Grenze International Journal of Engineering and Technology, June Issue

Ensuring Security and Energy Efficiency of WSN

Bharath RV[1], Adithya S[2], Charan Gangadkar R S[3], Shrihari M R[4], Ajay N and Mahesh M R[5]
[1]S J C Institute of Technology Chickaballapur 562101
[2-5]Mahesh M R NCET College Banglore
Email: bharathrv123@gmail.com,adithya2001.18@gmail.com, Charangangadkar@gmail.com,
shrihari.mr@gmail.com, n.ajay2@gmail.com, mahesathya@gmail.com

***Abstract*—The suggested approach uses blockchain technology to improve the data protection of wireless sensor networks. (WSNs). This study uses transmission of data and blockchain-based methods to construct a very secure WSNs infrastructure. Present-day wireless network is built using Internet of Things (IoT) design and strengthens data transmission reliability using a blockchain-based technique. Every small-area wireless sensor network in the research being suggested has primary data collections of nodes known as a mobile database,which serves as the foundation for the complete WSNs structure. This study's "mobile database" node employs embedded microcontrollers with operating systems, like the Raspberry Pi and Arduino Yun.the hash value of the transaction data, the previous block, and the current timestamp, as well as sensor data that was separately collected by the block's sensors. The transactional information utilised in our research is displayed is sensor data from a wireless network. In essence, the system uses the Merkeltree algorithm in combination with the hash function. Such programming makes it challenging to alter the content of the block using blockchain-based technology. The research methodology converts a database of sensor data into a blockchain-based transaction ledger. As a result, the suggested system gathers and analyses sensor data to enhance the wireless sensing network's topology. A system based on the blockchain can operate a private cloud end, according to the novel. This essay continues by visualizing the uploading drawing charts that match to the data collected by the sensors using big data analysis. Python coding languages make it simple to model and visualise the corresponding images because the web page servers of the system that is suggested is built with the operating system that is embedded. Finally, this work develops a computerized mobile data and internet server that applies the blockchain method to mobile databases using the JavaScript programming language and the Node.js runtime environment. The experiment, which used roughly 1600 data records, proved the proposed method to be accurate. The findings indicate that there is extremely little chance of data being altered, and there is nearly no chance at all.**

Keywords—Blockchain, the Internet of Things, wireless sensor networks, security, dependability, and energy efficiency

I. INTRODUCTION

This study adds blockchain technology to a wireless sensor network, which is a significant innovation (WSN). The suggested remedy reflects an enhancement to the remedy. This study builds on [1] with more, in-depth extensions, and more experimental results are addressed in [2]. A blockchain based web page system is supported when a blockchain-based approach is coupled with a web service [3][4]. Blockchain has the benefit of being decentralized, which means that data is not dependent on a one server. The sensed data must be collected and transformed in one

Grenze ID: 01.GIJET.9.2.374

location due to dependence on a single server.
The risks related to the data repository are reduced when filing dissemination is done using a blockchain-based mechanism [5].
This study suggests a blockchain-based approach that is built within WSNs architecture. The blockchain based method proven the trustworthy and has the strength to become the cutting-edge IoT method . Fig. 1 displays the full system architecture of this investigation. The left-hand hardware components are sensors for parameters including temperature, humidity, and air quality.
For measuring environmental data, the research employs a variety of microcontroller device models, and the common algorithm of artificial intelligence are used for basic data sorting [8].
The information are first sorted fundamentally, according to kind, and then maintained in a database using a cloud end connection. The method also runs data for inquiry, then converts the analysis into real-time webpage pictures using both the java script and python computer languages.
The suggested system can then provide a graphical analysis using the sensor data. A remote operator can simultaneously log in to the proposed system to view these results. As internet programmers and browsers may access the data from these sensors, this strategy is not limited to any particular mobile device operating system. If a browser application is available on the mobile device, the any operator can easily login with the system and view sense the data and also the systems graphical evaluation .
Many advantages of blockchain are used in this study. The fact that communicated messages are decentralized and difficult to tamper with is the most important factor. The use of distributed account and storage removes the need for centralised hardware or administration, aligns the rights and responsibilities of each node, and allows the nodes with encryption capabilities to retain the data blocks utilised in the study [11] [12]. The suggested blockchain-based solution stores the sensor data continuously after it has been verified and included to the block [13] [14] [15]. When attackers continuously look after more than 51% of the data-nodes, the blockchain based system functioning is compromised. Since updating the database on one of the nodes has no effect, the blockchain information is incredibly secure and trustworthy. As a result, anytime, anywhere, the solution being provided built around blockchain technology has all of the necessary sensor data. [16] [17] [18] \s [19].

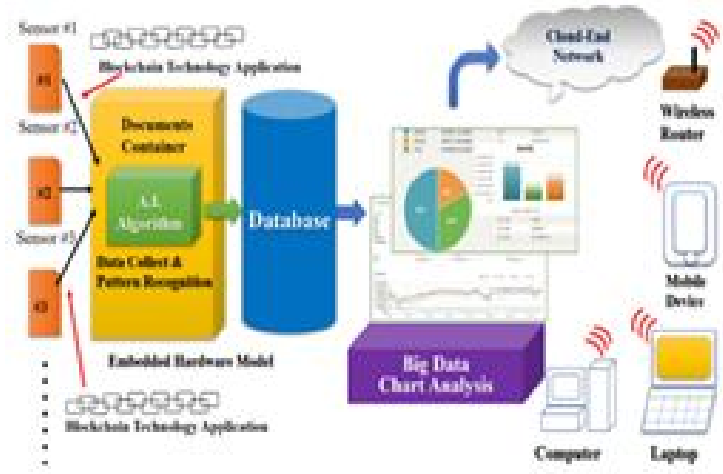

Figure 1: The proposed WSN with blockchain technology

II. BLOCKCHAIN STRUCTURE

Blockchain technology is distinguished by its uses the architecture of peer-to-peer network to accomplish decentralisation. Peer-to-peer networking-based early blockchain technology has improved the decentralised network design. [20 ,21]. The term "application" is frequently used in current research to describe software programming. Even so, the programming up such systems programmer that specifies a certain goal. Many of the millions of software developers presently in use a centralized server-client design. Despite the fact that the majority of network types are distributed, some cutting-edge network topologies are decentralized [22 ,23]. Conventional transactions rely on trustworthy central financial organizations acting as a middleman on both the client and server sides, Moreover, every transaction that passes through this centralized organization is tracked and governed. When compared, P2P network protocol is used by Bitcoin to enable direct user-to-user transactions without the requirement for a middleman [24 – 26].

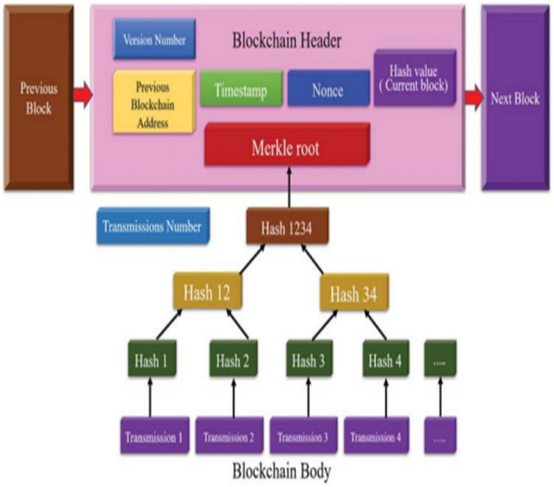

Fig.2 Block chain structure

A record of sensor data is created from the blockchain transaction document utilized in this study and saved in data blocks. The current number of sequences, the block header postcode, the timestamp, pseudo random (nonce), the target frame that contains the present frame (bits), and the Merkel's tree are all included in the data block. like a basic principle (Merkle-root). The data amount and information about the collected data are mostly included in the block body. Every piece of data is stored in a data block for ever and may be accessed later in the chain of data, much like information kept in a book. A data block's Merkle tree contains only digitally signed data. verifying that every component of acquired data is unique and that no transactions are saved more than once. The Merkle-tree hash function is then applied to all collected data to provide distinct values of it for the blocking of the header [27, 28]. Figure two presents the blockchain organization culture. The most illustrative aspect of the blockchain design is that the timestamp and information cannot be altered.

III. Cryptography Technology Application To Blockchain System

The FIPS has authorised a collection of cryptographic hash functions, which are called as the secure hash algorithms (SHAs) Different input data can be calculated using the SHA algorithm to create a fixed-length of strings known as a message digest, which is equivalent to digitally displayed message [29,30]. In blockchain system, hash functions are used extensively. The following are some benefits of using hash functions to store blockchain data:

a) A hash function processes data in a unidirectional manner, making It is quite difficult to infer the input information from the final output numbers.

b) The start vectors (256 bytes) and first block data are entered into SHA256 using the Merkle-Damgard translation technique to produce 256 bytes. A hash algorithm like SHA256 blocks the information for processing, with each block holding 512 bytes. Also, the initial vector and the next number are converted using the Merkle-Damgard algorithm, and this procedure is continued until the last data block. A 256-byte hash is the end result. As a result, the hash function will be longer the longer the input data are.

c) The output value of a hash function will differ significantly if the input values are numerously different A dual SHA256 hash function is the hashing algorithm that blockchain systems utilize the most frequently. The initial Binary number having a length of 256 bits often generated for verify after raw data of varied length have been displayed using 2 SHA256 hash algorithms [31,32]. The blockchain's uneven encryption process is shown in Figure 3. Figure 3 implements the elliptic curve cryptography (ECC) technique, a typical asymmetric encryption method.. As seen in Figure. 3Typically, an operating system-secure random source sends a 256-bit random value to the blockchain system as a private key. As there are 2256 private keys in existence, it is challenging to hack the key [33–36].

Messages and message digests are the electronic equivalents of documents and fingerprints. A document should be analyzed by a cryptographic hash function algorithm in order to protect its integrity. The result is a fingerprint-like compressed representation of the message known as the message digest. In Figure. 4 [37], the creation of a message digest is shown.

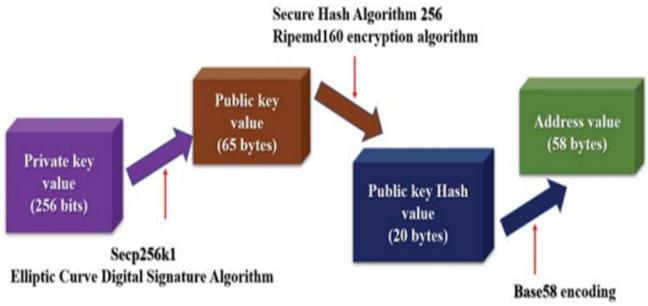

Figure 3: Asymmetric encryption on the blockchain

Messages and message digests are the electronic equivalents of documents and fingerprints. A document should be analyzed by a cryptographic hash function algorithm in order to protect its integrity. The result is a fingerprint-like compressed representation of the message known as the message digest. In Figure. 4 [37], the creation of a message digest is shown.

Despite their similarities, both frames—document-fingerprints and message-message digest—have some differences. Information and information descriptions could be delivered individually or collectively, however documents and fingerprints are physically linked. The most crucial thing is to safeguard message summaries against modifications. The system runs the password hash function once more to verify a message's or file's integrity. The new digest is compared to the previous digest by the system. The initial message has not changed if the two are the same. In Figure. 5, the process diagram for file integrity checking is displayed.

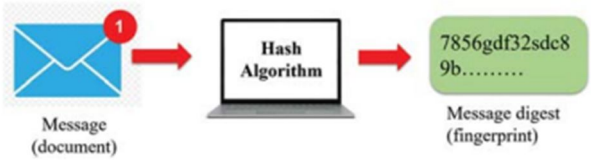

Figure 4: shows a message and its digest.

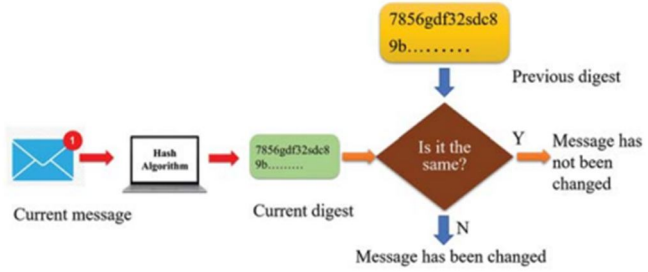

Figure 5: procedure for verifying file integrity

IV. Data Fusion Algorithms

Data fusion from several sensors is the combination of data obtained from multiple sensors and data sources. To gain a deeper knowledge of the observed event, Under some circumstances, the appliance containing the data fusion feature instinctively evaluates data and conducts data processing. There are several benefits to using data fusion technology to run the data transvered by various heterogeneous sensor and also at the various levels and from various perspectives in water-environment control and monitoring systems. The water condition identification system contains several sensors, a large amount of data, and a broad spread. The system is broken up into many subsystems that each conduct distinct analyses, and the findings of these analyses are then incorporated to get the mixed result of the present complete system. This reduces the strain on communications systems and calculation amount at the control center. In the proposed fusion system, local fusion is combined with global fusion using a decentralized two-level fusion architecture as shown in the Figure.

A. Local Fusion Algorithm

The traditional vector Kalman filter approach can achieve local fusion since the subsystem dimensionality is typically low and the number of water detection sites is frequently modest. A q-dimensional vector is created from

signals obtained from every aquatic detection location. assuming there are q total water detection points. M(K) = [m1 (K)m2 (K)⋯mq (K)] T. The method sound is a series of separate noises. white noise δ (k) = [δ1(k)δ2(k)⋯ δq(k)] T. Then, the mathematical model of the multidimensional random signal can be expressed as:

$$M(k) = BM(k-1) + \delta(k-1), \quad (1)$$

where B = diag(b1b2 ⋯ bq) the coefficient matrix is denoted.

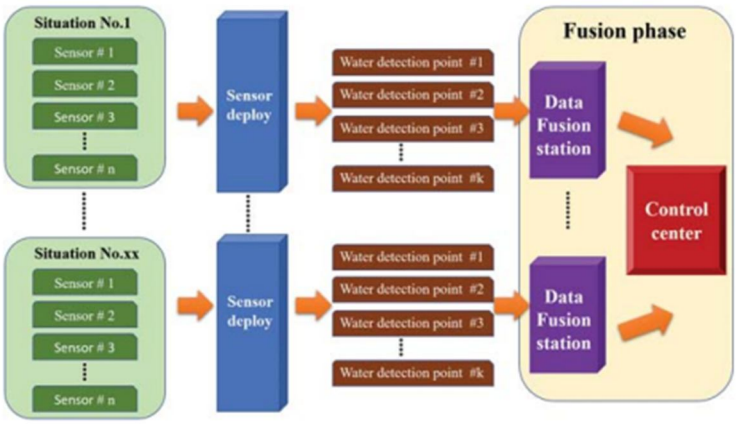

Figure 6: The fusion system's composition

The following formula can be used to represent an r-dimensional measurement data vector N(K) when the initial r components of the random signal M(K) (r q) are continuously detected at time K:

$$N(k1) = DM(k1) + T(k1) \quad (2)$$

Where D = diag(d1d2 ⋯ dr) denotes the observation matrix, and T(k1) = [t1(k1)t2(k1)⋯tr(k1)] is an additional measurement noise sequence. The following is an expression for the vector Kalman filter algorithm:

$$m\hat{}(Nk1) = Bm\hat{}(k1-1) + K(k1)[N(k1) - DMm\hat{}(k1-1)], \quad (3)$$

$$K(k1) = P1(k1)DT[DP1(k1)DT + R(k1)] - 1, \quad (4)$$

$$P(k1) = P1(k1) - K(k1)DP1(k1), \quad (5)$$

Where equation (3) denotes the equation for filter estimation, (4) denotes the equation for filter gain, and (5) denotes the equation for filter covariance. P1 (k) = BP(k 1)BT + Q (k 1) applies to (3)–(5).

The vector kalman method is a lowest technique for finding and correcting due to it is recursively filters regularly. This method makes It is als easy to use computers because to remove the real acctual time signal. The main programme and subprogram block representations for the vector version of the this filter are shown in Figs.7 and 8. The Kalman filter's state diagram is shown in Figure. 7 together with a feedback form, and its numerous state computation and conversion procedures are shown in Figure. 8.

The backpropagation (BP) technique is typically used to train forward neural networks. Unfortunately, the conventional BP approach has weak robustness and is quite sensitive; it is essentially the least squares estimation. to Outliers are a concern, thus the resilient BP algorithm (RBP), which can be stated as:

$$WIJ(k+1) = Wij(k) + \eta 1 \sigma jOI + \alpha 1[Wij(k) - Wij(k-1)], \quad (9)$$

$$\theta j(k+1) = \theta j + \eta 1 \sigma j + \alpha[\theta j(k) - \theta j(k-1)], \quad (10)$$

where η1 denotes the learning rate, α1 is the inertia term constant, and Ψ(e) = ρ (e), ρ(e) is the Hampel function. The output function is denoted as 0 and can be expressed as:

$$O_i = f_i(neti) = 1 + exp\left(-\sum_J w\,ij\,0j - \theta_i\right)^{-1} \quad (11)$$

$$\delta jj = Oj\ (1 - Oj)\ (e) \text{ (output layer)}, \quad (12)$$

$$\delta j = Oj\ (1 - Oj) \sum \delta kWk\text{j (hidden layer)}, \quad (13)$$

where f(m) represents the Sigmoid function.

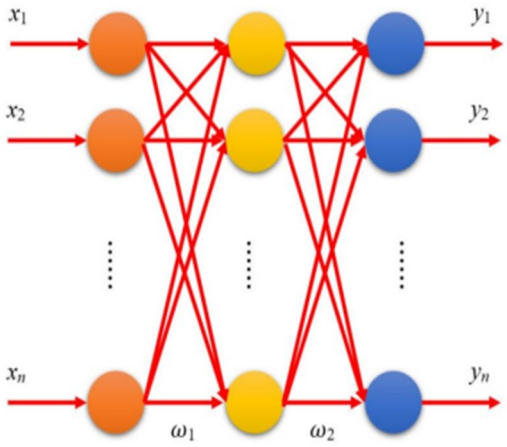

Fig 9: The single hidden layer neural network structure

V. BLOCKCHAIN-BASED WSN STRUCTURE

Blockchain exclusively transfers non-rewritable data, which results in an extremely high degree of security. The benefits of applying this safeguard to private WSNs are enormous. WSN is constructed by the most recent network configuration . Each root node is connected to almost all the sensor gadgets such as sensor0, sensor one and so on as shown in Figure 10. A number that identifies the order of blockchain joining is also present on each primary node.Each blockchain gathers information about measurements from every nodes of the remaining blocks along with information gathered by its own sensors. In other words, the most important node also obtains the sensor data when a second blockchain is generated for a node block. As a result, decentralization is used since each node stores sensor data for both itself and for other nodes, and no one node serves as the central nodeBased on calculations made by an internet-based research team for network cryptography, the most secure encryption has been selected for P2P connections between all blockchain nodes [16–19]. every information stored in the block is also maintaind by an upgraded system operator using aiml with the goal to look after the connection in the blockchain and correct the issues with the original version bitcoin mining processes. The connection between nodes on the blockchain in a WSN is depicted in Figure 10 [20]. The asymmetry cryptographic algorithm links the node sequences shown in Figure 10 with arrows, where each node represents a block's most recent and previous blocks' hash functions. Although hash functions are actually made up of many words, for the sake of clarity, they are represented in this article as a bunch of four single-digit numbers.

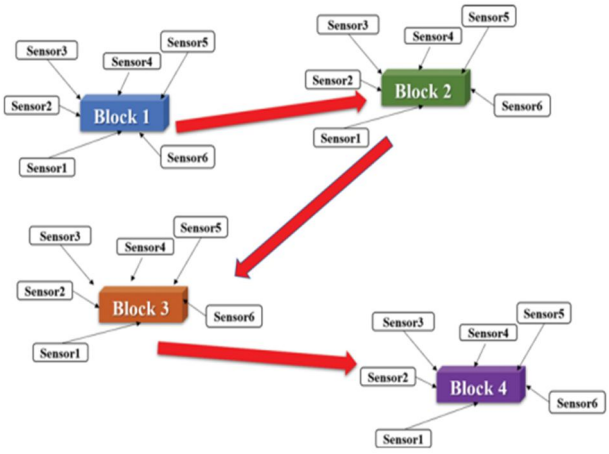

Figure 10: Blockchain technology integration in a WSN system

Figure 11: Normal block chain connecting of a WSN's primary servers

Figure 12 shows the succession of blocks with erroneous hash functions. Figure 12 shows incorrect linking because the results of the points in the series are distinct. The system instantly stops linking and data transfer in that blockchain when like erroneous linking is discovered. A brief period of delay is necessary after the blockchain linking is finished to guarantee that all of the WSN data in each subarea has been transmitted.

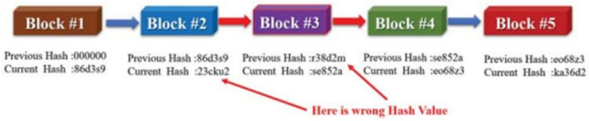

Fig 12: A abnormal block chain connections between a WSN's primary nodes

VI. Private Blockchain Implementation

Regardless of the message length, the SHA256 algorithm will provide a 256-bit hash result for each message. A message digest is the name for the 256-bit hash value that was produced. The hexadecimal string typically used to represent the message digest has a length of 64 characters and corresponds to an array with a size of 32 bytes. The SHA256 algorithm employs 64 hash variables and eight starting hash values. The eight initial numbers of the SHA256 algorithm have the following hashes:
H0 := 0x6a09e667,
H1 := 0xbb67ae85,
H2 := 0x3c6ef372,
H3 := 0xa54ff53a,
H4 := 0x510e527f,
H5 := 0x9b05688c,
H6 := 0x1f83d9ab,
H7 := 0x5be0cd19.
The first eight prime natural numbers, 2, 3, 5, 7, 11, 13, 17, and 19, form the decimal part of the square root, from which the beginning values of hashes are obtained. For instance, 0.414213562373095048 is roughly the fractional part of 2, and 0.414213562373095048 161 + a 162 + 0 163 +. As a result, the first 32 bits of the decimal representation of the square root of the prime number two are used, yielding the hash value 0x6a09e667. The SHA256 algorithm's 64 constants are displayed in Table. I.

Table 1: The 64 constants used in the SHA256 algorithm

27b70a85	2e1b2138	4d2c6dfc	53380d13
650a7354	766a0abb	81c2c92e	92722c85
a2bfe8a1	a81a664b	c24b8b70	c76c51a3
d192e819	d6990624	f40e3585	106aa070
19a4c116	1e376c08	2748774c	34b0bcb5
391c0cb3	4ed8aa4a	5b9cca4f	682e6ff3
748f82ee	78a5636f	84c87814	8cc70208
90befffa	a4506ceb	bef9a3f7	c67178f2
428a2f98	71374491	b5c0fbcf	e9b5dba5
3956c25b	59f111f1	923f82a4	ab1c5ed5
d807aa98	12835b01	243185be	550c7dc3
72be5d74	80deb1fe	9bdc06a7	c19bf174
e49b69c1	efbe4786	0fc19dc6	240ca1cc
2de92c6f	4a7484aa	5cb0a9dc	76f988da
983e5152	a831c66d	b00327c8	bf597fc7
c6e00bf3	d5a79147	06ca6351	14292967

The 64 prime natural integers are listed above. The first 32 bits are used to calculate this cube root's decimal component, similar to the starting values of the preceding seven hashes.

VII. Comparison Of Blockchain Pseudo-Code Description And Execution

Cryptocurrency's fundamental technology, blockchain, has gained popularity and been effectively applied in a variety of industries,including huge data, artificial intelligence, and virtual environments. The present blockchain system was contrasted conventional way in the WSN system to show how well it performed. Table. 2 contains the blockchain creation pseudo-code.

Table 2: Blockchain creation pseudo-code

Input: The previous block hash value, the current block number, the current clock data, and timestamp
Output: Nonce value and the current block hash value
Method:
Step 1: Set the first four digits of the current block hash value to zeros (set by the system), and then mine the nonce value.
Step 2: $nonce = 0$
Step 3: while (the first four digits of the current block hash value are equal to zero)
{
  Step 3.1: Calculate the current block hash value
  Step 3.2: $nonce = nonce + 1$
}
Step 4: Return nonce value and the current block hash value
end

VIII. Results Analysis

Many farmlands environmental sensing tests of rice growth were carried out using a wireless sensor network and the blockchain integrated technology. The measured data included air temperature and humidity, light illumination, UV light, average wind speed, maximum wind speed, total amount of precipitation per hour, soil temperature and humidity, and sensor battery power curves. Fig. 12 shows the sensor and microcontroller components. Twenty sensor nodes in total were positioned all across the rice fields. In Fig. 13, the sensor information gathered from the distant sensors is shown. The MySQL database system was employed by the suggested system.

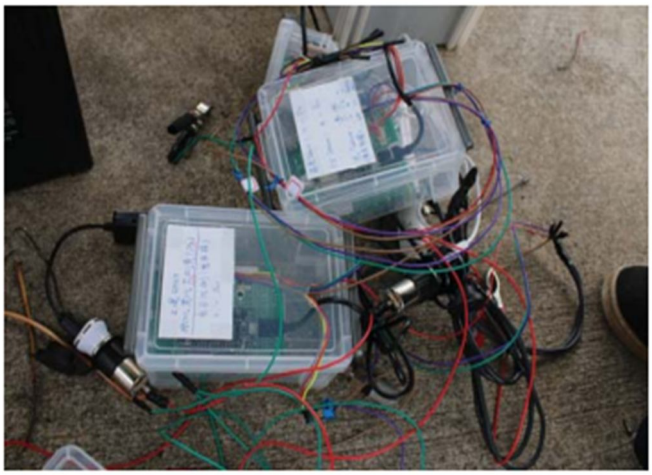

Figure 13: real-world microprocessor and sensing apparatus

The findings revealed that while daily temperature and humidity variations were very minimal, water irrigation had an impact on soil temperature and humidity changes. The time of sunrise caused a change in the UV light. The experiment concentrated on the accurate transmission of remote sensing data. Using the suggested blockchain technology, these sensing data from the fields are packed and processed. There has been no tampering with any of the sensing data.
The experimental farm's numerous environmental characteristics were measured during the experiment. The experimental farm served as the setting for growing rice. From February through August, a little over half a year,

was used to measure the crops. Sunlight, UV light, wind speed, soil temperature, soil moisture content, and other characteristics were among the measured parameters.

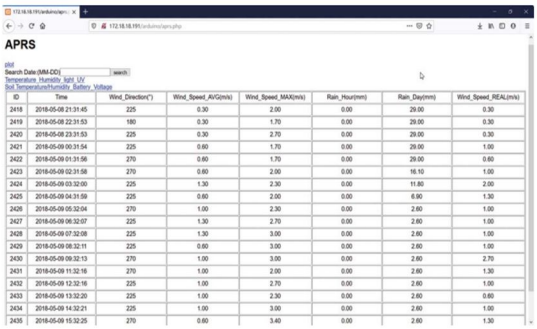

Figure 13: The sensor data obtained from remote sensors

IX. Conclusion

The following issues must be further considered when implementing blockchain into WSNs: the issue with blockchain data transmission lag and issues caused by the growth in measurement data volume.
Processing cryptography and a common key decryption are required to link a blockchain. Additionally, verification of the link's sooner and later sequence is necessary in order to communicate data on a brand-new blockchain.In order to accomplish instantaneous data updating and storage, a number of issues must be overcome. When employing blockchain technology, the hash function and key for encryption computation are required. However, as data volume expands, calculation time also does so, lowering the efficiency of the data transport. Therefore, processing data will require more time when large-scale calculations are involved. The aforementioned issues can be resolved using techniques like the restarting function of blockchain, which will continually update the transfer of data to the current result. One further way to get around the problems listed above is to use a control system and a simplified hash functions . Additionally, symmetric encryption can be used instead of asymmetric system encryption to streamline blockchain security.

References

[1] S.Y.Wang, et at., “Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation,” in 2018 Int. Symp. on Computer, Consumer and Control, Taichung, Taiwan, pp. 149–152, 2018
[2] D. Puthal, et at., “The blockchain as a decentralized security framework , IEEE Consumer Electronics Magazine, vol. 7, no. 2, pp. 18– 21, 2018.
[3] K. Fan, et at.,“Blockchain-based efficient privacy preserving and data sharing scheme of content–centric network in 5G,” IET Communications, vol. 12, no. 12, pp. 527– 532, 2018.
[4] W. Yin, et at., “An anti-quantum transaction authentication approach in blockchain,” IEEE Access, vol. 6, pp. 5393–5401, 2018.
[5] L. Thomas, et at.,“Automation of the supplier role in the GB power system using blockchain-based smart contracts,” CIRED Open Access Proceedings Journal, vol. 2017, no. 1, pp. 2619–2623, 2017.
[6] A. Anjum, et at.,“Blockchain standards for compliance and trust,” IEEE Cloud Computing, vol. 4, no. 4, pp. 84–90, 2017.
[7] J. Gao, et al., “Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid,” IEEE Access, vol. 6, pp. 9917–9925, 2018
[8] A. A. Moldovyan, et at., “Randomized pseudo– probabilistic encryption algorithms,” in 2017 XX IEEE Int. Conf. on Soft Computing and Measurements, St. Petersburg, Russia, pp. 14–17, 2017.
[9] Islam, et at., “Blockchain based secure data handover scheme in non-orthogonal multiple access,” in 2018 4th Int. Conf. on Wireless and Telematics, Bali, Indonesia, pp. 1–5, 2018
[10] J. Gu, B. Sun, et al., “Consortium blockchain-based malware detection in mobile devices,” IEEE Access, vol. 6, pp. 12118–12128, 2018.