smart Device:** The smart devices in the oil and gas field entail diverse tools that help in sensing and controlling parameters including pressure, temperature, flow rate, among others, and monitoring health of equipment as well. These devices are designed with lightweight cryptographic processing to enable secure interaction the fog nodes and other users. Staying connected to these devices through the integration of blockchain technology ensures that data [35], [36] .

5. PROPOSED SCHEME

The work presented in this paper about the fog-enabled private blockchain-based identity authentication scheme in the Oil and Gas Field monitoring focuses on identity authentication with secure, efficient, and scalable blockchain networks. The scheme is divided into three main phases: Registration: Creating an Account and Logging in. All phases play an essential role in safeguarding the system.

Table.1. Description of Notations

Notation	Description
FID	Identity of the fog node
SID	Identity of the specified smart device
PDi	Pseudo-identity of the end user
IDi	Identity of the end user
Puk_u	Public key of entity *u*
Prk_u	Private key of entity *u*
Gen	Generation algorithm of the fuzzy extractor
BC	Blockchain in the proposed scheme
Rep	Reproduce algorithm of the fuzzy extractor
SC	Smart contract
T_i	Timestamp
ΔT	Maximum transmission delay
TA	Trusted authority
U_i	i^th user
P_i	Smartphone of U_i
n	Nonce
$h(\cdot)$	One-way hash function
A	Attacker
ReqCard	Registration card containing fog node and smart device IDs and signature
ReqAuth	Authentication request
Access Credential	Access credentials issued by the blockchain
M_1	Message 1 in off-chain authentication
M_2	Message 2 in off-chain authentication
Signed(M)	Digital signature of message MM using the sender's private key
MAC1	Media access control address of entity i
TOKEN	Token generated for authentication
ω	Biometric information (e.g., fingerprint)
PW_i	Passphrase of the end user
s	Secret string generated by the fuzzy extractor
r	Auxiliary string generated by the fuzzy extractor

The Table.2 depicts all the notations used in the proposed scheme which will help the reader understand, which components and operations are included in the fog-enabled private blockchain-based identity authentication system for Oil and Gas Field monitoring.

5.1 INITIALIZATION PHASE

initialization stage trusted authority (TA) to perform initialization of the fundamental components necessary for secure identification and communication within the network::

5.1.1 Identity Generation:

- Set distinct identities ID for All the entities in the network like fog nodes, IoT devices and users. These IDs are unique identifiers that generated by using a hash function (ID_i =hash(MAC_i)) on the entity's media access control (MAC) address.

5.1.2 Key Pair Generation:

- The TA generates a public-private key pair for All entities. These keys are used for encryption, decryption, and digital signatures within the authentication process.
- Public-Private Key Pair: (Puk_u, Prk_u), where *u* represents the entity.

5.1.3 Fog Node and Device Mapping:

- Each smart device in the Oil and Gas Field is mapped to a corresponding fog node based on predefined mapping rules. This mapping ensures efficient management and authentication of devices.

5.1.4 Token Generation:

- Fog nodes generate a token (ReqCard) for each smart device they manage. The token includes the fog node ID (FID), smart device ID (SID), and a signature created using the fog node's private key.
- Token: $ReqCard=\{FID,SID,Signature_{FID}\}$

5.1.5 Blockchain Initialization:

- The initialization information, including the IDs and public keys of all entities, is recorded on the private blockchain in the form of transactions. This ensures that all subsequent actions can be securely verified.

Algorithm 1: Initialization Phase

Input: List of Fog Nodes (FN), IoT Devices (ID), Users (Ui)

Output: Initialized Blockchain (BC) with IDs and $Keys$

```
For all entities the ($TA$) generates unique IDs and Key
Pairs:
    for each $FN$ in Fog Nodes do
        $FID \leftarrow hash(MAC_{FN})$
        $(Puk_{FN}, Prk_{FN}) \leftarrow generate\ key\ pair()$
    end for
    for each $ID$ in IoT Devices do
        $SID \leftarrow hash(MAC_{ID})$
        $(Puk_{ID}, Prk_{ID}) \leftarrow generate\ key\ pair()$
    end for
    for each U_i in Users do
        $ID_i \leftarrow generate\ unique\ id()$
        $(Puk_{Ui}, Prk_{Ui}) \leftarrow generate\ key\ pair()$
    end for

Fog Nodes generate tokens for IoT Devices:
    for each $FN$ in Fog Nodes do
        for each $ID$ assigned to $FN$ do
            $ReqCard \leftarrow \{FID, SID, sign_{(FID,Prk\_FN)}\}$
        end for
    end for

Store Initialization Data on Blockchain ($BC$):
    for each $FN$, $ID$, $U_i$ do
        store on blockchain($BC, \{FID, Puk_{FN}\}$)
        store on blockchain($BC, \{SID, Puk\_ID\}$)
        store on blockchain($BC, \{ID_i, Puk_{Ui}\}$)
    end for

4. Confirm Initialization:
    return Initialization_Confirmed
```

5.2 REGISTRATION PHASE

The registration phase involves registering all entities, including fog nodes, IoT devices, and users, on the blockchain. This phase ensures that each entity is authenticated, and their information is securely stored.

5.2.1 *Fog Node Registration:*

- Fog nodes submit a request to registrar in blockchain, which triggers a smart contract for verification.
- The fog node's verifies the identity using MAC address on TA. If verified, the fog node is added to the blockchain network as a full node.
- Registration Transaction: $ReqRegistration(MACFID,FID)$

Algorithm Fog Node Registration

Input: Fog Node (FN), Blockchain (BC)

Output: Registered Fog Node (FN)

```
1. FN submits registration request to BC:
    ReqRegistration $\leftarrow \{MAC_{\mathrm{FN}}, FID\}$
2. TA verifies FN information:
if verify($FID, MAC_{FN}$) then
        store on blockchain($BC, \{FID, Puk_{FN}\}$)
        return FN_Registered
    else
        return Registration Failed
    end if
```

5.2.2 *Smart Device Registration:*

- Each smart device, along with information about its managing fog node, submits a registration request to the blockchain.
- The smart contract verifies the smart device's identity and its association with the fog node. If verified, the device is added to the blockchain.
- Registration Transaction:

$ReqRegistration(MAC_{FID}, FID, MAC_{SID}, SID, ReqCard_{FID}, Puk_{SID})$

IoT Device Registration Algorithm

Input: IoT Device (ID), Fog Node (FN), Blockchain (BC)

Output: Registered IoT Device (ID)

```
ID submits registration request through FN to BC:
    ReqRegistration ← {MAC_FN, FID, MAC_ID, SID, ReqCard,
Puk_ID}
TA verifies ID and FN information:
    if verify(SID, MAC_ID) and verify(FID, MAC_FN) and
verify_token(ReqCard) then
        store_on_blockchain(BC, {SID, Puk_ID})
        return ID_Registered
    else
        return Registration_Failed
    end if
```

5.2.3 *User Registration:*

- Users register with the TA by submitting their unique identity, passphrase, and biometric information (e.g., fingerprint).
- The TA calculates a pseudo-identity (PID) for the user and stores the user's information on the blockchain.
- User's mobile device stores the PID and other necessary information for future authentication.
- Registration Process: $\{ID_i, PW_i, \omega\} \rightarrow Gen(\omega) = (s, r) \rightarrow PW_1 = h(PW_i \parallel s)$

User Registration Algorithm

Input: User (U_i), Fog Node (FN), Blockchain (BC)

Output: Registered User (U_i)

```
User ($U_i$) generates $PID$ and submits registration request to $FN$:
    $PID_i \leftarrow hash(ID_i, r)$
    ReqRegistration $\leftarrow \{ID_i, PW_i, \omega\}$
    $(s, r) \leftarrow Gen(\omega)$
    $PW_i \leftarrow hash(PW_i, s)$
$FN$ verifies user information and generates $PID$:
    if verify user ($ID_i, PW_i, \omega$) then
        store on blockchain ($BC, \{PID_i, r\}$)
        return User Registered
```

```
else
    return Registration Failed
end if
```

6. AUTHENTICATION PHASE

The authentication phase involves mutual authentication between users and IoT devices, facilitated by fog nodes. This ensures that only authorized users can access the devices and data.

6.1 USER AUTHENTICATION REQUEST

6.1.1 User Initiates Authentication:

- The user initiates authentication by entering their identity (IDi), password (PWi), and biometric information (ω) on their mobile device (Pi).
- The mobile device verifies the user's identity using a fuzzy extractor: Rep$(\omega,r)\rightarrow s*$ $UPW*=h(IDi\|s*)$ If $UPWi=UPW*$, the user is authenticated locally.

6.1.2 Submit Authentication Request:

- The mobile device submits an authentication request to the blockchain, triggering a smart contract.
- **Authentication Request:** ReqAuth(IDi, PWi, SID)

Algorithm 3: User Authentication Request

Input: User Identity (ID_i), Password (PW_i), Biometric Information (ω), Smart Device ID (SID)

Output: Access Credential (AccessCredential)

```
1. User enters ID_i, PW_i, ω on mobile device (P_i).
2. Mobile device verifies user identity using fuzzy extractor:
   (s^*, r) <- Gen(ω)
   UPW^* = h(ID_i || s^*)
   if UPW_i != UPW^* then
       return Authentication Failed
   end if
3. Mobile device submits authentication request to blockchain:
   ReqAuth(ID_i, PW_i, SID)
```

6.2 BLOCKCHAIN AUTHENTICATION

6.2.1 Smart Contract Verification:

- The smart contract on the blockchain verifies the user's pseudo-identity ($PIDi$) and the smart device's identity (SID).
- If verified, it returns an access credential.

6.2.2 Access Credential:

- The access credential includes a token ($TOKEN$), the user's pseudo-identity ($PIDi$), the fog node ID (FID), and a timestamp ($T1$).
- **Access Credential:** AccessCredential=$\{TOKEN,r,PIDi,FID,T1,\Delta T\}$

Algorithm 4: Blockchain Authentication

Input: Authentication Request (ReqAuth)

Output: Access Credential (AccessCredential)

```
1. Smart contract verifies user's pseudo-identity (PID_i) and
smart device ID (SID):
  if verify(PID_i) and verify(SID) then
      TOKEN = h(SID || PID_i || FID)
      AccessCredential = {TOKEN, r, PID_i, FID, T_1, ΔT}
      return AccessCredential
  else
      return Authentication Failed
  end if
```

6.3 OFF-CHAIN AUTHENTICATION

6.3.1 User Sends Access Credential:

- The user sends the access credential to the fog node managing the smart device.
- **Message 1 (M1):** $M1=\{TOKEN,r,PIDi,T2,n,\Delta T\}$
- Signed($M1$) $Pukuser$

6.3.2 Fog Node Verifies Credential:

- The fog node verifies the access credential and the user's signature.
- If valid, it sends a response message back to the user.
- Message 2 (M2): $M2=\{n-1,T3,\Delta T\}$ Signed($M2$) $PukFID$

6.3.3 Mutual Authentication:

- **User to Fog Node:** $\{M1$, Signed($M1$), $Pukuser\}$
- **Fog Node to User:** $\{M2$, Signed($M2$), $PukFID\}$

Algorithm 5: Off-Chain Authentication

Input: Access Credential (AccessCredential), Fog Node ID (FID), User's Public Key (Puk_user)

Output: Secure Communication Channel

```
1. User sends access credential to fog node:
  M_1 = {TOKEN, r, PID_i, T_2, n, ΔT}
  Signed(M_1)
  Puk_user
2. Fog node verifies access credential and user's signature:
  if verify(TOKEN, r, PID_i, FID, T_1) and
verify_signature(Signed(M_1), Puk_user) then
      M_2 = {n-1, T_3, ΔT}
      Signed(M_2)
      Puk_FID
      send M_2 to user
  else
      return Authentication Failed
  end if
3. User verifies fog node's signature and nonce:
  if verify signature (Signed(M_2), Puk_FID) and (n-1 ==
n_received) then
      establish secure channel()
      return Secure Communication Established
  else
      return Authentication Failed
  end if
```

6.4 SECURE COMMUNICATION ESTABLISHMENT

- Upon successful mutual authentication, a secure communication channel is established between the user and the smart device.
- The user can now access the smart device and its data securely.

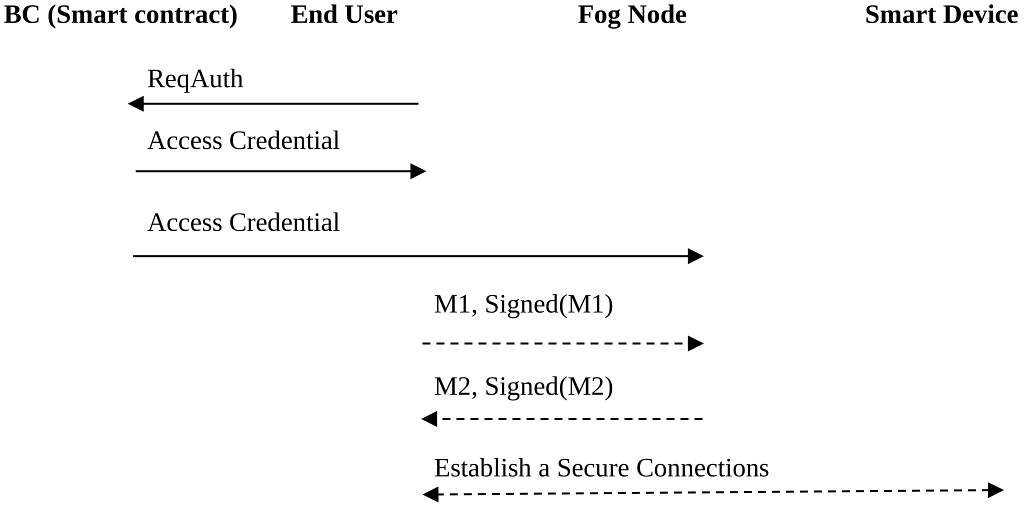

Fig.3. Sequence Diagram - exchange messages between end user to the smart device

These algorithms and the sequence diagram outline the steps involved in the enhanced authentication phase, ensuring a secure and efficient mutual authentication process between users and IoT devices in the fog-enabled private blockchain-based identity authentication system for Oil and Gas Field monitoring.

7. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

In this section, first, outline the general and specific security requirements of a typical IoT setting in which the Oil and Gas Field monitoring is to be established; second, examine the level of security provided by the proposed fog-enabled private blockchain-based identity authentication scheme; third, examine and discuss the results stemming from the performance assessment of the proposed scheme. The security requirements that are applicable to the IoT environment are security of privacy, and security of data confidentiality, data received, and data transmission. In the next section, describe how our scheme fulfills the above security goals and analyze its efficiency.

7.1 SECURITY ANALYSIS

The proposed fog-enabled private blockchain-based identity authentication scheme for Oil and Gas Field monitoring robustly addresses numerous security challenges inherent in IoT environments. Here, we provide evidence from our proposed scheme to demonstrate its effectiveness in combating these security threats.

- **Denial of Service (DoS):** Though there is a potential problem of DoS attacks, our scheme harnesses the strength of fog computing to prevent this. When the information is processed over multiple fog nodes, high volumes of authentication requests inundating a single node can be addressed. Moreover, the decentralized architecture of the blockchain guarantees there is no individual node controlling all the operations, making it harder for DoS attacks to come into play. Every scrub has its own authentication processing even when some of them are affected or attacked in another way the system will still function as the other scrub is processing the request.
- **Man-in-the-Middle (MITM) Attack:** Thus, in order to address MITM threats, our scheme utilizes a high-quality encryption and digital signing mechanisms. Neither the users' messages, fog nodes' information, or the IoT devices interact without the encryption done with the help of public private keys. In mutual authentication process, user equipment and the fog node each exchange signed messages that proves it's identity. This checks and balances system makes it impossible for anyone to intercept or modify messages in mid- transfer.
- **Replay Attack:** The proposed scheme includes timestamps and nonces in each authentication message to prevent replay attacks. Each authentication request contains a unique timestamp and a nonce, ensuring that even if an attacker intercepts a message, they cannot reuse it at a later time. The smart contracts on the blockchain verify these timestamps and nonces, rejecting any requests that appear to be duplicates.
- **Sybil Attack and Spoofing Attack:** They have played positives roles where Sybil and spoofing attacks are eradicated with the use of blockchain and trusted authority registration. Fog nodes, as well as IoT devices, are required to achieve a registration, which makes them issue a trusted identification number checked on the blockchain. This method also helps in denying the attacker the ability to create multiple fake IDs or the ability to copy legitimate IDs.

- **Message Substitution Attack:** Digital signatures safeguard against message substitution attacks. Each message in the authentication process is digitally signed by the sender's private key and verified using the sender's public key. This ensures that any attempt to substitute a message with a fraudulent one will be detected, as the signature will not match the expected value.
- **Privacy and Anonymity:** User privacy and anonymity are preserved through the use of pseudo-identities (PIDs). Instead of using actual user identities, the scheme uses PIDs for authentication. Biometric information is processed using fuzzy extractors, ensuring that sensitive data is not exposed. Transactions on the blockchain use hashed values and PIDs, further protecting user privacy and ensuring anonymity in the network.
- **Mutual Authentication:** The scheme helps in achieving user-IoT device authentication wherein every user gains assurance of the credibility of the IoT device, and at the same time, the IoT device also gains assurance of the credibility of the user. As for the steps of the authentication, the two INVITEs exchange signed messages that include the ID, timestamp, and nonce of the parties. This mutual exchange then confirms not only the user identity but the device identity as well to prevent unauthorized use.
- **Non-repudiation:** Non-repudiation is achieved through the use of blockchain and digital signatures. Each transaction and authentication request is recorded on the blockchain, providing a verifiable and immutable record of all actions. Digital signatures ensure that the origin of each message can be verified, preventing any party from denying their involvement in a transaction or communication.
- **Other Security Measures:** Hence, there is a significant improvement in the overall security and robustness of the analytical scheme tested in this paper due to its decentralized structure and fog computing. Through the dispersion of control and data in the nodes, it is easier to work without a particular node that at any given time may fail. Smart contracts adopted in the process of verification also helps in elimination of human interference resulting into the efficient process of authentication.

7.2 FORMAL ANALYSIS

We introduce the AVISPA tool in this section, AVISPA is a popular software used for verifying the security of cryptographic protocols. It helps determine if a protocol is secure or vulnerable to known attacks by checking it against established security models using a special coding language called High-Level Protocol Specification Language (HLPSL).

```
/* HLPSL Specification for Fog-
enabled Private Blockchain-based
Identity Authentication Scheme */
Role user(U, F, I : agent, PKU,
SKF, SKI : public.key, S, T : text)
played_by U
def=
 local
   State: nat
   NonceU, NonceF. : text
   SID : text
   X, Y, Z : text
 init
   State := 0
 transition
   0.  State = 0 /\ start(U, F, I, PKU,
SKF, SKI, S, T) =|>
       State' := 1 /\
       NonceU' := new()
       request(U, F, NonceU', S, T)
       sid' := S
   1.  State = 1 /\ request(F, U,
NonceU, NonceF, PKU) =|>
       State' := 2 /\
       NonceF' := new()
       X' := pkcrypt(SKF, {NonceU,
NonceF, SID, U})
       send(U, F, X')
   2.  State = 2 /\ receive(F, U,
NonceF, Y) =|>
       State' := 3 /\
       Z' := pkcrypt(SK_I, {NonceF,
SID, F})
       send(U, I, Z')
end role
```

```
Role fog(F, U, I : agent,
PKU, SKF, SKI :
public._key, S, T : text)
played_by F
def=
 local
   State: nat
   NonceU, NonceF : text
   SID : text
   X, Y, Z : text
 init
   State := 0
 transition
   0.  State = 0 /\ start(U, F,
I, PKU, SKF, SKI, S, T)
=|>
       State' := 1 /\
       NonceF' := new()
       request(F, U,
NonceU, NonceF, PKU)
   1.  State = 1 /\
receive(U, F, NonceU, X)
=|>
       State' := 2 /\
       Y' := pkcrypt(SKF,
{NonceF, SID, F})
       send(F, U, Y')
end role
```

```
Role iot(I, U, F : agent, PKU,
SKF, SKI : public_key, S, T :
text)
played_by I
def=
 local
   State: nat
   NonceF, SID : text
   X, Y, Z : text
 init
   State := 0
 transition
   0.  State = 0 /\ start(U, F, I,
PKU, SKF, SKI, S, T) =|>
       State' := 1
   1.  State = 1 /\ receive(U, I,
Z) =|>
       State' := 2 /\
       request(I, U, NonceF,
SID)
end role
```

```
Role session(U, F, I : agent,
PKU, SKF, SKI : public_key, S,
T : text)
def=
 composition
   user(U, F, I, PKU, SKF, SKI,
S, T) /\ fog(F, U, I, PKU, SKF,
SKI, S, T) /\ iot(I, U, F, PKU,
SKF, SKI, S, T)
end role
environment()
def=
 const
   U, F, I : agent
   PKU, SKF, SKI : public_key
   S, T : text
 intruder_knowledge = {U, F, I,
PKU, SKF, SKI}
 init
   composition
     session(U, F, I, PKU, SKF,
SKI, S, T)
end role
```

The proposed scheme's HLPSL specification is analyzed using the Security Protocol Animator for AVISPA (SPAN) simulation tool. The results from the CL-AtSe and OFMC back-ends indicate that the proposed protocol is SAFE against well-known attacks such as MITM, replay, and impersonation attacks. The analysis also confirms that the secrecy of the session key is maintained. Thus, the proposed model is suitable for practical use cases requiring robust authentication, such as smart agriculture, smart healthcare, and banking sectors.

OFMC	CL-AtSe

SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/fog_authentication.if
GOALS
  secrecy_of(NonceU)
  secrecy_of(SID)
  authentication_on(NonceU)
BACKEND
  OFMC
COMMENTS
STATISTICS
  Searchtime: 0.08 seconds
  Parsingtime: 0.01 seconds
  Nodes visited: 60
  Depth of search: 10
	SUMMARY
	SAFE
	DETAILS
	BOUNDED_NUMBER_OF_SESSIONS
	  TYPED_MODEL
	PROTOCOL
	/home/span/span/testsuite/results/fog_authentication.if
	GOALS
	  secrecy_of(NonceU)
	  secrecy_of(SID)
	  authentication_on(NonceU)
	BACKEND
	  CL-AtSe
	STATISTICS
	  Analtysed : 0 states
	  Reachable : 0 states
	  Translation: 0.00 s
	  Computation: 0.00 s

8. PERFORMANCE EVALUATION

The blockchain-based authentication scheme proposed in this paper uses fog nodes to provide a set of localized computing services for the whole network so that data does not have to be sent to the cloud for processing each time, which greatly reduces the latency. At the same time, all fog nodes are added to the blockchain and each fog node manages a set of smart devices. This setup allows users to authenticate with the fog node managing the device instead of directly communicating with the smart device, streamlining the process.

Additionally, since the authentication process is performed in a decentralized manner on the blockchain, the authentication authority is composed of multiple fog nodes, which increases the system's throughput. Smart devices in IoT have limited storage capacity and computing power, so they are registered to join the blockchain only as light nodes. In contrast, fog nodes possess relatively powerful computing power and memory space, making them suitable for storing most of the data written to the blockchain ledger during the authentication process.

In this section, we analyze the performance of the proposed scheme to verify its effectiveness. Due to the lack of specific reference objects for blockchain-based smart home authentication schemes using fog nodes, we cannot prove our effectiveness by comparing it with other schemes. Instead, we analyze each phase of the authentication scheme to obtain its communication cost and computational overhead to assess whether the scheme meets the design requirements.

8.1 COMPUTATIONAL OVERHEAD

In this subsection, we evaluate the computational overhead of the proposed fog-enabled private blockchain-based identity authentication scheme. The analysis focuses on the computational requirements of different entities (users, fog nodes, and IoT devices) during the registration and authentication phases. This assessment will help demonstrate the practicality and effectiveness of the scheme in real-world deployments.

- **User Authentication :** The computational overhead for users primarily involves cryptographic operations required for generating nonces, encrypting authentication requests, and verifying digital signatures. Users generate a nonce, encrypt the authentication request using their public key (PukU), and perform digital signature verification upon receiving responses.
- **Fog Node Processing :** Fog nodes are pivotal in the authentication process, handling significant computational tasks such as decrypting incoming requests, verifying and generating digital signatures, and interacting with the blockchain. The fog nodes decrypt messages using their private key (PrkF) and verify the signatures to ensure message authenticity. Additionally, they generate new signatures for outgoing messages and validate transactions on the blockchain.
- **IoT Device Registration and Authentication:** IoT devices registered as light nodes due to their limited computational and storage capacities have minimized computational overhead. During the registration and authentication phases, they perform essential cryptographic operations such as encryption, decryption, and digital signature verification. Despite their limited resources, the offloading of intensive tasks to fog nodes allows IoT devices to function efficiently.

The evaluation of the suggested fog-enabled private blockchain-based identity authentication scheme from an implementation perspective demonstrates that the solution is viable for integration into practical systems. the proposed scheme equitably divides the computational tasks between the users, fog nodes to utilize each of them at best since all of them have their specific abilities. Users and smart things are required to perform basic cryptographic operations that can be managed in conventional computational power, but IoT nodes perform more complex computations and blockchain operations. This efficient division of the computational work supports the structure of the scheme and therefore it can be deemed as highly applicable to providing secure and efficient identity authentication in IoT applications such as monitoring of Oil and Gas Field.

The time for performing the cryptographic primitives used in the scheme is presented on Table.2. By observing the above table, we can conclude that the hash functions, the message authentication codes, the and the fuzzy extractors require considerably low computation time which well fits the IoT devices. The complex mathematical computations including (T_h , T_{hamc} , T_{mac} , T_e , T_{ed} , T_f, T_{PB}, T_{Req}) will be managed by the fog nodes and also the blockchain.

Table.2. Approximate running time of cryptographic primitives

Operation	Computation Cost (s)
$Hash\ MAC\square T_h$	0.0052
$Hash\ function T_{hamc}$	0.0052
$Message\ authentication\ code\ T_{mac}$	0.0052
$multiplication\ of\ ECC\ point T_e$	0.0171

$Symmetric\ decryption\ /encryptionT_{ed}$	0.0215
$Fuzzy\ extractor\ Gen/RepT_f$	0.0171
$Pairing\ BilinearT_{PB}$	0.496
$Request\ Generate\ in\ BCT\ T_{Req}$	0.001

The computational costs of our proposed scheme are compared with those of other related schemes in Table 2. Our scheme demonstrates a lower computational cost, which indicates its efficiency. This comparison further highlights the advantages of integrating fog computing with blockchain technology to distribute the computational load effectively.

Table 3. Comparison of computations cost

Proposed scheme	**Total of computations cost**
Arun et al. [37]	$2T_{ed}$ +$23T_h$=0.1626
Khalid et al. [38]	$2T_{ed}$ + T_{Req} + T_h=0.0492
Arun et al. [39]	$3T_{ed}$ + T_{Req} + $2T_h$=0.0759
Singh and Chaurasiya [40]	$2T_{ed}$ + T_{PB} + $7T_h$ = 0.5487
Namane et al. [41]	$2T_{ed}$ + $13T_h$ =0.1106
Our	T_f +T_{Req} +$2T_h$ = 0.0285

9. CONCLUSION

The proposed fog-enabled private blockchain for Oil and Gas Field monitoring and identity authentication tackles crucial issues in efficacy, security, and delay. Fog computing along with the blockchain system helps to enhance identity authentication by incorporating IoT devices integrated with the blockchain to improve authenticity and security while using multiple localized fog nodes to process data effectively and make the result more scalable.

Our approach utilizes fog nodes as intermediaries to bridge IoT devices and the blockchain, which evidently decreases the communication lag and increases the system's performance. Private blockchains have strict access controls and admittance rights for the participants in the chain, which guarantees maximum efficiency and security. Moreover, the use of fuzzy extractors improves system privacy and security through the management of biometric details. From the analysis, insights, and security and privacy threats described in this paper, it is evident that our scheme is robust to counter DoS, MITM, replay, Sybil, and message substitution forged attacks. The formal verification performed with the AVISPA tool corroborates the fact that the developed protocol is secure against major known threats thus protecting the session key confidentiality and applying a strong mutual authentication.

From the performance analysis, there is a low computational and communication overhead that are specific for real-time systems. This distribution of computing tasks enables the compromising of load between the users, fog nodes and IoT devices while at the same time precluding the overpowering of one entity by the other in terms of resource utilization. In conclusion, the approach of using a fog enabled private blockchain-based identity authentication can assert that this approach can effectively and efficiently monitor and manage Oil and Gas Fields, which is a highly demanding industry, and is also scalable and secure.

REFERENCES

[1] T. Miller, A. Staves, S. Maesschalck, M. Sturdee and B. Green, "Looking Back to Look Forward: Lessons Learnt from Cyber-Attacks on Industrial Control Systems", *Proceedings of International Conference on Journal of Critical Infrastructure Protection*, Vol. 35, pp. 100464-100523, 2021.

[2] A. Bendovschi, "Cyber-Attacks - Trends, Patterns and Security Countermeasures", *Procedia Economics and Finance*, Vol. 28, pp. 24-31, 2015.

[3] K. Chen, "Internet-of-Things Security and Vulnerabilities: Taxonomy Challenges and Practice", *Journal of Hardware and Systems Security*, Vol. 2, No. 2, pp. 97-110, 2018.

[4] I. Butun, P. Osterberg and H. Song, "Security of the Internet of Things: Vulnerabilities Attacks and Countermeasures", *Proceedings of International Conference on Communications Surveys and Tutorials*, Vol. 22, No. 1, pp. 616-644, 2019.

[5] M.G. Samaila, M. Neto, D.A.B. Fernandes, M.M. Freire and P.R.M. Inacio, "Challenges of Securing Internet of Things Devices: A Survey", *Security and Privacy*, Vol. 1, No. 2, pp. 20-36, 2018.

[6] S. Drame-Maigne, M. Laurent, L. Castillo and H. Ganem, "Centralized Distributed and Everything in between: Reviewing Access Control Solutions for the IoT", *ACM Computing Surveys*, Vol. 54, No. 7, pp. 1-34, 2021.

[7] K. Yue, "A Survey of Decentralizing Applications Via Blockchain: The 5G and beyond Perspective", *Proceedings of International Conference on Communications Surveys and Tutorials*, Vol. 23, No. 4, pp. 2191-2217, 2021.

[8] R.A. Luchian, G. Stamatescu, I. Stamatescu, I. Fagarasan and D. Popescu, "Iiot Decentralized System Monitoring for Smart Industry Applications", *Proceedings of International Conference on Control and Automation*, pp. 1161-1166, 2021.

[9] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P.K. Singh and W.C. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems", *IEEE Access*, Vol. 8, pp. 54371-54401, 2020.

[10] Z.S. Ageed and S.R.M. Zeebaree, "Distributed Systems Meet Cloud Computing: A Review of Convergence and Integration", *International Journal of Intelligent Systems and Applications in Engineering*, Vol. 12, No. 11, pp. 469-490, 2024.

[11] P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain", *Big Data and Cognitive Computing*, Vol. 7, No. 4, pp. 165-172, 2023.

[12] R. Yang, "Public and Private Blockchain in Construction Business Process and Information Integration", *Automation in Construction*, Vol. 118, pp. 103276-103290, 2020.

[13] N. Ghadimi, Z.D. Koozehkanani and S.A. Mortazavi, "Presenting a Blockchain-Based Nonlinear Model for the Security of Smart Home", *International Journal of*

Nonlinear Analysis and Applications, Vol. 34, No. 3, pp. 1-13, 2024.

[14] Y. Zhao, Y. Qu, Y. Xiang, Y. Zhang and L. Gao, "A Lightweight Model-based Evolutionary Consensus Protocol in Blockchain as a Service for IoT", *IEEE Transactions on Services Computing*, Vol. 16, No. 4, pp. 2343-2358, 2023.

[15] H. Zeng, G. Dhiman, A. Sharma, A. Sharma and A. Tselykh, "An IoT and Blockchain-Based Approach for the Smart Water Management System in Agriculture", *Expert System*, Vol. 40, No. 4, pp. 12892-12995, 2023.

[16] T. Bosona and G. Gebresenbet, "The Role of Blockchain Technology in Promoting Traceability Systems in Agri-Food Production and Supply Chains", *Sensors*, Vol. 23, No. 11, pp. 5342-5356, 2023.

[17] P.C. Sharma, M.R. Mahmood, H. Raja, N.S. Yadav, B.B. Gupta and V. Arya, "Secure Authentication and Privacy-Preserving Blockchain for Industrial Internet of Things", *Computers and Electrical Engineering*, Vol. 108, pp. 1-17, 2023.

[18] C. Toma and M. Popa, "IoT Security Approaches in Oil and Gas Solution Industry 4.0", *Informatica Economica*, Vol. 22, No. 3, pp. 46-61, 2018.

[19] Y. Zuo and Z. Qi, "A Blockchain-based IoT Framework for Oil Field Remote Monitoring and Control", *IEEE Access*, Vol. 10, pp. 2497-2514, 2021.

[20] G.A. Senthil, P. Suganthi, R. Prabha, M. Madhumathi, S. Prabhu and S. Sridevi, "An Enhanced Smart Intelligent Detecting and Alerting System for Industrial Gas Leakage using IoT in Sensor Network", *Proceedings of International Conference on Smart Systems and Inventive Technology*, pp. 397-401, 2023.

[21] P. Chattopadhyay, H.P. Patel and V. Parmar, "Internet of Things in Smart Agriculture", *Proceedings of International Conference on Electronics and Sustainable Communication Systems*, pp. 536-540, 2022.

[22] J. Cui, Y. Zhu, H. Zhong, Q. Zhang, C. Gu and D. He, "Efficient Blockchain-Based Mutual Authentication and Session Key Agreement for Cross-Domain IIoT", *IEEE Internet of Things Journal*, Vol. 11, No. 9, pp. 16325-2024, 2024.

[23] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen and J. Chang, "Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT", *IEEE Internet of Things Journal*, Vol. 9, No. 22, pp. 22501-22515.

[24] N. Islam, Y. Faheem, I.U. Din, M. Talha, M. Guizani and M. Khalil, "A Blockchain-based Fog Computing Framework for Activity Recognition as an Application to E-Healthcare Services", *Future Generation Computer Systems*, Vol. 100, pp. 569-578, 2019.

[25] R.L. Kumar, F. Khan, S. Kadry and S. Rho, "A Survey on Blockchain for Industrial Internet of Things: Blockchain for Internet of Things", *Alexandria Engineering Journal*, Vol. 61, No. 8, pp. 6001-6022, 2022.

[26] A. Dorri, S.S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT Security and Anonymity", *Journal of Parallel and Distributed Computing*, Vol. 134, pp. 180-197, 2019.

[27] F.N. Tareen, "Efficient Load Balancing for Blockchain-Based Healthcare System in Smart Cities", *Applied Sciences*, Vol. 13, No. 4, pp. 2411-2432, 2023.

[28] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi and K. Salah, "A user Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes", *Proceedings of International Conference on Computer Systems and Applications*, pp. 1-8, 2018.

[29] S.H. Jang, J. Guejong, J. Jeong and B. Sangmin, "Fog Computing Architecture based Blockchain for Industrial IoT", *Proceedings of International Conference on Computational Science*, pp. 593-606, 2019.

[30] M.I. Lopez and A. Barsoum, "Traditional Public-Key Cryptosystems and Elliptic Curve Cryptography: A Comparative Study", *International Journal of Cyber Research and Education*, Vol. 4, No. 1, pp. 1-14, 2022.

[31] S. Mahmood, M. Gohar, J.G. Choi, S.J. Koh, H. Alquhayz and M. Khan, "Digital Certificate Verification Scheme for Smart Grid using Fog Computing", *Sustainability*, Vol. 13, No. 5, pp. 2549-2560, 2021.

[32] R. Praveen and P. Pabitha, "A Secure Lightweight Fuzzy Embedder based User Authentication Scheme for Internet of Medical Things Applications", *Journal of Intelligent and Fuzzy Systems*, Vol. 44, No. 5, pp. 7523-7542, 2023.

[33] X. Xu, Y. Guo and Y. Guo, "Fog-Enabled Private Blockchain-based Identity Authentication Scheme for Smart Home", *Computer Communications*, Vol. 205, pp. 58-68, 2023.

[34] F.G. Ghajar, A. Sikora and D. Welte, "Schloss: Blockchain-Based System Architecture for Secure Industrial IoT", *Electronics*, Vol. 11, No. 10, pp. 1-13, 2022.

[35] W. Wang, H. Xu, M. Alazab, T.R. Gadekallu, Z. Han and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices", *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 10, pp. 7059-7067, 2022.

[36] L. Fu, "Blockchain-Enabled Device Command Operation Security for Industrial Internet of Things", *Future Generation Computer Systems*, Vol. 148, pp. 280-297, 2023.

[37] C. Zhang, L. Zhu, and C. Xu, "BPAF: Blockchain-Enabled Reliable and Privacy-Preserving Authentication for Fog-based IoT Devices", *IEEE Consumer Electronics Magazine*, Vol. 11, No. 2, pp. 88-96, 2022.

[38] U. Khalid, M. Asim, T. Baker, P.C.K. Hung, M.A. Tariq and L. Rafferty, "A Decentralized Lightweight Blockchain-based Authentication Mechanism for IoT Systems", *Cluster Computing*, Vol. 23, No. 3, pp. 2067-2087, 2020.

[39] M. Arun, B.S. Rawal, R. Lakshmana Kumar and B. Balamurugan, "Mutual Authentication and Authorized Data Access Between Fog and user based on Blockchain Technology", *Proceedings of International Conference on Communications*, pp. 37-42, 2020.

[40] S. Singh and V.K. Chaurasiya, "Mutual Authentication Scheme of IoT Devices in Fog Computing Environment", *Cluster Computing*, Vol. 24, No. 3, pp. 1-12, 2020.

[41] S. Namane, M. Ahmim, A. Kondoro and I. Ben Dhaou, "Blockchain-Based Authentication Scheme for Collaborative Traffic Light Systems using Fog Computing", *Electronics*, Vol. 12, No. 2, pp. 1-14, 2023.