LAM-IoT: Lightweight Authentication Model for monitoring systems in IoT-enabled smart homes based on DID using IOTA

Sameera Abbas Fadhel1 and Dr. Ahmed S. Nori2

[1] Computer Science Department, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq
[2] Cyber Security Department, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq
*Corresponding Author: Sameera Abbas Fadhel

ABSTRACT

The Internet of Things (IoT) is an important technology; however, it has many security vulnerabilities. The authentication process is essential for ensuring the security of the whole IoT systems, as it serves as the first line of defense against different cyber-attacks. Traditional techniques of authentication are frequently centralized, which are unable to satisfy the requirements of IoT in terms of scalability and resources' consumption. Some drawbacks of these techniques include their high computation costs, single point of failure, and violation of privacy. Decentralized authentication techniques are suggested as a solution to the problems with centralized authentication. Blockchain is a well-known technology that can be used to authenticate and grant high-trust, decentralized access to IoT devices and data. However, with its limitations in terms of scalability, throughput, and storage capacity, blockchain is an unsuitable option for devices with limited resources in the IoT environment. Hence, in order to overcome these problems, a more scalable solution approach is required to be formulated. In this paper, we propose a new lightweight authentication model for IoT-based smart house monitoring system utilizing IOTA Tangle, Decentralized Identifier (DID), and Stronghold vault technologies. We examined and confirmed the functionalities of the proposed model through automated security testing with the Scyther tool. The testing validated the proposed model's effectiveness. The model works efficiently in a constraint IoT environment, as shown by the analysis of additional assessment criteria like communication and storage costs.

KEYWORDS

IOTA, IoT, Authentication, DLT, DID.

1. INTRODUCTION

The Internet of Things (IoT) is a network of interconnected heterogeneous devices and embedded sensors that have certain characteristics in common, like low power consumption, minimal memory, and restricted computing power [1]. The high number of interconnected devices through various protocols makes it susceptible to several forms of attacks. Therefore, there is a real need to build and develop lightweight authentication methods for the IoT devices [2]. Privacy and Security of data transmission, as well as the reliability and authenticity of the identity of entities engaging in network activities, were all considered as important issues [3]. Identification of entities in the digital world has always been a top priority. Authentication still depends on the usage of passwords and usernames, which is open to various attacks. Centralized identity managing systems rely on certain identity service nodes, and they may be susceptible to the single point of failure issue [4]. Decentralized identification techniques differ from conventional methods in that they do not depend on centralized identity providers (IdPs). Commonly, these decentralized systems make use of technologies such as blockchain, distributed file systems, decentralized ledger technology (DLT), and other new decentralized structures like tangles and hashgraphs [5][6]. Decentralized identities for IoT devices can be established using the IOTA Digital Identity framework, guaranteeing private and secure communication between them [7]. Decentralized Identity (DID) is a new kind of digital identity that is globally unique and linked to both a subject and a DID document. This DID identifies the entity that is referred to as the "Subject," also commonly known as the "DID subject" [8].

In this paper, we proposed a solution for IoT devices' identification and a data access control employing IOTA Tangle and identity technologies. The contributions of this paper are as follows:

1- Due to lack of a credible and provable identity, internal and external threats impinge on the network entity identities. On the same note, since the present relying on conventional Public Key Infrastructure (PKI) has a tendency of having a single point of failure through centralized Certificate Authorities (CAs), and the scalability issues arising with conventional blockchain based identity management solutions, there is need for a new more efficient, more lightweight identity management framework. This model uses Distributed Ledger Technology (DLT) employing IOTA which is Directed Acyclic Graph (DAG) based technology. It enhances the transactional throughput, decreases transaction confirmation time, minimizes control consumption and removes transaction charges hence being more suitable in the IoT setting.

2- We developed the conventional processes of identity management through syncing fog nodes that serve as master nodes with IOTA identity as well as Tangle. This optimization helps to facilitate the act of identity management for IoT devices within a very short time based on registration and authentication processes.

3- The layout generates a secure data transmission between edge device (Raspberry Pi) and master fog node which is paramount when it comes to data integrity and security. This communication is protected using the MQTT (Message Queuing Telemetry Transport) protocol regarding data exchanged in between these nodes; it is encrypted to prevent access or manipulation by unauthorized parties. Also, there is the issue of continual data acquisition from the sensors and their transmission through the IoT monitoring system. Sensors' data, necessary for users and to get a real-time control, is sent to the ThingSpeak cloud-based platform. ThingSpeak is an application that provides users with graphical displays and statistics of the sensors' readings. The information presented in this case not only helps in improving the monitoring of the data collected from the IoT sensors as well as helps in the decision making processes, as the data collected can be presented in the format which is easy for making decisions.

4- The experimental evaluation involves practical implementation where Raspberry Pi with few connected sensors interrelates with a fog node. The proposed model is explored and validated through security and functionality and verified using Scyther tool [9]. The lightweight security management requirements in the proposed model can satisfy the demand of IoT devices.

The remainder of this paper is structured as follows: Section 2 presents the existing work; Section 3 describes the essential technologies employed in this paper; Section 4 delineates the proposed model and provides an in-depth overview of it; Section 5 assesses the proposed model's performance, analyzes its security implications, and evaluates its functionality; and Section 6 summarizes the key findings and contributions of this research.

2. LITERATURE REVIEW

Previous studies and works that were used as main sources for this work will be discussed in this section. These studies and works are related to the topics of work on IOTA and DID-for IoT applications.

A novel approach to the management of secure identities for IoT devices is presented, which is based on self-sovereign identity. This approach provides an identity that is self-owned, controllable, unique, secure, interoperable, portable, decentralized, and persistent. The following four major contributions are made by this work: i) Developing an IoT device registration, identification assignment, issuance, and verifiable claim assertion system based on distributed ledger technology (DLT). ii) Design an algorithm for a trust score. iii) Developing a mechanism to mitigate risk. iv) Credentials or claims that can be verified. Entities could share their own claims to support their self-identity instead of sharing identifying information that has a higher level of privacy [10].

This study offers a new identification based on Distributed Ledger Technology (DLT) for IoT devices. The identities that IoT devices assign to themselves are known as Self Sovereign Identities (SSI), and they are controlled publicly and decentralized on the DLT network. The framework offers a Web of Trust (WoT) method in addition to the Identity Management System (IdMS) to allow automatic trust evaluation of any identity. Great scalability and low processing costs were achieved by accessing and storing data over the IOTA Tangle. The relationships between different identities and their recorded trust toward one another are presented in a WoT in order to support trust ratings [11].

An IoT architecture built on the IOTA Tangle network is proposed in this study. It solves the problem of safe communication between the sensor and the IOTA Tangle network by using a lightweight identity authentication method. To efficiently manage the identities of sensors and cluster heads, it also establishes a whitelist and blacklist method. The designed architecture includes Sensor Node, Cluster Head (CH), and Base Station (BS). It provides an authentication method between restricted IoT devices and the cloud, which can guarantee the data's integrity from generation to cloud. It also controls the device and decreases the management cost by keeping the device's identity in IOTA. This paper also separates the identity verification authority from the data storage [12].

We suggested a lightweight blockchain for IoT devices. In order to reduce the amount of resources used in mining, the Proof of Authentication (PoAh) was implemented as a consensus algorithm. To increase throughput and system response time, the DAG-based blockchain architecture was used. Conventional consensus algorithms require high energy consumption during mining. PoAh introduces a cryptographic authentication method as a consensus method to address this problem. PoAh uses fast and effective cryptographic techniques for its digital signature and hash function. A transaction's approval in the PoAh consensus method is determined by the full node based on the transaction creator's authority. The transaction will be approved if the creator's public key is included in the list of authorized devices [13].

The main goal of this study is to demonstrate how data preservation has been implemented and executed from industrial automation and control systems to IOTA. The suggested method for preserving data with IOTA DAG technology will be executed and implemented within simulation environment or a testbed. During the implementation phase, the performance of the data preservation process will be monitored and evaluated, with an emphasis on variables like cost-effectiveness, efficiency, and scalability. The system considered in this study contains three main components: Sensor Node, Cluster Head, and Base Station. This study focuses on perform identity authentication for sensing devices with limited resources and securely upload sensing data from these devices to the Tangle for storing [14].

In this study, the Transport Layer Security (TLS) security protocol will be modified and adapted to the Self-Sovereign Identity paradigm. This is done by using a decentralized digital identity model that depends on Decentralized Identifiers (DIDs) and Distributed Ledger Technology (DLT), like Blockchain and Tangle. DIDs can be thought of as addresses pointing to a DLT block. This work's primary goal was to give decentralized digital identities to Internet of Things devices in order to integrate them into the SSI ecosystem. These Internet of

Things-restricted devices may authenticate with each other through their decentralized digital identities and by using the SSI-aware TLS 1.2 protocol, which was executed into the Mbed TLS library [15].

DIVA was originally proposed in this work, which is a reputation system for secure transmission in VAnets based on Decentralized Identifiers. We specifically assert that it is appropriate to use IOTA for securely record reputation scores and Decentralized Identifiers (DIDs) for identifying participating vehicles. For the purposes of DIVA, every vehicle must have a unique ID in order to exchange road data with other network entities. To do this, participating vehicles are identified by DIDs, and their participation is controlled by Verifiable Credentials (VCs). The paper's main original contributions are as follows: i) We provide a novel VANET reputation scheme based on DID. ii) The first large-scale dataset has been created and released. iii) We have deployed and thoroughly tested DIVA in 5G-enabled deployment scenarios as well as against that dataset [16].

3. TECHNOLOGICAL FRAMEWORK

This section demonstrates the essential technologies that employed in the proposed model.

3.1 Distributed ledger

Due to the problem that arises from centralization which includes single points of failure, researchers have received distributed ledger technology a lot of attention because of the features such as decentralization, immutability, and public verifiability. One of the well-known Decentralized Ledger Technologies is Blockchain which is originally proposed by Nakamoto [17], it is changed the face of digital currency by introducing an innovative way to holds an open and digitally verifiable record of transactions without the requirement of a central authority. On the other hand, blockchain has several disadvantages that come with its innovative features inclusive of; scalability, the ever-higher energy demand because of Proof-of-Work consensus, high storage demands given the entire ledger will be stored, variable transaction fees, and potential privacy concerns on public blockchains. These aspects raise questions on the advisability of using blockchain especially for light weighted frameworks and their applications.

There are more types of DLT mentioned in the IOTA case, the so-called ‘Tangle’ employing a Directed Acyclic Graph (DAG). Tangle, the DAG structure of IOTA, eliminates problems like the orphan block and enhances scalability which are factors seen in the conventional blockchains. The IOTA Tangle also provides the same functionality where every transaction involves a small PoW. The Influence of IOTA is much higher, compared to the standard blockchain platforms. While, most of the block-chain network requires the users to pay transaction fees for setting up transaction priorities that are to be solved by miners, IOTA is a feeless space. IOTA does this because to perform a transaction, you have to approve two previous transactions, thereby increasing the engagement of users in protecting the network without charging. Moreover, unlike the blockchains fixed to traditional single chain processing of transactions, IOTA works with the structure called Tangle which enables parallel processing of the transaction. This design greatly enhances the system’s generated throughput and scalability which makes IOTA capable of accommodating a larger number of users and transactions in its network.

3.2 device identity

Regarding the nature of devices, their identities are handled with the help of IOTA Identity which is known as a decentralized identity system of the IOTA Foundation. Its objective is to guarantee a trustful, verifiable, and indubitable method to assert identity during transactions between entities (persons, devices, or companies), in particular for the digital world. To this end, IOTA Identity also uses the Tangle’s distributed ledger technology to generate the two kinds of addresses and handle anything to do with identity without relying on centralized authorities. This approach ensures privacy, security, and control over the digital identities in the IoT [18].

3.3 Stronghold Vault

The Stronghold vault represents an advanced cryptographic storage solution developed by the IOTA Foundation. It is specifically designed to securely store sensitive information, such as private keys, using robust encryption methods and stringent security protocols. This technology plays a crucial role in enhancing the security and reliability of digital transactions and interactions within the IOTA network, ensuring the protection of critical information against unauthorized access and potential vulnerabilities [19] [20].

4. PROPOSED FRAMEWORK

This section gives an overview of the proposed framework's structure and elaborates on specific details. It is presumed that the edge device in the monitoring system possesses computational resources, specifically; the computing tasks that IoT device can undertake include transmitting messages using encrypted protocols like MQTT and communicating with the fog node (master). Additionally, operations such as digital signature, authentication, and the responsibility for storing edge information and deploying it to the IOTA Tangle are handled by the fog node.

4.1. System architecture

The architecture of the distributed IoT monitoring system comprises four layers as follows:

1- The edge layer, which includes devices and sensors. 2- The fog layer, represented by the Master node. 3- The IOTA Tangle layer. 4- The data visualization layer, which employs the ThingSpeak platform. The architecture is illustrated in Figure 1.

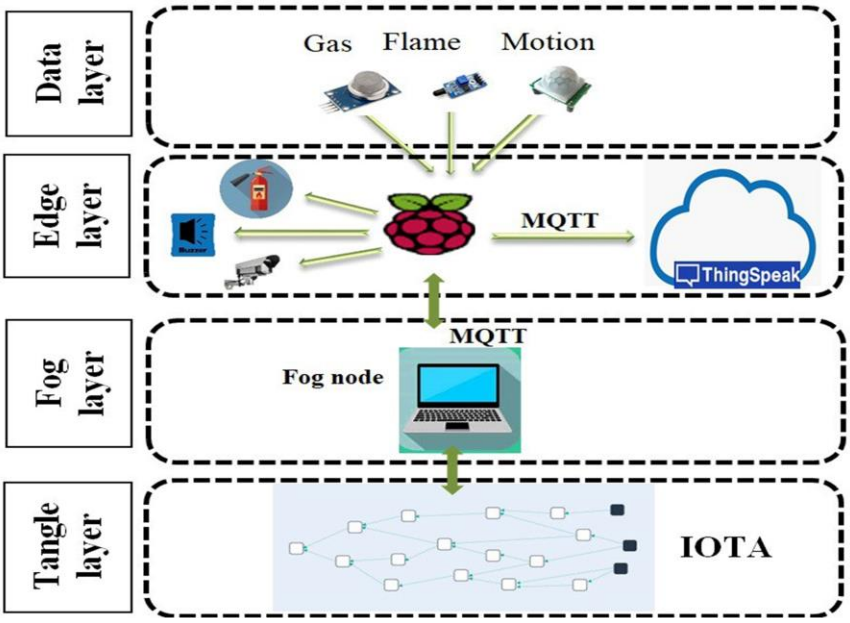


Figure 1: Framework structure (The proposed model's architecture consists of four layers: Edge Layer, Fog layer, The IOTA Tangle layer and data visualization layer)

4.1.1 The edge layer:

The edge layer comprises heterogeneous IoT devices characterized by constrained computing and storage capacities (specifically, Raspberry Pi devices were utilized in this study). These devices are tasked with real-time data sensing and collection within smart home environments, monitoring variables such as flame levels, gas concentrations, and motion detection. Based on these inputs, they enact corresponding security protocols to ensure safe household operations. Due to the limited storage capabilities inherent to IoT devices, conventional approaches necessitate hosting classified data in third-party repositories. However, centralized storage methods are susceptible to vulnerabilities, including potential risks of hacking and malicious activities. Consequently, this framework emphasizes the adoption of decentralized storage mechanisms to mitigate such risks. Notably, only IoT devices possessing authenticated identities are permitted to engage in network activities within this setup.

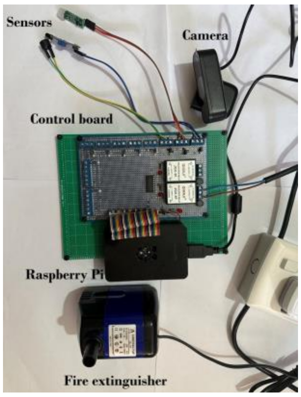


Figure 2: Edge Layer with its related sensors

4.1.2 The fog layer:

The fog layer constitutes a network centered around a master fog node serving as an access point for IoT devices, specifically Raspberry Pi devices, to connect to the network, fog node has the capability to manage a cluster of edge devices in its proximity, thereby assuming a significant portion of the computational workload typically handled by these devices. This arrangement effectively alleviates the operational burden on these lightweight devices and systems, and Mitigates latency issues associated with network data transmission. Additionally, fog node is deployed to manage device information including (mac address, sensors names and it associate pin numbers), assign identities to each edge device and its associated sensors employing IOTA identity library, and integrate them into the IOTA Tangle.

4.1.3 The IOTA Tangle layer:

To eliminate such scaling issues that come with the pack in classical blockchain structures, the proposed solution incorporates IOTA technology including its Tangle network structure. Due to its feature of supporting scalability and facilitating fee-less transactions, this technology fits well for IoT enviornments in terms of its ability to boost the stability and effectiveness of the network.

4.1.4 The data visualization layer:

The last layer is the data visualization layer, where the ThingSpeak platform is employed to enable remote monitoring of the residential properties [21]. The cloud platform allows edge devices to securely transmit sensor readings using the MQTT protocol, which guarantees secure and effective communication of sensor readings during monitoring house conditions remotely.

4.2 The proposed model’s overview:

The proposed model comprises three main components as follow: identity management, authentication processes and the activation of monitoring systems and its related sensors. The relation of these system components is indicated in the proposed model and the interaction among them is illustrated in Figure 3. First of all, the model employs the DAG-based distributed ledger technology called IOTA Tangle partnered with the IOTA Identity library. It becomes a single point of management for identity, which helps the consensus on the identity of the edge devices that are inactive. It can also guarantee the validity or the anti-forgery of each edge device's identity in the system and non-repudiation. Second of all, employing the Stronghold vault mechanism, fog node safely stores data belonging to edge devices and its related sensors. At last, as data created by IoT sensors can be rather sensitive, and, most of all, devices' identifications must be preserved, the edge devices use MQTT to transmit sensors' readings to ThingSpeak cloud-based platform for further prevention of misuse or any malicious activity.

4.3. Details of the proposed model:

This section describes the overview of the authentication process of the proposed model in details.

4.3.1 Identity management:

In the proposed model, the device identity management comprises primarily of two phases which including: device identity registration and device identity retrieval.

The proposed model leverages the IOTA Identity Framework so that the edge devices/sensors will possess unique global identities that will prove their credibility. The IoT system works with the understanding that edge devices and sensors will require authentication to gain access to the network, this creates the necessary framework which prevents skewed or fraudulent actions. Thus, the use of the IOTA protocol with the IOTA Identity framework allows the entire process of interaction between users and the monitoring system to be fully automated and secure. To ensure the monitoring system operates smoothly, the edge device and its sensors must first undergo authentication. The initial step involves registering edge device identities. Given the constrained computational capabilities of edge devices, the authentication process is delegated to a fog node (acting as the system's master). Upon receiving the MAC address (edge ID) of edge device and attributes of its sensors, employing IOTA identity framework, fog node generates identity attributes. These attributes are structured as an identity document (Decentralized Identifier DID), enabling security functionalities like identity authentication and verifiability. A DID functions as a reference to a DID Document, which includes essential data such as public keys. These keys allow the edge device to authenticate its identity and can be verified online. If the edge device and its associated sensors are not registered, the edge device sends a registration request to the fog node, which includes its ID (MAC address) along with sensor attributes. The fog node registers the new edge device if the administrator accepts the registration request; otherwise, a decline message is sent back to the edge device. Upon successful registration, the fog node generates a Verifiable Credential (VC). VC includes various attributes, among which are:

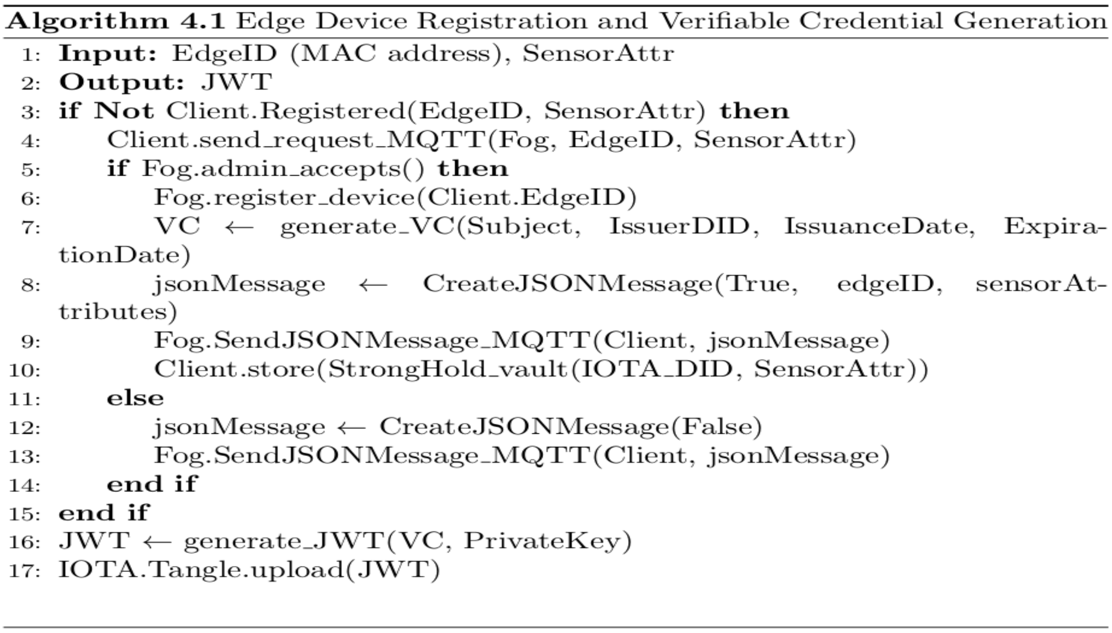
1. **Subject:** The set of claims made by the issuer, comprising objects that contain properties relevant to a particular entity including MAC address, sensors attributes (names and its ids).

2. **Issuer:** The identifier of the entity issuing the credential, commonly represented by their DID (Decentralized Identifier).

3. **Issuance Date:** A timestamp indicating the date and time when the credential becomes effective and valid.

4. **Expiration Date:** An optional timestamp indicating when the credential expires and is no longer considered valid.

Following the preparation of the verifiable credential, the issuer (fog node) generates a signed JSON Web Token (JWT) that encapsulates the VC within its claims, employing one of their private keys. This mechanism enables verifiers to autonomously verify the credential's authenticity by referencing the corresponding public key from the issuer's DID Document. Algorithm 4.1 illustrates edge device registration process in the proposed model utilizing IOTA identity framework. In IOTA Identity, the creation of public and private keys typically utilizes standard cryptographic algorithms to guarantee security and integrity of devices' identities and transactions. The specific algorithm used is the Elliptic Curve Digital Signature Algorithm (ECDSA) [22], commonly with the curve secp256k1. This curve is also applied to other blockchain technologies, such as Bitcoin, because of its characteristics in term of supporting security.



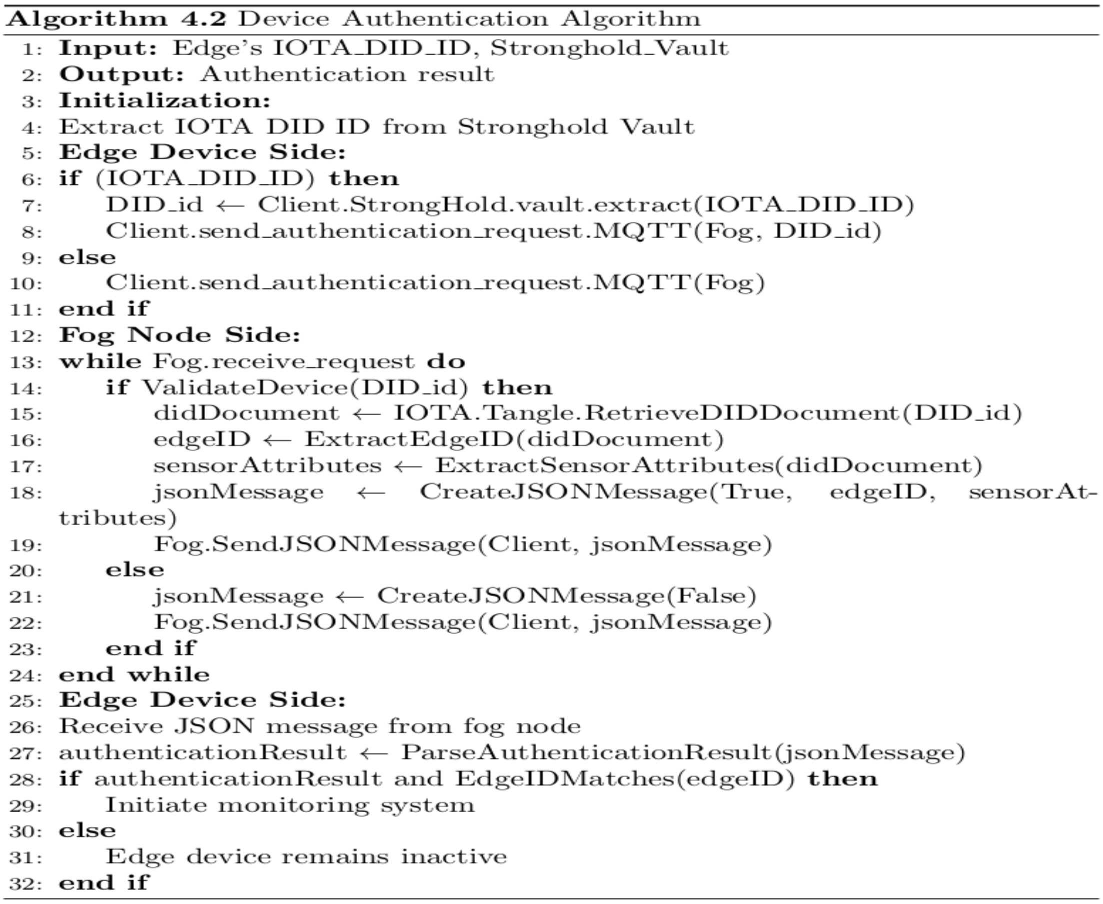
Algorithm 4.1 Edge Device Registration and Verifiable Credential Generation

```
Input: EdgeID (MAC address), SensorAttr
Output: JWT
if Not Client.Registered(EdgeID, SensorAttr) then
    Client.send_request_MQTT(Fog, EdgeID, SensorAttr)
    if Fog.admin_accepts() then
        Fog.register_device(Client.EdgeID)
        VC ← generate_VC(Subject, IssuerDID, IssuanceDate, ExpirationDate)
        jsonMessage ← CreateJSONMessage(True, edgeID, sensorAttributes)
        Fog.SendJSONMessage_MQTT(Client, jsonMessage)
        Client.store(StrongHold_vault(IOTA_DID, SensorAttr))
    else
        jsonMessage ← CreateJSONMessage(False)
        Fog.SendJSONMessage_MQTT(Client, jsonMessage)
    end if
end if
JWT ← generate_JWT(VC, PrivateKey)
IOTA.Tangle.upload(JWT)
```

During the device identity retrieval phase, edge device uses an ID known as an IOTA DID ID that is kept in a Stronghold Vault. The edge device uploads an authentication request using MQTT communication as a secure protocol to fog node. The fog node needs to confirm the registration status in the IOTA identity framework using the edge's IOTA DID ID and fetch the related information from the obtained DID document in the Tangle. Upon this validation of the DID document, the fog node extracts the edge device identifier which is edge's MAC address and the attributes of the device's sensors.

After that, the fog node prepares message-based JSON format to contain the result of the mutual authentication, the ID and other attributes of the edge device ID, and its communicating sensors IDs. This message is then transmitted back to the edge device via MQTT. Upon receiving the JSON message from the fog node, the edge device verifies the authentication result and compares its own ID (MAC address) with the received ID from the fog node. Similarly, the edge device verifies its sensors' attributes against those received from the fog node.

If the authentication process is successful, confirming the authenticity of both the edge device and its sensors, the edge device proceeds to initiate the monitoring system. Conversely, if authentication fails at any stage, the edge device remains in an inactive state and does not proceed with its operational tasks. Algorithm 4.2 demonstrates authentication steps of the proposed model including identity retrieval process.



Algorithm 4.2 Device Authentication Algorithm

```
Input: Edge's IOTA_DID_ID, Stronghold_Vault
Output: Authentication result
Initialization:
Extract IOTA DID ID from Stronghold Vault
Edge Device Side:
if (IOTA_DID_ID) then
    DID_id ← Client.StrongHold.vault.extract(IOTA_DID_ID)
    Client.send_authentication_request.MQTT(Fog, DID_id)
else
    Client.send_authentication_request.MQTT(Fog)
end if
Fog Node Side:
while Fog.receive_request do
    if ValidateDevice(DID_id) then
        didDocument ← IOTA.Tangle.RetrieveDIDDocument(DID_id)
        edgeID ← ExtractEdgeID(didDocument)
        sensorAttributes ← ExtractSensorAttributes(didDocument)
        jsonMessage ← CreateJSONMessage(True, edgeID, sensorAttributes)
        Fog.SendJSONMessage(Client, jsonMessage)
    else
        jsonMessage ← CreateJSONMessage(False)
        Fog.SendJSONMessage(Client, jsonMessage)
    end if
end while
Edge Device Side:
Receive JSON message from fog node
authenticationResult ← ParseAuthenticationResult(jsonMessage)
if authenticationResult and EdgeIDMatches(edgeID) then
    Initiate monitoring system
else
    Edge device remains inactive
end if
```

4.3.2 Authentication processes:

After the edge device and its associated sensors' attributes are authenticated and their verification credentials are uploaded to the IOTA Tangle, fog node securely transmits an authentication approval message back to the edge device using the MQTT protocol. Alongside this message, the fog node also communicates the corresponding generated IOTA DID ID. The received IOTA DID ID is subsequently stored in an IOTA Stronghold Vault as illustrated in Algorithm 2.

4.3.3 Activation of monitoring systems:

Following successful authentication and approval, edge device initiates secure streaming of sensor readings via MQTT protocol to the ThingSpeak cloud. Based on these readings, the edge device performs corresponding actions such as activating fire suppression systems in case of fire, initiating image transmission from cameras upon detecting motion, and other specified responses. Figure 3 illustrates the whole interaction process.

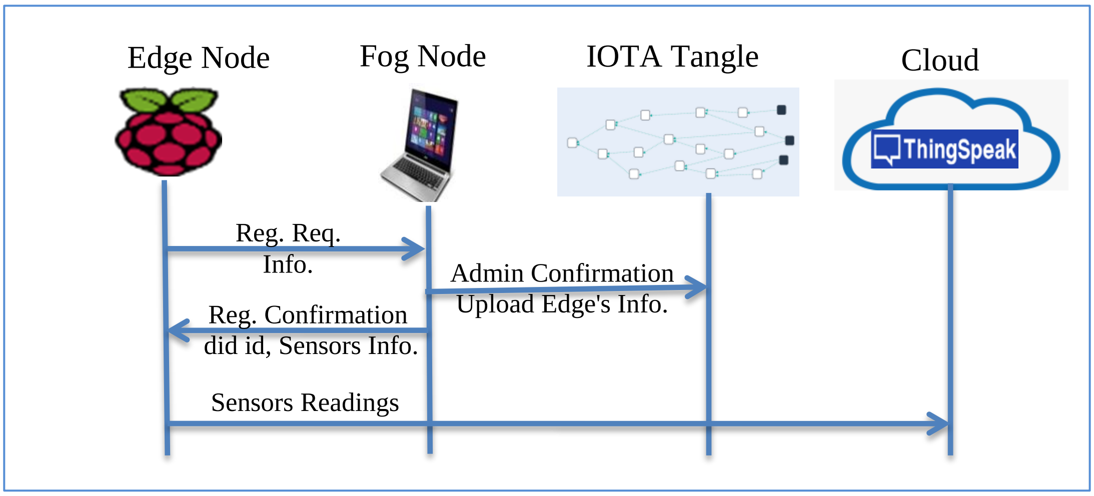


Figure 3: Flow chart authentication process

5. Evaluation and Results:

This section involves a detailed analysis of the proposed protocol performance,

5.1 Experiment Framework

The experimental framework consists of an edge device, a Raspberry Pi 4, which is interfaced with three sensors, a gas sensor, a motion sensor, and a flame sensor. Furthermore, a camera is also interfaced to the Raspberry Pi which records photo/video when motion is detected, storing these images/videos for further analysis or record-keeping. The setup also comprises a water pump that starts pumping water to put off the fire once the flame sensor identifies fire and a buzzer that is used to produce a beep sound in response to detecting fire, motion or gas.

Thus, edge device with sensors and actuators is communicating with a fog node (PC) which is connected to the local IOTA network through the IOTA sandbox environment (can be connected to the one of the IOTA endpoints). Secure communication channel is created between the edge device and the fog node using MQTT protocol to establish secure and reliable data transfer communication.

The Raspberry Pi (edge node) is set to constantly reading sensors' data. Upon detection of any specific events such as gas leaks, motion, or fire, it performs the following actions:

- **Motion Detection:** Its action is oriented towards snapping pictures and storing them locally or at the fog node for further analysis.
- **Fire Detection:** The water pump is activated to douse the fire, and the buzzer alerts nearby individuals to the fire hazard.
- **Gas Detection:** The buzzer is activated to alert individuals to the presence of gas, potentially averting dangerous situations.

The edge device also connects to the ThingSpeak cloud-based platform via MQTT. Data collected from various sensors are sent to this platform only if the edge device and its corresponding sensors are authenticated with the help of the suggested authentication framework. This model also make sure that only allowed and authorized devices are allowed to send data improving security and integrity of the system.

A fog node is used for the initial data accumulation and hence, for basic data processing and connections with the IOTA network. Fog node role is important as it makes data integrity and security measures are preserved when passing through the communication channel. The IOTA sandbox setup allows handling large amount of data in a highly secure and scalable way thanks to the specific nature of the distributed ledger technology which does not allow both data to be altered and unauthorized access by malicious actors.

5.2 System Security Analysis

This section examines how the proposed model mitigates certain attack scenarios to reach high security level and fulfill lightweight features in the IoT environment as follows:

5.2.1 Malicious Fog Node

In the IOTA network, before a fog node can begin a new transaction, they are supposed to validate two other transactions. Thus, for instance, if a fog node among the participating nodes in the network approves illegitimate transactions, other fog nodes will proceed to decline any transaction initiated by the fog node, resulting in the transaction not being confirmed in the network. The concept of designing IOTA means that only the fog nodes shall be capable of validating the right transactions in the network and this makes it secure. Additionally, if a certain fog node has a bad intention of initiating illegitimate transaction into the IOTA network, the other two nodes of the IOTA network do not verify the transaction initiated by the malice fog node thus makes such attacks almost impossible to succeed.

5.2.2 Spam attack

Proof of Work (PoW) is a measure that IOTA suggested to prevent a node from filling the Tangle with a huge number of transactions. Responding to attacks of spam, PoW is used by IOTA which demands the expenditure of resources by any node intend to send a transaction or a message. This requirement introduces a high cost on a potential attacker hence the low possibility of spam and the integrity of the network. By requiring PoW, IOTA ensures that generating a large number of transactions (as would be the case in a spam attack) consumes significant computational resources. This resource cost acts as a deterrent against spamming the network because the attacker must expend considerable processing power, making such attacks economically and practically unfeasible on a large scale. To enhance the lightweight nature of the proposed model, all processes related to the IOTA Tangle, including Proof of Work (PoW) calculations, are offloaded to fog node. This strategic delegation minimizes the computational load on individual edge devices, thereby ensuring efficient and resource-conserving operations within the system.

5.2.3 Mitigation of Mathematical Modeling attack

A strong lightweight authentication protocol like a Physical Unclonable Function (PUF) for a robust lightweight authentication could likely be at risk of modeling attacks which are based on machine learning. These mathematical models are developed with a high accuracy by using the Machine Learning methods such as Support Vector Machines (SVM), and logistic regression (LR) algorithms [23]. Among the Challenge-Response Pairs (CRPs) of a certain lightweight protocol behavior, a subset of CRPs is required to train the machine learning system so that ML system can learn depending on challenge-response behavior properly intending to model the authentication protocol correctly. Nevertheless, by means of this mathematical model, an predict any random node behavior with a comparatively high level of probability.

According to most of the proposed lightweight authentication protocols, an adversary can obtain the CRPs in two cases. First, by getting possession of IoT device (edge). In response to the threats, the proposed framework, particularly algorithm 4.2 in section 4 shall be authenticated by the fog node before it considered as edge node with its sensors. Moreover, even if the attacker gains the physical device, the essence of the IOTA DID remains safe, it will be safeguarded at the Stronghold vault. Second, the adversary can tap into the channel traffic and get at transmitted data. To avoid this, the proposed protocol incorporates the MQTT protocol for the encryptions of the transmitted messages.

6. RESULTS

6.1 Automated Security Testing Using the Scyther Tool

It has been ensured that all security assumptions of the proposed protocol have been implemented using Scyther [9], a tool for automatic analysis of security protocols. The decryption process analysis carried out by Scyther uses its operational semantics based on the Security Protocol Description Language (SPDL). Scyther establishing the claimed security aspects of the protocol across any number of sessions and particularly that the session will terminate. It simultaneously checks the messages that are transmitted to other party. This attempt of protocol analysis also yields verification, falsification, and security analysis to ensure that the given protocol is correct. Using of the SPDL scripts containing the secret authentication responses, encryption of the messages and messages flow, are employed to implement the proposed protocols.

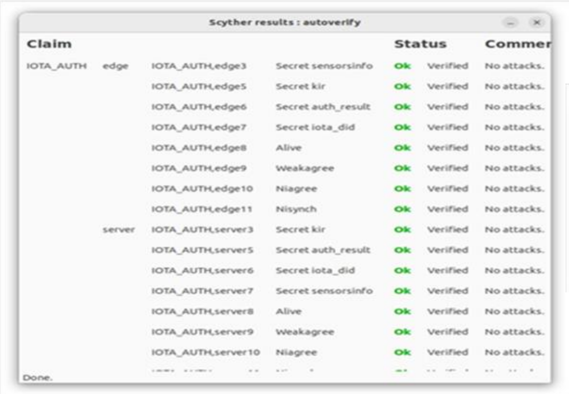
6.2 Simulation Setup

The Scyther software v1. 1. 3 was carried out on an OS Platform of 64-bit Ubuntu Linux Operating System Version 22. 04. 2 (LTS) along with Graphviz v2. 38 and Python v2. 7. The specifics of the simulation are described in the Table 1 below.

The proposed model was implemented and validated through the Scyther tool. As it has been observed in Figure 4(a), the protocol goes on to forge the synchronous claims without any evidence of attacks. Moreover, the proposed protocol fulfills the automatic claims of Niagree, Nisynch, Alive, and Weakagree as per the Scyther tool. These properties relate to non-injective agreement, non-injective synchronization, aliveness and weak agreement repectively. In addition, Figure 4(b) also depicts the proof of correctness of the outlined protocol which in this case, focuses on the evaluation of the propriety of the security protocols to conform with the designed purposes of security parameters and ensure that network is vulnerabilities free.

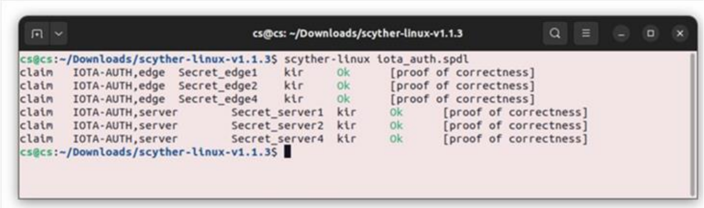
Table 1: SCYTHER TOOL PARAMETERS USED FOR ANALYSIS

Verification parameters	Advanced parameters
Default parameter specification	
Max. runs: 5 Matching type: typed matching	Search pruning: Find best attack Max. patterns/claim: 10
Customized parameter specification	
Max. runs: 10 Matching type: Find all type flaws	Search pruning: Find all attack Max. patterns/claim: 10



```
Claim                                                      Status        Commer
IOTA_AUTH  edge    IOTA_AUTH,edge3     Secret sensorsinfo   Ok   Verified  No attacks.
                   IOTA_AUTH,edge5     Secret kir           Ok   Verified  No attacks.
                   IOTA_AUTH,edge6     Secret auth_result   Ok   Verified  No attacks.
                   IOTA_AUTH,edge7     Secret iota_did      Ok   Verified  No attacks.
                   IOTA_AUTH,edge8     Alive                Ok   Verified  No attacks.
                   IOTA_AUTH,edge9     Weakagree            Ok   Verified  No attacks.
                   IOTA_AUTH,edge10    Niagree              Ok   Verified  No attacks.
                   IOTA_AUTH,edge11    Nisynch              Ok   Verified  No attacks.
           server  IOTA_AUTH,server3   Secret kir           Ok   Verified  No attacks.
                   IOTA_AUTH,server5   Secret auth_result   Ok   Verified  No attacks.
                   IOTA_AUTH,server6   Secret iota_did      Ok   Verified  No attacks.
                   IOTA_AUTH,server7   Secret sensorsinfo   Ok   Verified  No attacks.
                   IOTA_AUTH,server8   Alive                Ok   Verified  No attacks.
                   IOTA_AUTH,server9   Weakagree            Ok   Verified  No attacks.
                   IOTA_AUTH,server10  Niagree              Ok   Verified  No attacks.
```

Figure 4 (a): Scyther automatic proposed model analysis report



```
cs@cs:~/Downloads/scyther-linux-v1.1.3$ scyther-linux iota_auth.spdl
claim   IOTA-AUTH,edge  Secret_edge1    kir     Ok      [proof of correctness]
claim   IOTA-AUTH,edge  Secret_edge2    kir     Ok      [proof of correctness]
claim   IOTA-AUTH,edge  Secret_edge4    kir     Ok      [proof of correctness]
claim   IOTA-AUTH,server        Secret_server1  kir     Ok      [proof of correctness]
claim   IOTA-AUTH,server        Secret_server2  kir     Ok      [proof of correctness]
claim   IOTA-AUTH,server        Secret_server4  kir     Ok      [proof of correctness]
cs@cs:~/Downloads/scyther-linux-v1.1.3$ 
```

Figure 4 (b): Scyther proof of correctness report

Table 2. shows a comprehensive security feature comparison between the proposed work and existing literature. This comparison is crucial for highlighting the advancements and improvements made by the proposed protocol over previous methods.

Table 2: SECURITY FEATURE COMPARISON

Feature	Ref[24]	Ref[25]	Ref[26]	Ref[27]	Ref[28]	The proposed protocol
Attack analysis						
Protection against obtaining Secret Key	✓	✓	X	✓	✓	✓
Protection against DoS attack	X	✓	✓	X	✓	✓
Protection against Modeling attack	✓	X	X	✓	X	✓
Protection against Spam attack	✓	✓	✓	X	X	✓
Protection against Malicious attack	✓	X	✓	X	X	✓
Data safeguarding	X	X	X	X	✓	✓

where "✓" indicates that the function is supported, and "x" indicates that the function is not supported

6.3 Communication and Storage overhead

The network overhead associated with transmitting a payload, such as an authentication request and response, using the MQTT protocol involves several critical factors. Firstly, the MQTT protocol incurs a fixed header overhead of 1 to 2 bytes, which varies based on the specific message type. Furthermore, a PUBLISH message generally has a minimum overhead of approximately 2 to 4 bytes. Additionally, the size of the payload, which corresponds to the authentication request, must be taken into account. The implementation of Quality of Service (QoS) levels in MQTT introduces further overhead due to the necessity for message acknowledgments. Consequently, the total estimated overhead for transmitting such a message is approximately 2048 bits. Figure 6(a) illustrates the communication overhead of the proposed protocol against relevant existing frameworks.

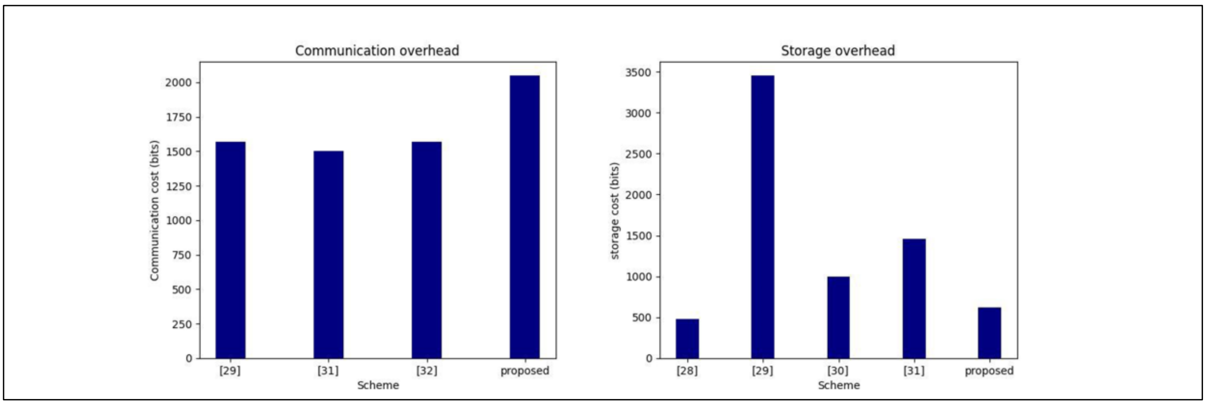


Figure 6 (a): Communication overhead **Figure 6 (b):** Storage overhead

In this context, the communication cost refers to the total number of bits transmitted and received during the authentication procedure. The length of each message is determined by two scenarios: first, when the edge device sends an authentication request, and second, when the fog device responds with an authentication reply to the edge device. This determines the size of the parameters used in these messages. The communication costs of the proposed model are compared with those of existing schemes. As shown in Figure 6(a), the number of transmitted bits in the proposed model is slightly higher than in [29], [31], and [32], but it achieves an optimal balance for secure communication between edge and fog devices. In addition, most of the existing schemes are primarily tested and validated through simulations.

The overall cost of storing the edge DID ID in the proposed model is determined based on the size of the DID ID. Each edge device stores its DID ID in memory. As illustrated in Figure 6(b), the total storage cost demonstrates the superiority of the proposed model over most of the existing schemes.

7. CONCLUSION

In this paper a new lightweight authentication model for IoT-based smart house monitoring system utilizing IOTA Tangle is proposed, the IOTA identity and Stronghold vault technologies have been employed. The proposed framework is implemented with Python language, Wasm script and Node.js (JavaScript/TypeScript). Sensors reading streamed to the ThingSpeak cloud platform securely via MQTT protocol. Both edge and fog devices are securely connected to a broker using the MQTT protocol as well, which helps secure transmission of data and reduces the spread of attacks over the network. Additionally, if the system detects any unauthorized device including an edge device or sensor, the entire edge device is unauthenticated and remains inactive. After a successful authentication process, the proposed system responds appropriately based in sensors readings.

Concerning the verification of the proposed scheme, it has been verified and assessed using the Scyther tool. It has been also validated against different real-world cyber-attacks and compared with other relevant studies available in the literature. The testing proved the effectiveness of the proposed scheme since it proved data integrity and security. Also, other assessment metrics including communication and storage cost was also analyzed and proved that the scheme works effectively in constraints IoT environment. The comparison with other solutions showed that the proposed scheme was more robust and profound in terms of security, which made it possible choice to improve the security of IoT systems.

REFERENCES

[1] H. D. Zubaydi, P. Varga, and S. Molnár, “Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review,” Sensors, vol. 23, no. 2, 2023, doi: 10.3390/s23020788.

[2] S. Abbas Fadhel and A. Sami Nori, “Lightweight Authentication for Devices in Internet of Thing Environment: A Survey,” AL-Rafidain J. Comput. Sci. Math., vol. 17, no. 2, pp. 55–62, 2023, doi: 10.33899/csmj.2023.181632.

[3] S. Wang, H. Li, J. Chen, J. Wang, and Y. Deng, “DAG blockchain-based lightweight authentication and authorization scheme for IoT devices,” J. Inf. Secur. Appl., vol. 66, no. March, 2022, doi: 10.1016/j.jisa.2022.103134.

[4] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, “A Survey on Decentralized Identifiers and Verifiable Credentials,” vol. 14, no. 8, pp. 1–30, 2024, [Online]. Available: http://arxiv.org/abs/2402.02455

[5] S. K. Roy, “Decentralized Identity and Access Management (IAM) and Self-Sovereign Identity,” Int. J. Res. Eng. …, vol. 6, no. 12, pp. 201–210, 2023, [Online]. Available: https://journal.ijresm.com/index.php/ijresm/article/view/2898

[6] M. Alizadeh, K. Andersson, and O. Schelen, “Comparative Analysis of Decentralized Identity Approaches,” IEEE Access, vol. 10, no. July, 2022, doi: 10.1109/ACCESS.2022.3202553.

[7] K. Vemula, “an End-To-End Decentralized Internet of Things (Iot) Data Model,” Dalspace.Library.Dal.Ca, vol. 15, no. 5, 2023, [Online]. Available: http://hdl.handle.net/10222/82869

[8] H. Li, Y. Jing, and Z. Guan, “The Review and Comparison between Centralized and Decentralized Digital Identity Systems,” Mob. Inf. Syst., vol. 2024, pp. 1–10, 2024, doi: 10.1155/2024/6651273.

[9] C. J. F. Cremers, “The scyther tool: Verification, falsification, and analysis of security protocols: Tool paper,” in International conference on computer aided verification, Springer, 2008, pp. 414–418.

[10] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, and Z. Cui, “Distributed, secure, self-sovereign identity for iot devices,” in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT),

IEEE, 2020, pp. 1–6.

[11] M. Luecking, C. Fries, R. Lamberti, and W. Stork, “Decentralized identity and trust management framework for Internet of Things,” in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2020, pp. 1–9.

[12] I.-C. Lin, C.-C. Chang, and Y.-S. Chang, “Data Security and Preservation Mechanisms for Industrial Control Network Using IOTA,” Symmetry (Basel)., vol. 14, no. 2, p. 237, 2022.

[13] B. Wang and X. Hu, “Lightweight blockchain system for resource-constrained IoT devices,” in 2nd International Conference on Internet of Things and Smart City (IoTSC 2022), SPIE, 2022, p. 1224902.

[14] I.-C. Lin, P.-C. Tseng, Y.-S. Chang, and T.-C. Weng, “IOTA Data Preservation Implementation for Industrial Automation and Control Systems,” Processes, vol. 11, no. 7, p. 2160, 2023.

[15] A. Solavagione, “Self-Sovereign Identity aware TLS handshake with MbedTLS.” Politecnico di Torino, 2023.

[16] A. Feraudo, N. Romandini, C. Mazzocca, R. Montanari, and P. Bellavista, “DIVA: A DID-based reputation system for secure transmission in VANETs using IOTA,” Comput. Networks, vol. 244, no. March, p. 110332, 2024, doi: 10.1016/j.comnet.2024.110332.

[17] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[18] M. Luecking, C. Fries, R. Lamberti, and W. Stork, “Decentralized Identity and Trust Management Framework for Internet of Things,” IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2020, 2020, doi: 10.1109/ICBC48266.2020.9169411.

[19] N. Gligori, L. Polo, A. Amditis, T. Georgakopoulos, A. Fraile, and G. Scholar, “IOTA - Based Distributed Ledger in the Mining Industry : Efficiency , Sustainability and Transparency,” 2024, doi: 10.20944/preprints202401.0650.v1.

[20] F. Rosenkranz, “Invention of a working prototype to demonstrate the IOTA Streams and Wallet protocols for a meter with additional focus on economic efficiency and the technical preparation of scalability.” Westsächsische Hochschule Zwickau, 2023.

[21]https://thingspeak.com

[22] L. Perugini and A. Vesco, “On the integration of Self-Sovereign Identity with TLS 1.3 handshake to build trust in IoT systems,” Internet of Things (Netherlands), vol. 25, no. February, pp. 1–13, 2024, doi: 10.1016/j.iot.2024.101103.

[23] U. Ruhrmair et al., “PUF modeling attacks on simulated and silicon data,” IEEE Trans. Inf. Forensics Secur., vol. 8, no. 11, pp. 1876–1891, 2013, doi: 10.1109/TIFS.2013.2279798.

[24] U. Chatterjee et al., “Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database,” IEEE Trans. Dependable Secur. Comput., vol. 16, no. 3, pp. 424–437, 2019, doi: 10.1109/TDSC.2018.2832201.

[25] M. A. Qureshi and A. Munir, “PUF-RAKE: A PUF-Based Robust and Lightweight Authentication and Key Establishment Protocol,” IEEE Trans. Dependable Secur. Comput., vol. 19, no. 4, pp. 2457–2475, 2022, doi: 10.1109/TDSC.2021.3059454.

[26] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things,” IEEE Trans. Consum. Electron., vol. 65, no. 3, pp. 388–397, 2019, doi: 10.1109/TCE.2019.2926192.

[27] G. V. Pinto, J. P. Dias, and H. Sereno Ferreira, “Blockchain-Based PKI for Crowdsourced IoT Sensor Information,” Adv. Intell. Syst. Comput., vol. 942, pp. 248–257, 2020, doi: 10.1007/978-3-030-17065-3_25.

[28] S. Roy, D. Das, A. Mondal, M. H. Mahalat, B. Sen, and B. Sikdar, “PLAKE: PUF-Based Secure Lightweight Authentication and Key Exchange Protocol for IoT,” IEEE Internet Things J., vol. 10, no. 10, pp. 8547–8559, 2023, doi: 10.1109/JIOT.2022.3202265.

[29] P. Gope and B. Sikdar, “Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices,” IEEE Internet Things J., vol. 6, no. 1, pp. 580–589, 2019, doi: 10.1109/JIOT.2018.2846299.

[30] H. S. Jennath, V. S. Anoop, and S. Asharaf, “Blockchain for healthcare: Securing patient data and enabling trusted artificial intelligence,” Int. J. Interact. Multimed. Artif. Intell., vol. 6, no. 3, pp. 15–23, 2020, doi: 10.9781/ijimai.2020.07.002.

[31]S. Das, S. Namasudra, S. Deb, P. M. Ger, and R. G. Crespo, “Securing IoT-Based Smart Healthcare Systems by Using Advanced Lightweight Privacy-Preserving Authentication Scheme,” IEEE Internet Things J., vol. 10, no. 21, pp. 18486–18494, 2023, doi: 10.1109/JIOT.2023.3283347.

[32] H. Wang, J. Meng, X. Du, T. Cao, and Y. Xie, “Lightweight and Anonymous Mutual Authentication Protocol for Edge IoT Nodes with Physical Unclonable Function,” Secur. Commun. Networks, vol. 2022, no. 1, 2022, doi: 10.1155/2022/1203691.