Securing IoT Smart Irrigation Systems with Adapted Blockchain Based Approach

Rabaie Benameur [1,2], Bouabdellah Kechar [1,2], Zahia Bidai [1,2] and Amine Dahane [1,2,3,*]
[1]*Laboratory of Industrial Computing and Networks (RIIR), Oran, Algeria*
[2]*University of Oran 1, Oran, Algeria*
[3]*Institute of Applied Science and Technology ISTA, Oran, Algeria*
Correspondence: dahane.amine@univ-oran1.dz

***Abstract*—Blockchain (BC) technology promotes the scalability and stability of Internet of Things (IoT) applications and avoids the need for a single trusted authority. However, an IoT Smart Irrigation System (ISIS) comprises constrained devices such as microcontrollers and IoT gateways. A lightweight consensus mechanism is required to reduce computational costs in such systems. This paper presents a novel secure architecture for ISIS based on an adapted BC approach by implementing a lightweight Proof of Authority (PoA) consensus mechanism called Aura (Authority Round). The proposed mechanism is designed to overcome reported security limitations in commonly private BC. We apply our solution to the existing ISIS prototype developed in our laboratory. Experimental results show the feasibility and efficiency of BC technology in ISIS.**

***Index Terms*—Smart Irrigation System, IoT, Blockchain, PoA consensus, Security, Prototyping.**

I. Introduction

Internet of Things (IoT) has become a domain of immense influence that offers novel services to various applications [1]. An IoT Smart Irrigation System (ISIS) is a prominent IoT application that controls water use precisely according to cultures' water demands . It depends on numerous climatic and soil parameters such as air temperature, humidity, and soil moisture where plants grow [2]. However, the current architucture of ISIS as illustrated in Fig. 1 is highly susceptible to cyberattacks at Cloud, Fog and Edge layers. Therefore, integrity, tractability, and authentication mechanisms are required to detect security issues and deny unauthorized interactions with the system. Using the BC security framework in the IoT makes a lot of sense since it offers immutability, trust, and anonymity. However, the challenging problem which will be taken is how to adapt the BC technology to low-cost equipment included in smart irrigation system, such as microcontrollers and cheap computers. The main objective of our work is to improve our previous work [3, 4] by including the security aspect in ISIS. To achieve this goal, we implemented a lightweight Proof of Authority (PoA) consensus similar to Aura (Authority Round) [6]. This mechanism is designed to overcome the security limitations reported in private BCs by taking into account the reputation of validator nodes. Finally, we apply our solution to the existing ISIS prototype. The rest of the paper is organized as follows: Section II briefly surveys the related work. Section III presents the security of ISIS based on BC technology. Section IV describes the ISIS prototype's implementation aspects and hardware components. Section V presents the performance evaluation of our solution and discusses the experimental results. Section VI concludes the paper and outlines the directions for future work.

II. Related work

In this section, we present recent research on security in ISIS. We focus on papers that use BC technology and cryptography techniques. Authors in [5] developed a safe, cloud-connected smart multi-crop irrigation systems that can reduce water consumption and solves the problem of rainfall-induced over-irrigation. The irrigation decisions are made in real-time based on soil moisture predictions during precipitation. Access Control and BC technologies ensure data security. Experimental results indicate the efficacy of the solution in overcoming excessive irrigation. A part of the study in the research paper [8] proposed a smart centralized water piping system with several valves installed in the agricultural areas to supply water automatically. A smart seed roller has been created to plant the seeds automatically into the ground. A tiny siren is included in the planned system to protect the crop from animals, birds, and thieves. Anand et al. [6] proposes adaptive water scheduling based on a wireless sensor network (WSN) in precision agriculture. BC technology is used to secure data transfer in the cloud. Sachan et al. [8] design a security architecture based on ECC, the SHA-256 algorithm, and the Artificial Bee Colony (ABC) algorithm to improve the security of IoT-based ISIS. The proposed approach utilizes the ABC technique to generate the ECC private key. According to the results, the best encoding and decoding times were 100 and 150 iterations, respectively. Furthermore, compared to DES, ECC, and SHA-256 and RC4 ECC SHA-256, the suggested models total throughput was about 50.04 % and 55.29 % higher in encryption, and 51.36 % , 58.41 % higher in decryption. Table. II shows the most common IoT cyber

979-8-3503-9672-0/23/$31.00 ©2023 IEEE

attacks against ISIS. Data tampering attacks the integrity of stored data in databases. The most utilized database in ISIS is MySQL [10], which suffers from SQL injection vulnerability. Flooding and Distributed Denial of Service (DDOS) attacks can easily make services unreachable due to the limited computational capacity of IoT devices. Sinkholes and Sybil attacks target public BC. However, it's hard to apply these attacks in private BC (all network nodes are pre-authenticated). Table. I shows a comparison between our approach and the existing works according to security features and results. The security of ISIS edge devices is not considered in security studies that use BC technology, and no implementation or results are published [7,8]. Our approach provides data availability and traceability compared to traditional cryptography mechanisms [5]. We also developed a low-cost secured prototype of ISIS based on BC technology.
In summary, the existing security mechanisms utilized in ISIS are based on cryptography algorithms applied to edge devices. However, security threats can occur in all IoT layers of ISIS.

III. Security of ISIS based on BC technology

Smart devices generate a huge amount of data with high velocity, allowing the farmer to control continuously and remotely sensors (air temperature, soil moisture, etc.) and actuators such as water pumps. For these reasons, the Proof of Work (PoW) consensus is not suitable for IoT environments because it requires expensive hardware and much more time to validate transactions, decreasing the performance of ISIS. To counter these drawbacks, we proposed a secure ISIS architecture and a lightweight version of PoA, both described in this section.

A. The proposed secure ISIS architecture based on BC

As shown in Fig. 2, the suggested design is built on the edge, fog, and cloud levels. The edge layer includes smart devices linked to a gateway through a mesh wireless sensor network. The microcontroller takes data from sensors and transfers it to the gateway. The source node can also accept user orders via the communication module and modify the state of the actuators. These nodes are installed in many small farms under the same authority. Each area contains an IoT gateway (fog layer) that deals with bidirectional communications between edge devices in the same area. Gateways are connected to a P2P network over the internet, and each gateway has all features of a full node since it stores a copy of the main chain and validates blocks. The Cloud layer also includes full node containers to perform the availability of the BC. Authorized end-users can view stored data in the chain and remotely set actuators' states. Soil parameters forecasting models based on Deep Learning (DL) are deployed in IoT gateway to improve network latency and cloud resource usage. These models employ historical data stored in the BC to forecast lost sensing measurements using the LSTM/GRU networks [3, 4]. The BC storage technique preserves the inputs to DL models from information tampering attempts.

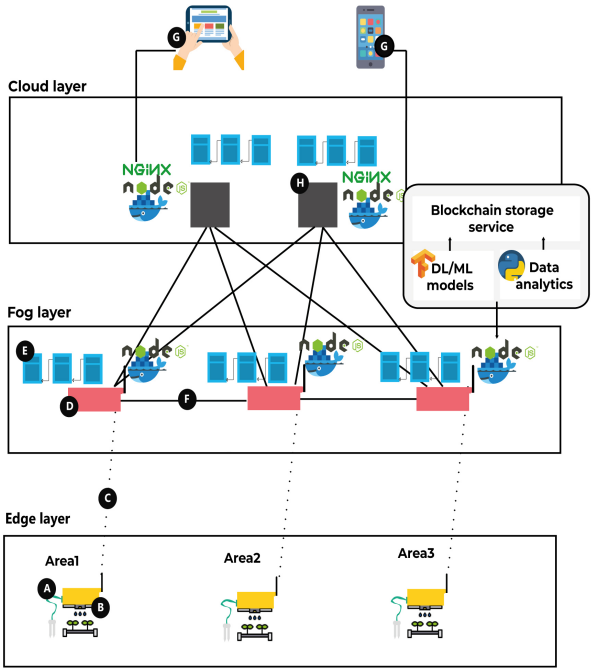

Fig. 1. The proposed architecture of secured ISIS: (A) Data acquisition node (Sensors), (B) Actuators (water pump),(C) Wireless link, (D) IoT gateway, (E) BC register, (F) BC secured communications channels, (G) End-user devices. (H) Cloud BC instance.

B. The proposed version of PoA consensus for ISIS

ISIS requires less latency, computing power, and no fees. Therefore, we will implement a version of the Proof of Authority (PoA) consensus to respect these constraints. PoA is another technique for achieving consensus among authorized BC nodes. PoA provides low latency and constant block generation interval and does not require high computing power as it is based on node identity and reputation. There are many versions of PoA consensus. In our case, we will implement Aura consensus [9]. Network nodes must be authorized as voting nodes. Then, the voting nodes will elect validator nodes based on identity and reputation. The selected validators must eventually show themselves to the network. These nodes are allowed to add new blocks to the BC. The leader is the only validator node that can generate new blocks at the current time. This strategy allows other nodes to recognize and kick malicious nodes attempting to add rogue blocks to the chain, as illustrated in Fig. 2. Before generating a new block, the leader must validate all pending transactions in the queue and respect block generation limits. The created block is signed with a private key and sent to all other validator nodes. The validator nodes receive blocks and verify if the current interval leader node generates them. The leader's public key is used to verify the received block. Each validator node checks block generation limits and the execution of transactions included in the block. The leader that generates invalid blocks or does not propose any blocks can be excluded from the list of validating nodes, as illustrated in Fig. 2. Validator three is banned from

TABLE I
COMPARISON BETWEEN OUR APPROACH AND THE EXISTING SOLUTIONS IN THE LITERATURE.

Articles	Authentication	confidentiality	Availability	Data integrity	Traceability	Prototype	Lowcost
[6]	✗	✗	✓	✓	✓	✓	✓
[8]	✗	✗	✓	✓	✓	✗	✗
[5]	✓	✓	✗	✓	✗	✗	✗
Our approach	✓	✓	✓	✓	✓	✓	✓

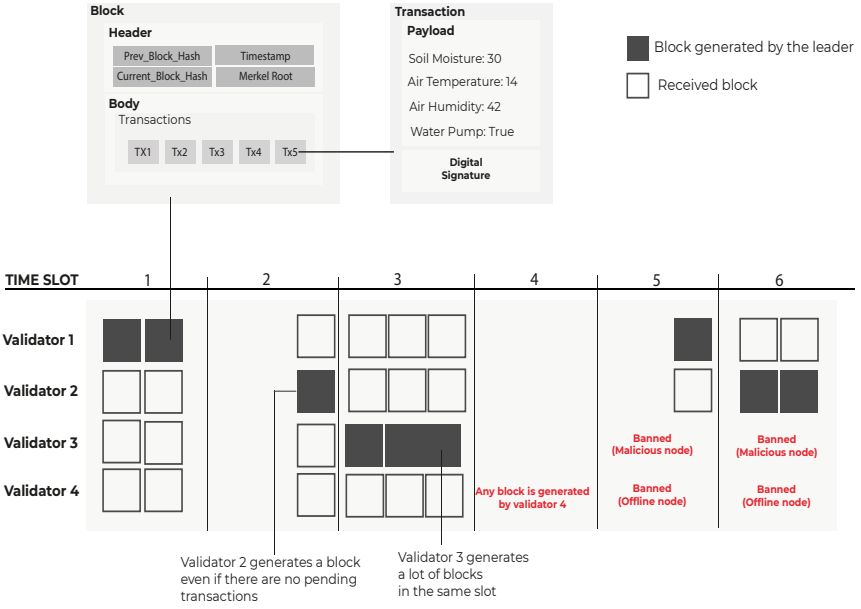

Fig. 2. Functioning principle of PoA consensus in Aura BC (example of a P2P network with 4 validators)

the BC network since it generates a lot of blocks in the same slot (flooding attack). Similarly, validator four does not validate any blocks (offline node).

IV. IMPLEMENTATION

In this section, we will discuss all the necessary steps to implement our proposed solution. We chose an open-source software stack and low-cost electronic prototyping platforms such as Arduino and Raspberry Pi. Fig. 3 shows the different components of the ISIS prototype described below.

A. Source node (Edge layer)

Data collection of current climatic and soil parameters is crucial in ISIS. We built a smart device, as illustrated in Fig. 1.A and Fig. 3.A based on an Arduino microcontroller (Arduino Uno + Arduino Mega), including temperature, humidity, optical density, and soil moisture sensors. A radio module named NRF24L1 module transmits data over WSN. Bidirectional radio communication is established to trigger the irrigation with a water pump (illustrated in Fig. 3.A.14). Before transmitting data to the next hop, the data must be structured and signed using the private key of the source node as shown in Algorithm 1.

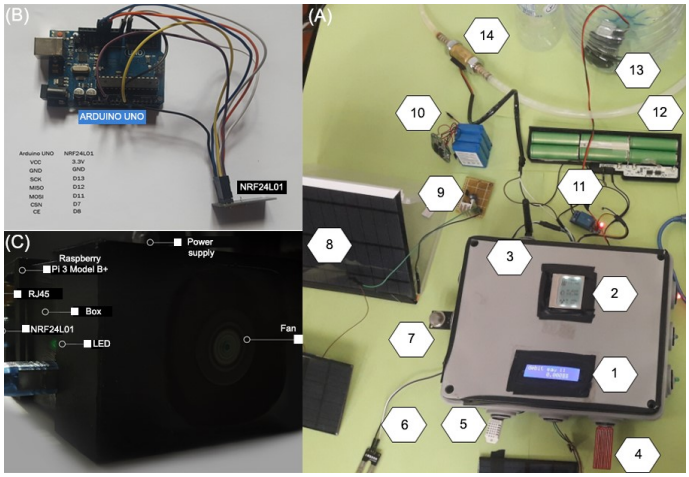

Fig. 3. The ISIS prototype components : (A) Source node components: (1) Box, (2) LCD Display,(3) NRF24L01 communication module (4) Water level sensor, (5) DHT22, (6) Soil moisture sensor, (7) MQ2 sensor, (8) Solar panel, (9) LDR sensor (10) Power supply 9v (11) Relay, (12) Power supply 12v (13) Water pump (14) Water flow sensor.(B) Relay node. (C) IoT gateway.

TABLE II
THE MOST COMMON IOT CYBERATTACKS AT THE FOG/CLOUD LAYERS AND SECURITY SOLUTIONS FOR ISIS.

Attack	Effects of the attack on ISIS	Security solutions
Information tampering [11] (Data destruction, manipulation). Security vulnerabilities, network attacks, and malware injection are the potential causes of this attack.	-Data Integrity (Sensors data tampering, bad irrigation decision). -Unauthorized Control of actuators causes agricultural field water flooding. -ISIS failure (bad irrigation decision).	-BC is immutable.
DDOS [12] is a malicious attempt to overload the normal traffic of a targeted IoT system by surrounding the infrastructure with a flood of internet traffic.	-ISIS performance degradation. -ISIS failure.	-Decentralization of IoT gateways. -Replication of data between BC nodes. -Unreachable node can be excluded from the list of validating nodes.
Flooding attack [13] occurs when an intruder sends many transactions to the target node until the resources of the target node are completely wasted.	-ISIS performance degradation. -ISIS failure.	-Denies validators that generate many blocks in the same slot. -Network nodes are pre-authenticated.
Sinkhole [13] occurs when a group of persons gains control of over 51% of a BC.	-Data Integrity. -Unauthorized Control of actuators. -ISIS failure.	-Obtaining control of the nodes in a permissioned blockchain network is very difficult because nodes are pre-authenticated.
Sybil attack [13] uses a single node to simultaneously operate many active fake identities.	-Data Integrity. -Unauthorized Control of actuators. -ISIS failure.	-Network nodes are pre-authenticated.

B. Relay node (Edge layer)

Relay node forward frames to the IoT gateway when multiple hops are needed to achieve the IoT gateway, as shown in Algorithm 2. It is based on an Arduino UNO board connected to the NRF24L1 module (illustrated in Fig. 3.B).

C. BC Fullnode (Fog/Cloud layer)

We implemented PoA consensus using Nodejs, a robust JavaScript-based open-source framework. We developed APIs for exchanging transactions and blocks between the complete nodes using the Express.js framework. Dockerization of Node.js scripts with the NGINX load balancer enables the BC network to quickly deploy new nodes and resolve heterogeneity issues. As shown in Algorithm 3, we sign transactions and exchange blocks with the elliptic curve digital signature algorithm (ECDSA), which offers short keys and requires less computational power. All BC procedures utilize the SHA256 algorithm as the hashing function because it is secure and collisions are uncommon [14] [15]. All communications between BC full node containers were secured with the SSL/TLS protocol. In the experiment, we will compare traffic between the current system (i.e., without BC mechanisms) and our proposed alternative, so HTTP is utilized between BC nodes. As depicted in Fig. 1.D and Fig. 1.H, we deploy docker containers in the google cloud console and Raspberry Pi 4.

Algorithm 1 Edge device embedded algorithm.
Input: Sensors record, interval, S_k: secret key, P_k: public key
Output: BC transaction.

```
while True do
    buffer=radio.receive()
    isValide=false
    if buffer!=null then
        data=buffer.data
        signature=buffer.signature
        hash=SHA256(data)
        isValide=(ECDSA.decrypt(hash,P_k)==signature)
    end if
    if isValide then
        setState(waterPump,data)
    end if
    data=Sensors.read()
    hash=SHA256(data)
    signature=ECDSA.encrypt(hash,S_k)
    transaction=concat(data,signature)
    send(transaction)
end while
```

Algorithm 2 Relay node embedded algorithm.
Input:
Transaction: transaction received from edge devices.
buffer:store received packets temporarily
interval: sleep interval.
Output: Transaction.

```
while buffer!=NULL do
    buffer=radio.receive()
    transaction=buffer.read()
    send(transaction)
    Sleep(interval)
end while
```

D. RESTful API

Data stored in the blockchain is accessible through APIs. A farmer can remotely display collected measurements through a web or mobile application. He can also run irrigation by changing the water pump state to on.

Algorithm 3 Transaction processing in IoT-gateway.
Input:
Transaction: received transaction
$block\_size$: The maximum size of block.
$validators\_list$: The IP addresses of the validator nodes.
Output: Pending transactions: list.

```
pendingTransaction=array[block_size]
while buffer!=NULL do
    transaction=buffer.receive()
    data=transaction.body
    signature=transaction.signature
    hash=SHA256(data)
    isValide=(ECDSA.decrypt(hash,P_k)==signature)
    if isValide then
        pendingTransaction.append(transaction)
    end if
    Multicast(transaction,validators_list)
end while
```

TABLE III
EXPERIMENTAL PARAMETERS AND HARDWARE DETAILS

Experimentation hardware	
Performance	**Details**
Name	Raspberry Pi 4B
OS	Debian 11 (bullseye) 32bit
CPU	ARM-Cortex-A72 4 x 1,50GHz
Storage	SanDisk Extreme Pro 32GB class A
Experimentation parameters	
Parameters	**Value**
Experimentation time	100 Seconds
Payload size	100 Bytes
Transaction size	172 Bytes
Time slot	1 Second
Maximum number of transaction in the block	100
Transaction rate	10-100 transactions/second
Number of transaction	1000-10000 transactions

V. EXPERIMENTAL EVALUATION

This section looks at how well the modified BC strategy works on the ISIS platform by implementing a lightweight Proof of Authority (PoA) consensus mechanism. We have developed a PoA blockchain network to demonstrate the viability and efficacy of the methodology mentioned in the preceding sections. Additionally, we have run numerous containers from a full-node image and configured these nodes as local network validators. The hardware and parameters used in the experimentation are shown in Table. III. We evaluated the CPU load and the average data usage by varying the number of validators and transactions.

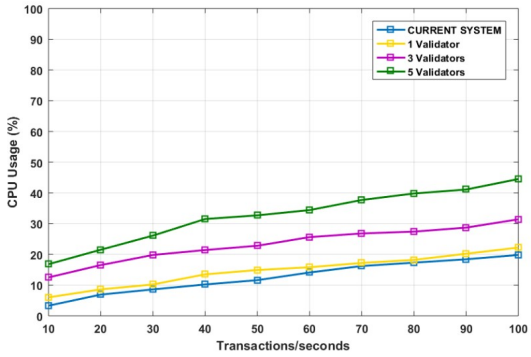

Fig. 4. Comparison of CPU usage between current and BC-based IoT gateway (Raspberry Pi 4).

A. CPU load of IoT gateway

The CPU load is an important metric to prove the efficiency of our approaches in dealing with high transaction rates without degrading ISIS. Fig. 4 shows CPU usage of IoT gateway in the ISIS. We used a Raspberry Pi 4 board (4GB model) to evaluate the performance of our solution in various transaction rates. The PoA-based solution consumes more CPU, especially when the transaction frequency is high and the number of validator nodes in the network increases due to multicast transmissions, transactions, and block validation.

There are low transaction rates in ISIS due to the slow volatility of weather and soil parameters. According to CPU usage curves illustrated in Fig. 4, an IoT gateway can handle over 100 transactions per second with less than 50% CPU usage. Otherwise, BC generates much traffic in the network when the number of validator nodes increases due to block validation.
The suggested consensus is effectively adaptable to ISIS compared to the alternative, such as PoW (Proof of work), which requires high energy consumption and expensive hardware. PoET (Proof of Elapsed Time) is another alternative that needs dedicated hardware compared to our approach based on open source and cheap hardware.

B. Average data usage

PoA consensus depends on communications between network nodes (transactions and block broadcasts). IoT gateways commonly utilize 4G and 5G technologies to connect to the internet. We will evaluate our solution according to the average data usage metric since it's billed. We used Wireshark to sniff and filter the network traffic of the loopback interface. The experiments evaluate the network data usage in a system with or without the security support of the BC mechanism according to a different number of validators in the network. The curves illustrated in Fig. 5 show that the secured system consumes more data because packets include transaction payloads and signatures. Additionally, PoA consensus generates high traffic related to blocks and transactions broadcast when the number of validator nodes in the network grows. However, the overall data usage (3.475

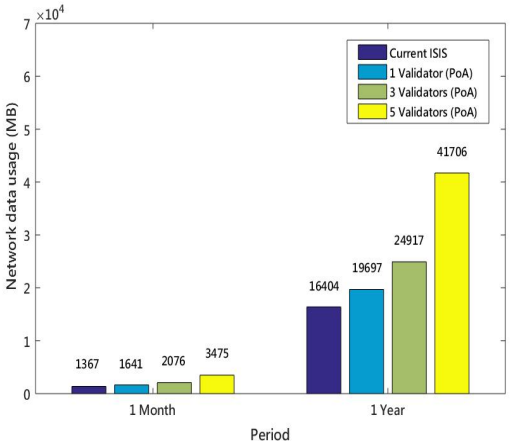

Fig. 5. Comparison of network data usage between current and BC-based ISIS.

GB in one month) is less than the amount stipulated in all agreements with Algeria's mobile service provider. Also, the proposed approach minimizes the cost of cloud storage and provides data availability through BC database replication in the local storage of IoT gateways.

VI. Conclusion and Future Work

In this paper, we have adapted BC technology to secure IoT smart irrigation systems by using PoA as a consensus mechanism. We implemented this mechanism with open-source software and applied it to an innovative, smart, sustainable, low-cost irrigation system for smallholder farmer communities built in the RIIR laboratory [16] [17]. We assessed its CPU load and network data usage resources' performance by varying the number of validators and transactions. The results show that the BC technology based on PoA consensus can be adapted to IoT applications as it consumes fewer resources (the results are comparable with those of the current system). In future work, we propose to conduct other evaluations of the proposed solution by comparing state-of-the-art mechanisms and considering other performance metrics such as latency, energy efficiency, etc.

Acknowledgements

This work has been supported scientifically by Research Laboratory in Industrial Computing and Networks (RIIR), partner of INTEL-IRRIS-PRIMA S2 2020-Project ID 1560 (https://intel-irris.eu/). It was founded by the PRFU project, code = C00L07UN310120220008 and the national food security research program (PNR).

References

[1] S. Kumar, P. Tiwari, M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review", J Big Data, vol. 6, no. 111, 2019.

[2] L. García. L. Parra, JM. Jimenez, J. Lioret and P. Lorenz, "IoT-Based Smart Irrigation Systems: An Overview on the Recent Trends on Sensors and IoT Systems for Irrigation in Precision Agriculture", Sensors, vol. 20, no. 4, pp. 1042, 2020.

[3] A. Dahane, R. Benameur, B. Kechar and A. Benyamina, "An IoT Based Smart Farming System Using Machine Learning", 2020 International Symposium on Networks Computers and Communications (ISNCC), Montreal, QC, Canada, pp. 1–6, 2020.

[4] A. Dahane, R. Benameur, B. Kechar, "An IoT Low-cost Smart Farming for Enhancing Irrigation Efficiency of Smallholders Farmers", Wireless Personal Communications, vol. 127, no. 4, pp. 3173–3210. 2022.

[5] S. K. Mousavi and A. Ghaffari, "Data cryptography in the Internet of Things using the artificial bee colony algorithm in a smart irrigation system", J. Inf. Secur. Appl, vol. 61, 2021.

[6] Anand, S.J et. al, "Iot-Based Secure And Energy Efficient Scheme For Precision Agriculture Using Blockchain And Improved Leach Algorithm", Turkish Journal of Computer and Mathematics Education, vol. 12 no. 10, pp. 2466-2475, 2021.

[7] A. Dahane, B. Kechar, Y. Meddah and O. Benabdellah, "Automated irrigation management platform using a wireless sensor network", Proc. 6th Int. Conf. Internet Things Syst. Manage. Secur. (IOTSMS), Granada, Spain, pp. 610-615, 2019.

[8] R. Sachan, S. Kaur and A. K. Shukla, "Smart Irrigation and Security System for Agricultural Crops and Trees,", in 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1-4, 2021.

[9] S. De Angelis, L. Aniello, F. Lombardi, A. Margheri, V. Sassone, "PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain", 2017.

[10] V.W. Samawi, "SMCSIS: an IoT based secure multi-crop irrigation system for smart farming", International Journal of Innovative Computing, Information and Control (IJICIC), vol. 17, no. 4, pp.1225-1241, 2021.

[11] A. Dahane, B. Kechar, A.E. Benyamina, R. Benameur, "Precision Agriculture: Automated Irrigation Management Platform Using Wireless Sensor Networks", In S. Abd El-Kader, B. Mohammad El-Basioni (Ed.), Precision Agriculture Technologies for Food Security and Sustainability (IGI Global), pp. 150-165, 2021.

[12] R. K. Shrivastava, S. Mishra, V. E. Archana and C. Hota, "Preventing data tampering in IoT networks," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, 2019.

[13] J. Deogirikar and A. Vidhate. "Security attacks in IoT: A survey, " 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37, 2017.

[14] A. Gajbhiye, D. Sen, A. Bhatt and G. Soni, "DPLPLN: Detection and Prevention from Flooding Attack in IoT," in International Conference on Smart Electronics and Communication (ICOSEC), pp.704-709, 2020.

[15] P. Gupta, S. Kumar, "A Comparative Analysis of SHA and MD5 Algorithm, " International Journal of Computer Science and Information Technologies, Vol.5, no.3, pp.4492–4495, 2014.

[16] A. Dahane, R. Benameur, and B. Kechar, "An Innovative Smart and Sustainable Low-Cost Irrigation System for Smallholder Farmers Communities," 3rd International Conference on Embedded Distributed Systems (EDiS), Oran, Algeria, pp. 37–42, 2022.

[17] INTEL-IRRIS : Intelligent Irrigation System for Low-cost Autonomous Water Control in Small scale Agriculture, Available: https://intel-irris.eu/ [Accessed: 26- March- 2023].