Article

Not peer-reviewed version

Mitigating Threats in LoRaWAN Air Pollution Monitoring: Blockchain-Integrated Wireless Security for Azores Archipelago

Nick Nguyen * , Sean Venezia , Joshua K Davis , Orlando Baiocchi , DC Grant

Posted Date: 24 April 2024

doi: 10.20944/preprints202404.1601.v1

Keywords: LoRaWan; Blockchain; Lightweight Scalable Blockchain; IoT devices; consensus mechanism; transaction processing

 doi:10.20944/preprints202404.1601.v1

Article

Mitigating Threats in LoRaWAN Air Pollution Monitoring: Blockchain-Integrated Wireless Security for Azores Archipelago

Nick Nguyen *, Sean Venezia, Joshua K. Davis, Orlando R. Baiocchi and DC Grant

University of Washington at Tacoma, UWT, School of Engineering and Technology Tacoma, WA, USA; sv34@uw.edu (S.V.); davisj34@uw.edu (J.K.D.); baiocchi@uw.edu (O.R.B.); dcgrant@uw.edu (D.G.)
* Correspondence: nml123@uw.edu

Abstract: The Azores Archipelago is a collection of volcanic islands near northwestern Portugal in the Atlantic Ocean. Because of the importance of accurate environmental monitoring for the advancement of research, transportation and tourism, a LoRaWan Sensor Network was developed to monitor levels of air pollution across these islands. This study presents an approach to the implementation of a blockchain network that is both lightweight and scalable, with the goal of preventing man-in-the-middle attacks on the design of sensor networks.

Keywords: LoRaWan; blockchain; lightweight scalable blockchain; IoT devices; consensus mechanism; transaction processing

I. Introduction

Ongoing research collaboration between University of Washington-Tacoma and University of the Azores has deployed a network of Internet of Things (IoT) devices for weather monitoring using a low-power wide-area network. This was done to effectively monitor and analyze the impact of tourism on the Archipelagos of the Azores (Portugal), which has been a UNESCO World Heritage Site, since 1983 [1]. (LoRaWan). This collaboration has resulted in a variety of experiments, as well as the development of a low-cost sensor [2], a calibrated intelligent sensor for weather monitoring [3], an air pollution detection system that uses edge computing [4], and an experimental implementation of LPWAN LoRa in both urban and forestall environments [5]. The study demonstrates the feasibility of applying blockchain technology in conjunction with Long Range (LoRa) in the IoT devices to ensure safe communication. This article proposes the development of Lightweight Scalable Blockchain implementing an Ordered Markle Tree as the data structure for the blockchain network.

The remaining parts of the paper are structured as described below. In Section II, a concise introduction to the Azores Archipelago project and issues regarding the data integrity of its communications are provided. This section also describes current man-in-the-middle attack concerns on the network, and the significance of using blockchain security as a potential method to secure communication between each Internet-of-Things device in a LoRaWan network.

Section III provides information on the existing network design. In Section IV, we will discuss the data structure and cryptographic protocols for the star topology network to mitigate risk against a man-in-the-middle attack. In the final section, we provide our conclusions and discuss possible future research.

II. Related Work

A. LoRaWAN Network for IoT

The physical layer used by LoRaWAN is called LoRa [6]. LoRa is a proprietary radio communication technique based on the Chirp Spread Spectrum (CSS) modulation [7] developed by

 doi:10.20944/preprints202404.1601.v1

Cycleo, later acquired by Semtech in 2012 [8]. “LoRa is one of the most used applications because of the facility to develop private networks operating in the unlicensed frequency bands (868 MHz in Europe, 915 MHz in USA and Brazil)” [6,9–11].

The information is dispersed across a frequency using a Spreading Factor (SF) used in CSS modulation. The number of chirps associated with each signal symbol is determined by the SFs, which are orthogonal to one another. The number of SFs that can be used in LoRa networks ranges from 7 to 12 and determines the amount of data that can be transmitted using the same number of bits. Capability of a receiver to demodulate the message is improved by increasing the number of bits used per symbol. A higher SF indicates that more bits are required to transmit the same information.

On the other hand, installing the end device at a greater distance from the gateway is feasible. Because SFs are guaranteed to be orthogonal to one another, multiple end devices can send their packets over the same frequency while utilizing a variety of SFs. Different bandwidths can be selected from 125, 250, and 500 kHz. In most cases, a bandwidth of 125 kHz is utilized by networks. Time on Air (ToA) refers to the time a single transmission uses the air interface to send a packet.

Determining the Time on Air (ToA) requires knowing the relation between the SF, bandwidth, and packet size. There can be large differences between the ToA of two packets of the same size using the same bandwidth but different SF. To put this into perspective, the time required to send a packet containing 50 bytes over a bandwidth of 125 kHz is 0.113 seconds when using SF 7, but it takes 2.62 seconds when using SF 12. When only the ToA is considered, the latency required to deliver a packet is at least 20 times higher with SF 12 than with SF 7. The article [12] provides a more in-depth comparison and considers other SFs. The SF, bandwidth, and packet size directly impact the link's throughput [13]. When it comes to throughput, one device's ability to transmit with a low value of SF is superior to another device's ability to transmit with a high value of SF. The increase in SF, on the other hand, also increases the transmission range [14]. The SF, throughput, and ToA relationship is broken down and summarized in Table 1. This table considers a packet with varying payload sizes, 125 kHz bandwidth, and no duty cycle restrictions.

LoRaWAN is a data link layer protocol developed by LoRa Alliance in 2015 and designed specifically for low-power, wide-area networks (LPWAN) in IoT applications [6,15,16]. It operates in the sub-gigahertz frequency bands to enable long-range communication with low data rates, extended battery life, and secure bidirectional communication. “In recent years, low-power wide-area networks (LPWAN) have been developed to provide a workable solution for applications that require energy efficiency as well as coverage over a large area [14]. At its core, LoRaWAN is a layered protocol stack that follows the LoRa physical layer modulation scheme. The stack comprises three main layers; Physical, Data Link, and Network. The LoRaWAN network itself consists of three key components; End Devices (or Nodes), Gateways, and Network Server. End-devices, which are part of the LoRaWAN network, send data to gateways to create a star network topology. Only one hop is permitted per the specification between the end devices and the gateway [6,9,10]. The most popular version of the LoRaWAN specification is 1.0.3 [10], while the current version is 1.1 [9].

LoRaWAN for IoT devices is categorized into different classes based on their communication and power-saving capabilities. LoRaWAN specifications define three device classes: Class A, B, and C. Each of these classes has specific characteristics and trade-offs in power consumption, latency, and communication timing.

Class A devices are the most power-efficient and commonly used class in LoRaWAN networks. They operate in a bi-directional communication mode with a scheduled receive window. After transmitting data, Class A devices open two short receive windows at predetermined time intervals, allowing for downlink communication from the network server. Class A devices have the lowest power consumption but experience longer latency as they only listen for downlink data after sending an uplink transmission.

Class B devices are an extension of Class A devices and provide additional features for reduced latency. In addition to the scheduled receive windows of Class A, Class B devices periodically open additional receive slots synchronized with the network's beacon. This allows for more frequent

 doi:10.20944/preprints202404.1601.v1

downlink communication from the network server, reducing latency. However, Class B devices consume slightly more power than Class A devices due to the additional receive slots.

Class C devices offer continuous receive mode, enabling them to always listen for downlink communication, except during their own uplink transmissions. This results in the lowest latency among the LoRaWAN device classes but at the expense of higher power consumption. Class C devices are typically connected to a more reliable power source or have access to a continuous power source, as they consume more energy than Class A and Class B devices.

B. Man-in-the-Middle Attack on LoRaWan

A Man-in-the-Middle Attack (MITM) is an attempt to disrupt the security and privacy of the data causing a confidentiality issue [17]. The main concern with an MITM attack is modification of data by unauthorized actors. The term Man-in-the-Middle is derived from a basketball mini-game in which two players attempt to pass the ball to one another, and a third player in the middle tries to intercept the pass. Man-in-the-middle attacks have also been referred to as monkey-in-the-middle attacks, a fire brigade attacks, or bucket brigade attacks [18]. MitM attacks involve an attacker intercepting and potentially altering communication between two parties who believe they are directly communicating with each other. Unlike traditional encryption-breaking techniques, MitM attacks exploit vulnerabilities in the communication protocols or infrastructure rather than directly targeting encryption algorithms. Encryption remains a crucial component in securing data. MitM attacks exploit weaknesses in the overall communication process to eavesdrop on sensitive information, modify the data or impersonate one or both parties [19].

For a Man-in-the-Middle Attack on a LoRaWan, an attacker will logically position themselves between the IoT device and the gateway [20]. The adversary may accomplish this goal by taking advantage of flaws in the communication protocols used by the devices or by physically tampering with them. The attacker can intercept and modify the data that is being transmitted between the device and the gateway. There are several potential vulnerabilities present in several of the LoRaWAN infrastructure components. Examples include unsafe key management, lack of end-to-end encryption, or inadequate device authentication [20].

Unauthorized access to the devices can jeopardize sensitive data and compromise crucial control systems. Countermeasures can be put into place to reduce the dangers connected with MitM attacks on LoRaWAN. These include: i) End-to-end encryption for data transmission to ensure the confidentiality and integrity of the communication. ii) Employ certain critical management practices, such as key rotation and secure storage, to ensure encryption keys are protected and not susceptible to theft or misuse. iii) Robust device authentication mechanisms, such as mutual authentication between IoT devices and gateways, can prevent unauthorized entities from participating in the network [21].

C. Blockchain Security

Blockchain is a secure ledger that organizes a dynamically growing list into a hierarchical data structure of expanding chain of blocks [22]. Each block stores cryptographically information about its transaction records. Blockchain can update its transactional records when adding a new block into its blockchain system through a verification process by using a consensus procedure [23]. A block will have a hash value of itself and the previous block's hash value in the chain, creating a cryptographic linkage between each block in the data structure. Because every block in the chain contains a cryptographic hash of the block that came before it, it is exceedingly difficult for an adversary to change any record without also changing all of the blocks that came after it. As the data kept in a blockchain network will retain both its integrity and its secrecy, the term “blockchain security” is used in academia and industry as a reference. The blockchain has three main important components, i) hash chain storage, ii) digital signature, and iii) consensus mechanism, allowing blockchain to add new blocks to its chain. Combining these three security techniques, blockchain can be used effectively against any attempt to tamper with the transaction data records stored inside its block [22].

 doi:10.20944/preprints202404.1601.v1

Hash pointers are cryptographic hashes that verify the integrity of the data stored in a block by pointing to the location where the data is stored. Since we can use a hash pointer as a checker to see if the data has been tempered, an adversary who tries to tamper with data by using MitM for any block would need to change the hash pointers of all previous blocks. However, this becomes increasingly difficult as the tampering would have to extend to the initial opening block – the genesis block – where the adversary will have to stop with the tampering process because it would be detected by comparing the recorded root hash pointer with the actual root hash pointer, ensuring tamper-resilience.

III. Current Network Design

A. Network Architecture

As economic and ecological needs continue to grow, alongside technological advancements. It is essential to do an analysis of the current design of the network in terms of both security and potential vulnerabilities. The architecture in question is an Internet of Things network that makes use of LoRa technology, which has recently attracted a lot of attention due to the fact that it can send vital data over great distances while using a relatively small amount of power [24]. The issue in the design is to meet certain parameters, such as power needs, as well as to achieve varied distances between end devices and gateways to the Wide Area Network (WAN).

In this particular scenario, the LoRa system is required to be utilized by the stakeholders in the Azores Air Quality Pollution Project. As shown in Figure 1, the first iteration of the LoRa system makes use of a network server powered by The Things Network (TTN) and implements a star network topology that is based on LoRaWAN [25].The RAKwireless 5146 LoRa concentrator module, shown in Figure 2, is used to construct the LoRaWAN gateway, which is then stacked on a Raspberry Pi 3 Model B+ (shown in Figures 3 and 4).

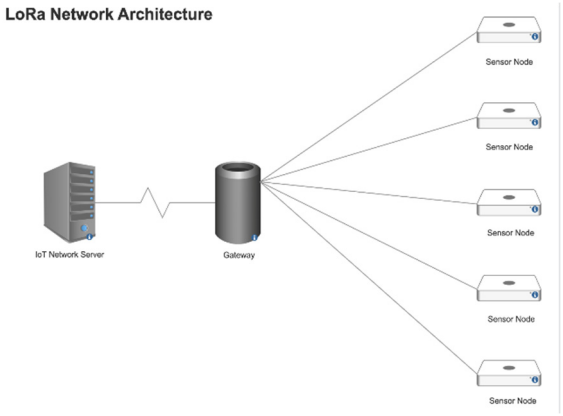

Figure 1. LoRa Network Architecture.

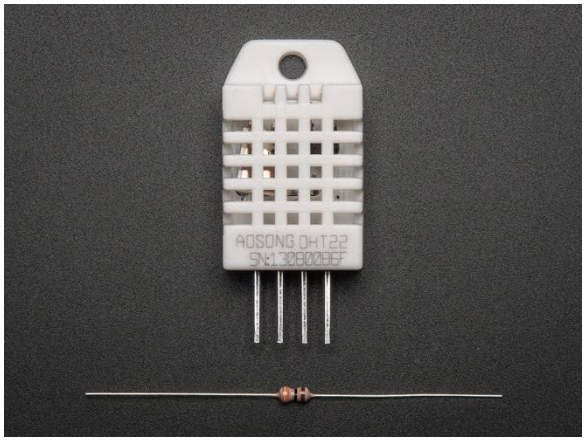

Figure 2. DHT22 Temperature humidity sensor.

 doi:10.20944/preprints202404.1601.v1

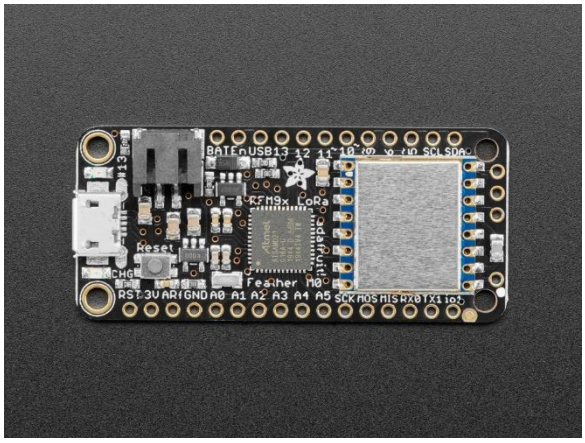

Figure 3. Adafruit Feather M0 RFM96 LoRa.

Figure 4. RAK5146 Gateway Concentrator Module.

This gateway acts as a data bridge between the sensor nodes and the TTN. It is essential to emphasize the significance of doing exhaustive risk assessments on the LoRa Internet of Things network design. It is necessary to take precautions including the implementation of secure authentication procedures, robust encryption mechanisms, and continuous monitoring for potential threats. In addition, patches and updates should be applied on a consistent basis in order to close any potential security holes. In order to stop potential attacks on the supply chain, it is also important to verify that only trusted hardware and software components are used.

The architecture of the LoRa network that is depicted in Figure 1 is based on a star network topology. In this topology, sensor nodes use LoRa communication technology to communicate with a gateway. After then, the gateway will send the data collected by the sensors to the server that is part of the TTN network, where it will be saved. Stacking a RAKwireless 5146 LoRa concentrator module atop a Raspberry Pi 3 Model B+ constitutes the LoRaWAN gateway's hardware configuration. The data bridge that connects the sensor nodes and the TTN is provided by the RAKwireless LoRa concentrator. Utilizing technology based on blockchains allows for the data that is being communicated to be protected against unauthorized access.

B. Current Hardware Specifications

Figure 2 depicts the communication architecture of the sensor nodes, which utilizes unidirectional antenna modulation with a spreading factor of 7, running at a bandwidth of 125 kHz on the US 902-928 MHz frequency [26]. This communication architecture is depicted in the figure. The utilization of the DHT-22 temperature and humidity sensor, which has an operating voltage of 3.3 Volts, makes the collection of data regarding the surrounding environment simpler. The code for the sensor is executed by the microcontroller that is a part of the system. This microcontroller is an ARM Cortex M0 CPU that runs at 3.3 Volts and is clocked at 48 MHz [27].

As shown in Figure 3, the RAK wireless concentrator performs its operations using the same parameters as the sensor nodes.

 doi:10.20944/preprints202404.1601.v1

It makes use of an omnidirectional antenna that is able to receive communications from any direction within a 360-degree radius.

IV. Blockchain Technology

A. Lightweight Scalable Blockchain Architecture Using Ordered Merkle Tree

The proposed architecture for IoT devices in the LoRaWan network is to implement LSB using a Merkle Tree data structure [28] where the data is constructed into a series of data blocked. In a Merkle tree, each internal node in the hierarchy will have a hash value of its children node.

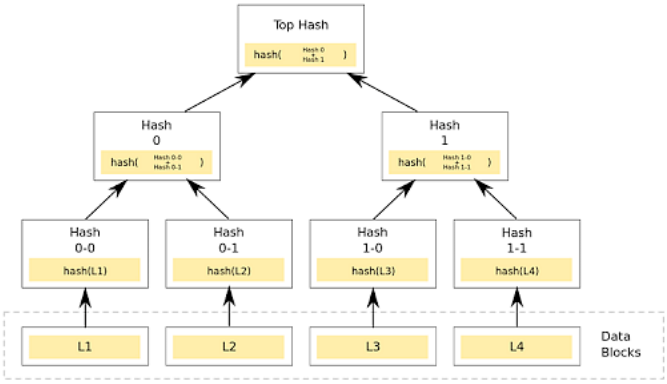

Figure 5. Binary hash trees for blockchain data encryption.

At the same time, a leaf node will hold the value of the direct hash value of the corresponding data block [29]. The weather data collected from the DHT22 Temperature humidity sensor will be formatted and sorted to create an Ordered Merkle tree (OMT) data structure [30].

In an OMT structure, each leaf in the tree will contain a triplet data:

$$L_n = \{k, k_n, a\}; \quad n \in N$$

Where k is the unique key in the dictionary, k_n is the next key, and a is the set of weather data value.

By implementing OMT, LSB can use the proof of existence process to mitigate the risk of MitM attack to control and manipulate weather data in the star topology network by verifying in each transaction that there is an existence of a key-value pair (k_p, a).

If keys value pair (k_p, a) in the OMT leaf does not exist within the interval $[k_i, k_n]$. There are three edge cases that imply:

$$If\ i < n, k_i < p < k_n, [k_p, k_p] \tag{1}$$

$$If\ i > n, i > p > n, [k_p, k_i] \tag{2}$$

$$If i = n, i = p = n, [k_p] \tag{3}$$

The OMT integrity verification process can verify the legitimateness of a large new weather dataset by comparing the hash value of specific data block L_n to the corresponding leaf node L_{n+c} in the Merkle tree. Enable the ability to quickly determine if the data block L_n has been tampered with by MitM. The dataset L_n will not have the corrected computed hash value if data has been tampered with.

V. Conclusion and Future Work

Further investigation of the project's hardware and software components will be an integral part of the work that will be done in the future for the lightweight scalable blockchain that is described in this article. Regarding the software, the objective will be to identify the most efficient piece of code to

 doi:10.20944/preprints202404.1601.v1

run on the Adafruit M0 and the RAK2287 while consuming the least amount of battery power, accumulating data from additional sensors, and integrating blockchain. Concerning the hardware, a study into the interoperability of multiple sensors for particular air contaminants is going to be required. In addition to this, testing will be necessary in order to guarantee that the system is both scalable and secure. In terms of scalability, the cryptographic protocols and hash calendar that the proposed architecture incorporates have the potential to lower the amount of overhead required for intermittent participants.

On the other hand, ambiguities in consensus can be reduced through the use of a separate timestamp ledger as well as the explicit specification of predicates. Other solutions have also been investigated to address the scalability of blockchains, and while they are similar to the methodology that has been described, these other strategies are not intended to handle precisely the quantity of data that is involved in calculations. As a result, future work will concentrate on properly scaling the lightweight scalable blockchain while also resolving scalability concerns in order to guarantee the system's performance and safety.

References

1. O. Baiocchi, F. C.C. Martins, F. Baiocchi, K. Biondi, S. Teng and C.P. De Souza, “User-Generated Data Collected from a Wireless Sensor Network: Monitoring Air Pollution Levels in the Azores, 2019, Guimarães. Anais do XI International Conference on Engineering and Computer Education - ICECE2019, 2019. p. 1-2.
2. M. R. Villarim, D. F. Medeiros, L. C. S Medeiros, C. P. de Souza, M. H. Pontieri, N. A dos Santos and O. Baiocchi, “A Calibrated Intelligent Sensor for Monitoring of Particulate Matter in Smart Cities,” Sensors and Transducers, vol. 250, no. 3, pp. 1–9, Mar. 2021.
3. K. Biondi, E. Al-Masri, O. Baiocchi, S. Jeyaraman, E. Pospisil, G. Boyer, and C. P. de Souza, “Air Pollution Detection System using Edge Computing,” in 2019 International Conference on Engineering Applications, ICEA 2019 - Proceedings, 2019.
4. M. R. Villarim, J. V. H. de Luna, D. F. Medeiros, R. I. S. Pereira, and C. P. de Souza, “LoRa performance assessment in dense urban and forest areas for environmental monitoring,” in INSCIT 2019 - 4th International Symposium on Instrumentation Systems, Circuits and Transducers, 2019.
5. J. P. Shanmuga Sundaram, W. Du and Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 371-388, Firstquarter 2020, doi: 10.1109/COMST.2019.2949598.
6. What Is LoRa? [online] Available: https://www.semtech.com/lora/what-is-lora.
7. Semtech, [Online]. Available: [Archived from the original on Julu 18, 2019]. [Accessed: February 5, 2020.]
8. J. P. Shanmuga Sundaram, W. Du and Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 371-388, Firstquarter 2020, doi: 10.1109/COMST.2019.2949598.
9. B. Reynders and S. Pollin, “Chirp spread spectrum as a modulation technique for a long-range communication,” in Proceeding of the 2016 Symposium on Communications and Vehicular Technologies (SCVT), Mons, Belgium, 22-22 November 2016, pp. 1-5.
10. LoRa Alliance, “LoRaWAN 1.0 Specification,” 2015 [Online]. Available: https://lora-alliance.org/resource-hub/lorawanr-specification-v10
11. LoRa Alliance, “LoRaWAN 1.0 Specification,” 2017 [Online]. Available: https://lora-alliance.org/resource-hub/lorawanr-specification-v11
12. LoRa Alliance, “LoRaWAN 1.0.3 Specification,” 2018 [Online]. Available: https://lora-alliance.org/resource-hub.lorawanr-specification-v103
13. J.P. Shanmuga Sundaram, W. Du, Z. Zhao, “A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 371-388, 2020.
14. J.Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, “A Survey of LoRAWAN for IoT: From Tehnology to Application, “Sensors, vol. 18, no. 11, pp.3995, 2018.
15. U.Raza, P. Kulkarni, and M. Sooriyabandara, “Low Power Wide Area Networks: An Overview,” IEEE Communications Survey & Tutorials, vol. 19, no. 2, pp.855-873, 2017.
16. L. Vangelista, A. Zanella, and M. Zorzi, “Long-Range IoT Technologies: The Dawn of LorRa,” in Future Access Enablers for Ubiquitous and Intelligent Infrastructures, V. Atanasovski and A. Leon-Garcia, Eds., Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 159, Springer International Publishing, Cham, Switzerland, 2015, pp. 51-58.
17. Mallik, Avijit. "Man-in-the-middle-attack: Understanding in simple words." Cyberspace: Jurnal Pendidikan Teknologi Informasi 2.2 (2019): 109-134.

 doi:10.20944/preprints202404.1601.v1

18. G. Nath Nayak and S. Ghosh Samaddar, "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, China, 2010, pp. 491-495, doi: 10.1109/ICCSIT.2010.5563900.
19. S. Heinrich, Public Key Infrastructure based on Authentication of Media Attestments. arXiv:1311.7182
20. B. Bhushan, G. Sahoo and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — A review," 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), Dehradun, India, 2017, pp. 1-6, doi: 0.1109/ICACCAF.2017.8344724.
21. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.
22. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction."
23. R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," ACM Computing Surveys, vol. 52, no. 3, Article No. 51, pp. 1-34, 2019. Available: https://doi.org/10.1145/3316481
24. LoRaWAN Part 1: How to Get 15 km Wireless and 10-Year Battery Life for IoT [online] Available: https://www.digikey.com/en/articles/lorawan-part-1-15-km wireless-10-year-battery-life-iot
25. Using LoRaWAN and The Things Network with Feather [online] Available: https://learn.adafruit.com/the-things-network-for feather.
26. Frequency Plans [online] Available: https://www.thethingsnetwork.org/docs/lorawan/frequency plans/index.html [19] LoRa and LoRaWAN: Techincal overview | DEVELOPER PORTAL [online] Available: https://lora developers.semtech.com/library/tech-papers-and-guides/lora-and lorawan.
27. Khalifeh A, Mazunga F, Nechibvute A, Nyambo BM. Microcontroller Unit-Based Wireless Sensor Network Nodes: A Review. Sensors. 2022; 22(22):8937. https://doi.org/10.3390/s22228937
28. R. C. Merkle, “A Digital Signature Based on a Conventional Encryption Function,” Advances in Cryptology, CRYPTO ’87. Lecture Notes in Computer Science 293. 1987.
29. D. Koo, Y. Shin, J. Yun, and J. Hur, “Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience,” Applied Sciences, vol. 8, no. 12, p. 2532, Dec. 2018, doi: 10.3390/app8122532.
30. M. Ramkumar, "Scalable Computing in a Blockchain," 2018 IEEE 39th Sarnoff Symposium, Newark, NJ, USA, 2018, pp. 1-6, doi: 10.1109/SARNOF.2018.8720499.