IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 10, 2021, accepted May 4, 2021, date of publication May 13, 2021, date of current version May 21, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3079708

Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks

SUNG-JUNG HSIAO[1] AND WEN-TSAI SUNG[2], (Member, IEEE)
[1]Department of Information Technology, Takming University of Science and Technology, Taipei 11451, Taiwan
[2]Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung 41170, Taiwan

Corresponding author: Wen-Tsai Sung (songchen@ncut.edu.tw)

This work was supported in part by the Department of Electrical Engineering, National Chin-Yi University of Technology, and in part by the Takming University of Science and Technology, Taiwan.

ABSTRACT The proposed approach uses blockchain-based technology to strengthen the data security of wireless sensor networks (WSNs). This paper integrates blockchain-based technology with data transfer to establish an extremely secure WSNs structure. The present wireless network is built on the architecture of the Internet of Things (IoT) and employs a blockchain-based method to make the reliability of data transmission strong. In this proposed research, many small-area wireless sensor networks establish the entire WSNs structure, and every small-area wireless sensor network has a primary data collection node called a ''mobile database.'' The ''mobile database'' node of this study uses embedded microcontrollers with an operating system, such as Raspberry Pi and Arduino Yun. This block contains the sensor data collected by itself and the hash value of the previous block. Then the hash value of its own block, which is also part of the hash calculation of the next block, was calculated through the mining calculation program. Any block in the proposed method includes the encrypted hash-value of the previous block, the current timestamp, and the transaction data. In our research content, the transaction data is represented as wireless network sensing data. Basically, the system employs the hash function for calculation using the Merkel-tree algorithm. Such programming makes the block with blockchain-based technology difficult to tamper with content. This study approach revises the blockchain-based transaction ledger to become a sensor data record. Therefore, the proposed system gathers and analyzes sensor data for more reliability in the wireless sensing network structure. Furthermore, the innovative system with blockchain-based technology can treat a private cloud-end. This paper also carries on to visualize the uploaded sensing data by the sensors and draws corresponding charts based on big data analysis. The wireless network architecture proposed in this paper is built on embedded devices, making it easy for the system to build a web server. Using Python or JavaScript programming language in the web environment is relatively more convenient for data visualization and data analysis. Finally, this study uses traditional methods and innovative methods to compare data transmission. When the system uses innovative methods with blockchain-based technology, it is almost impossible for any operator to tamper with the data transmitted by the sensor.

INDEX TERMS Blockchain, mobile database, embedded system, mobile web server, big data analysis, sensor.

I. INTRODUCTION

The application of blockchain technology in traditional wireless sensor networks is an innovative research method. This research is based on the improvement in [1] with additional detailed extensions, and more experimental outcomes are discussed [2]. When a blockchain-based method is integrated with a web service, it is a support blockchain-based web page system [3], [4]. The advantage of blockchain is decentralization, which means that data do not rely on a single server. Dependency on a single server needs the sensor data to be assembled and processed in one place. Utilizing a blockchain-based method for filing distribution minimizes hazards associated with the data repository [5]. This research proposes a blockchain-based method integrated into the WSNs structure. The blockchain-based approach has been shown to be reliable and has the potential to become the IoT innovative technique [6], [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Yunchuan Sun.

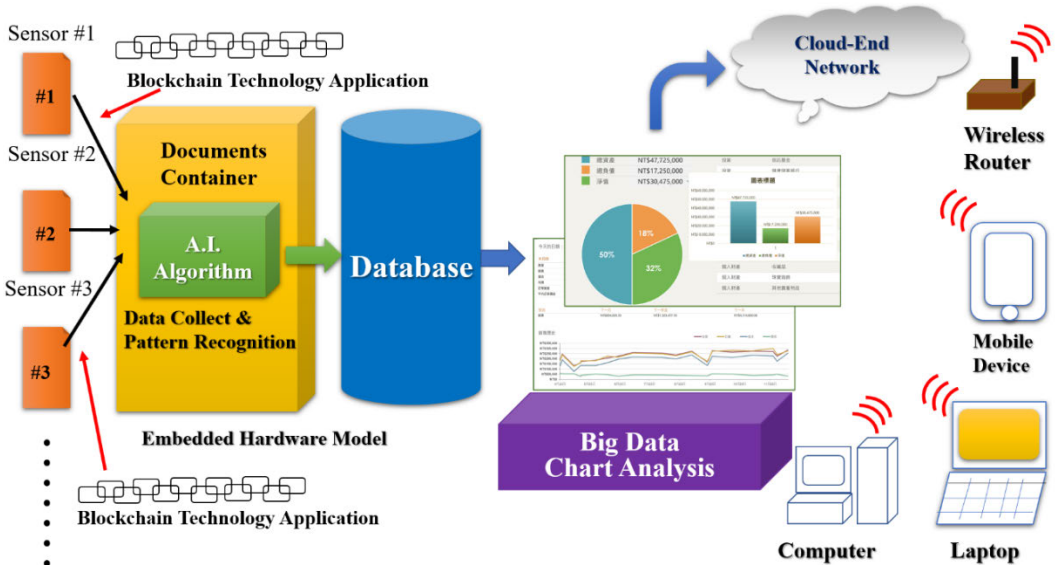


FIGURE 1. Proposed wireless sensor network (WSN) with the blockchain approach.

TABLE 1. The list of symbols and notations used in this paper.

Symbol	Description
$\mathbf{X}(k)$	Air detection point vector
$\omega(k)$	Sequence of independent white noise
A = diag $(a_1 a_2 \cdots a_q)$	Coefficient matrix
Y(k)	Measurement data vector
C = diag $(c_1 c_2 \cdots c_r)$	Observation matrix
K(k)	The filter gain value
$\hat{x}(k)$	The filter estimation value
P(k)	The filter covariance value
$g(z)$	Take the activation function of the hidden unit as the sigmoid function
x_{ni}	The implicit output
W	The variable W represents the weight
θ_j	Threshold value
η	The learning rate
α	The inertia term constant
$\rho(e)$	The Hampel function
$\boldsymbol{\Psi}$(e)	Derivative of the Hampel function

The complete system structure of this study is presented in Fig. 1. The hardware devices on the left are sensors for specifications such as temperature, humidity, and air quality. The research uses various microcontroller-device models for environment-data measurement and related artificial intelligence (AI) algorithms for fundamental data sorting [8].

After fundamental sorting, the data are stored in the database system with cloud-end connection according to their types. The method also executes data to study and thereafter maps the data into real-time webpage pictures utilizing the Python and JavaScript programming language. Next, the proposed system can supply the graphical analysis by the sensor's data. The proposed system can simultaneously allow a remote operator to login into the system to view these results. The data of these sensors are accessed by internet applications of browser; therefore, this method will not be restricted to any mobile hardware operating system. So long as the mobile device is provided with a browser application, the remote operator can handily login to the system and watch the sensor data and graphical analysis [9], [10].

This study employs many of the advantages of blockchain. The most significant point is that decentralized and sent messages are not easy to be tampered with. As a result of the use of distributed accounting and storage, there is no issue of centralized device or administration organization, the rights and responsibilities of any node are matched, and the blocks data in the research are together maintained by the nodes with encrypting functions [11], [12]. When the sensor data is confirmed and added to the block of the proposed blockchain-based method, it is stored continually [13]–[15]. When the hackers can control more than 51% of the nodes at the same time, it affects the operation of the blockchain-based system. Otherwise, modifying the database on a single node has no effect, so the blockchain data is very stable and reliable. Therefore, the data of the sensor of the proposed approach based on blockchain technology is complete at anytime, anywhere [16]–[19].

II. BLOCKCHAIN STRUCTURE AND RELATED RESEARCH WORK

The idiographic characteristic of blockchain-based technology is the employment of peer-to-peer (P2P) network structure to carry out decentralization. The initial blockchain

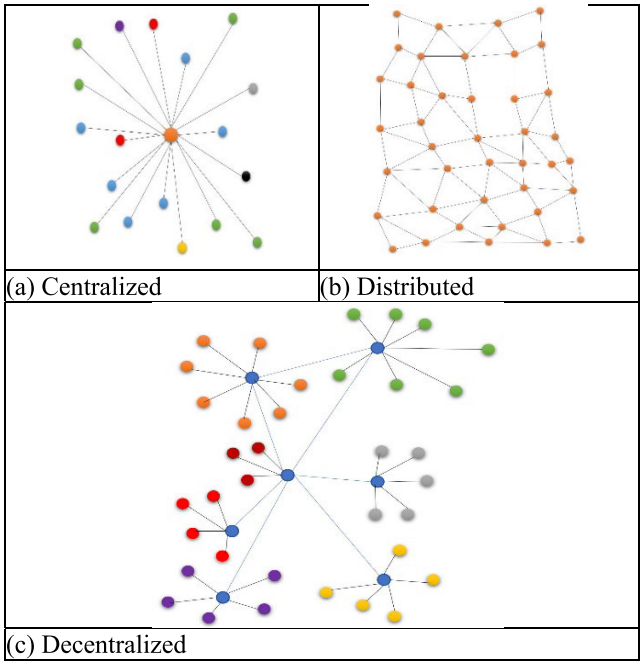


FIGURE 2. Three types of software network protocols.

technology based on P2P networking has improved the decentralized network structure [20], [21]. A lot of present studies use the discourse ''application'' for its relation with software programming. A programming application is a software used to delimit a goal. At present, millions of software applications are in employment, most of these follow the centralized server-client model. While some network types are distributed, a few innovative network structures are decentralized. Figure 2 illustrates three software network types [22], [23].

The centralized system, currently the most popular network software application model, directly controls the operation of each unit and processes the signal transmission from each center. All individual nodes depend directly on the rights management of the central point, and the entire network system sends and receives information according to the rights. The P2P network is a distributed network system architecture. Many file sharing and live video services on the internet implement P2P network protocols, such as the BitTorrent file downloading the application. Blockchain, which became functional after BitTorrent, also implements the P2P network protocol. In this network protocol, each node has the same status and does not belong to a central control position or plays the role of a transaction intermediary. Each node in the network serves as both the server and client and the nodes can choose to join or exit the network any time and to run either some functions or all functions simultaneously. The greater the number of nodes, the stronger the computing power of the whole system, the higher the data security, and the stronger the damage resistance. Bitcoin, a familiar technology, also uses the P2P network protocol. Accustomed transactions on both the client and server sides depend on credible central financial institutions serving as a medium, and any transaction by this centralized organization is written down and supervised. By contrast, Bitcoin uses the P2P network protocol, and thus, businesses can occur directly between users without any medium. References [24], [25].

The decentralized network is characterized by the following features: no node is indicated by other nodes and belongs to the key center in the whole network, the rights and, obligations between all nodes are equal, and if a node in any network stops working or exits, the overall operation of the system is not affected, thus making the network very robust. Decentralization reduces the dependence on centers or key nodes. Currently, most of the systems and services on the internet, such as Facebook, Twitter, and Google, adopt the centralized protocol; however, the internal system architecture and network of these services use a distributed network as the bottom layer, which improves the computing power and data reliability and shortens the service response time. This implies that a system can have a combination of centralized and distributed networks. However, for the user, the data, resources, management rights, and other aspects of the system are concentrated in the service company. The disadvantage of this type of networking is that as the number of users increases, the company's centrally managed infrastructure, servers, and networks all increase. Importantly, in the event of a failure, the rights of all users are affected. In addition, if the servers of these companies are inadvertently compromised, the data stored in the database can be tampered with or stolen; importantly, the companies have absolute ''manipulation rights'' for all user data [26]. The decentralized network has no central server feature. When a decentralized application (DApp) is released on the decentralized network, it cannot be withdrawn or stopped. The data in the DApp exists in all nodes, and each node is independent and unaffected. When any node stops working or exits the network, the overall network still operates. A number of DApps are built on decentralized noncritical centralized networking systems. Decentralized autonomous organizations (DAOs) are approximately the same in structure and nature as decentralized organizations (DOs). DAOs use AI for decision-making and maintenance, with no human intervention, and are therefore similar to fully automatic robots. When all the programs of a DAO are set, it starts working according to the established rules. Furthermore, during its operation, it can also be self-maintained and upgraded depending on the actual situation, thus perfecting and adapting to the operating environment through continuous self-renewal. Therefore, this study proposes a new blockchain architecture system using a hybrid of P2P and decentralized networks.

A complete blockchain system contains a number of technologies, including data blocks for storing data and digital signatures, timestamps, P2P network architecture, maintenance system algorithms, data mining workloads, proof rules, anonymous transmission data mechanisms, unspent transaction output (UTXO), Merkle tree, and other related technical concepts. Through these technologies, the blockchain creates

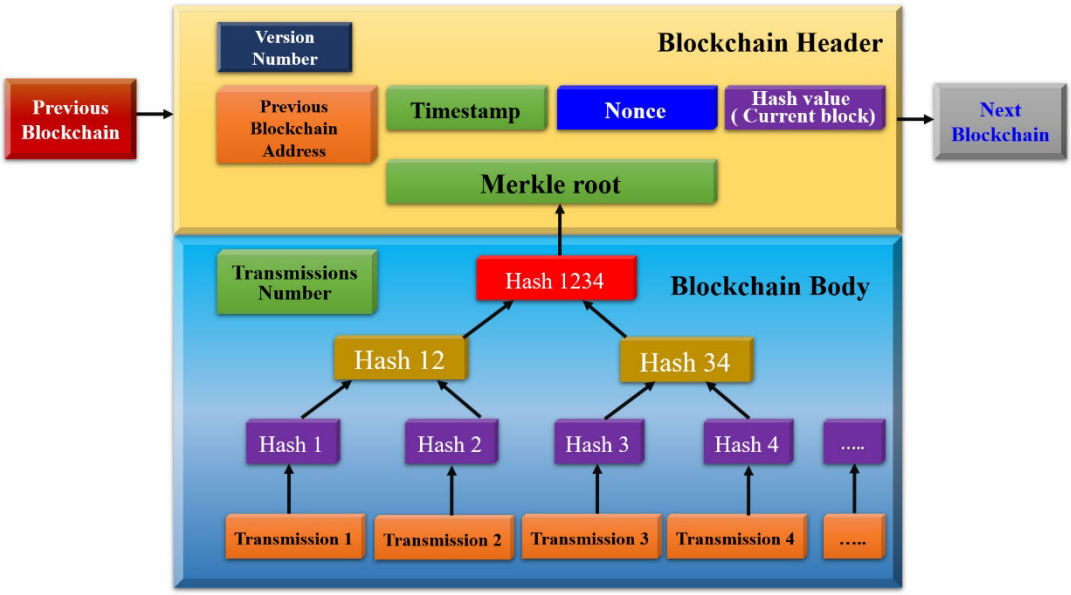


FIGURE 3. Structure of blockchain.

an inexhaustible engine on a noncentralized network and provides a continuous stream of blockchain networks for functions such as transmission, verification, and linking [27].

The method proposed that the blockchain transaction record becomes a sensor data record. The system generates a block every 10 minutes in the blockchain system, with each data block generally containing two parts, a header, and a body. The block header packages the present block number, the previous block hash-value, the current timestamp, the random-value (nonce), the hash value of the current block, and the Merkle tree.

The block content mainly contains the sensor data. In the research system, each part of sensor data is permanently recorded in the data block and can be queried by the operator. The Merkle tree in the block is digitally signed for each part of the sensor data, thus ensuring that every part of the sensor data obtained is no duplicate. The system getting all sensor data are processed by the Merkle-tree hash algorithm to generate Merkle-root values in the header-part of the block [28]. Figure 3 presents the blockchain-based architecture.

The most delegate characteristic of the blockchain structure is that the timestamp and the sensor data cannot be tampered with. The timestamp is a digitized postmark and an indispensable security mechanism in this information age. The timestamp is used for any electronic file or transaction to provide accurate proof of time and verification of any document modification or transaction content since the time of stamping. The electronic timestamp associates a message or document with a specific time that serves as evidence for the time the document was created. Once a timestamp is created, even if the certificate is expired or canceled, it still has the characteristic of nonrepudiation.

The distributed network architecture still has a central node concept and may have several concepts of central nodes. Each central node has other child node links. The decentralized network architecture is a concept without any single central node. Every node is equal, and the content is the same. Our system integrates these two network architectures. For data consistency, in addition to the decentralized network architecture, there also exists a distributed network architecture that increases the efficiency of the sensor's data transmission.

Xie et. al mentioned data security measures in a wireless sensor network environment [29]. Research about security attacks and countermeasures in surveillance wireless sensor networks was proposed by Sert *et.al.* [30]. Sharma et. al proposed sensor fusion for distributed detection of mobile intruders in surveillance wireless sensor networks environment [31]. Likewise, Yazici et.al also proposed a fusion-based framework for wireless multimedia sensor networks in surveillance applications [32].

III. CRYPTOGRAPHY TECHNOLOGY APPLICATION

The blocks in the blockchain system, such as bookkeeping, record the transaction information of all blockchains, and the blockchain revenue and expenditure of each blockchain user is permanently embedded in the data block for other queries. The transaction data in these data blocks are stored in the user nodes of each blockchain user; these nodes together form a blockchain and the distributed database system. The destruction of the data in any one node does not affect the normal operation of the entire database because the entire database is maintained by other healthy nodes [33], [34].

Hash functions also have important applications in blockchain systems. The data in the blockchain are not just the original data or transaction records but also their hash

function values; that is, the original data are encoded into a specific length in the form of numbers, and a string consisting of letters and numbers is recorded in the blockchain. The hash function has the following advantages for storing blockchain data.

1) The hash algorithm processing data is basically one-way, and the system cannot reversely compute the primeval data input value from the output result value.

2) A hash function, such as the secure hash algorithm 256 (SHA256), with each block containing 512 bytes, the Merkle-Damgard construction inputs the primeval data (256 bytes), and the first block to generate 256 bytes. In addition, the Merkle-Damgard transformation is performed for the primeval data and the next block; this is reiterated until the last block. The ultimate result is a 256-byte hash-value.

3) The system uses two different input values as an example (the difference between the two values is only one byte). When the output value of the two input values is calculated through the hash function, the result of the output value is very different. Generally, when two SHA256 hash functions are used to calculate original data of different lengths, the output lengths are the same. The above content is a function that compresses messages of any length into a message digest of a fixed length.

In summary, the hash function is a key technology in the blockchain system that provides a number of convenient encryption conditions for the blockchain system. In addition to the hash algorithm, an asymmetric encryption algorithm (e.g., the elliptic curve encryption algorithm) is used for encrypting transactions in the blockchain. This algorithm is based on mathematically related keys; that is, the data information encrypted using a key can be decrypted by using only a specific related key. A pair of keys comprises a public key and an undisclosed or private key. For example, a public key is like a bank account, while a private key is like the password for that account or the signature of the account owner. A transaction on the blockchain can be considered efficient when the transaction's private key signature is a valid digital signature, which can be verified using the transaction initiator's public key. The public key can be determined from the private key through the algorithm, but the private key cannot be derived from the public key. Figure 4 presents the blockchain asymmetric encryption technology. The elliptic curve cryptography (ECC) algorithm with representative asymmetric encryption technology uses in the blockchain-based system. The blockchain-based system receives a 256-bit random value as a private key from an operating system. The total number of private keys is 2^{256}, which makes it difficult to crack the key [35], [36].

The three commonly used cryptographic techniques are symmetric key encryption, asymmetric key encryption, and hash algorithms. Usually, the blockchain method is based on the hash algorithm as its core technology. There are several methods for protecting the integrity of files, one of which is to use fingerprints. If the user needs to ensure that the content of his document cannot be changed, the user can stamp his

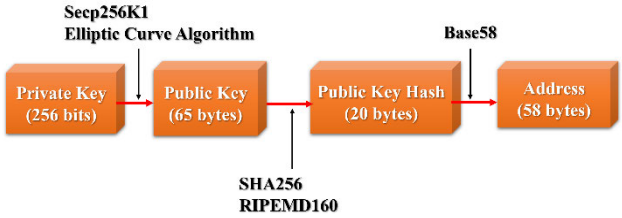


FIGURE 4. The blockchain asymmetric encryption technology.

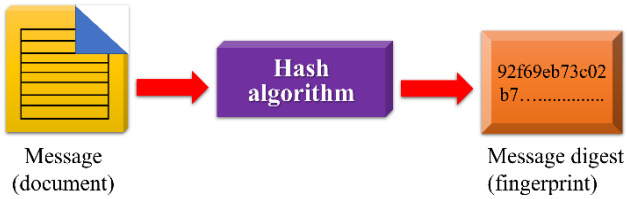


FIGURE 5. The message and digest.

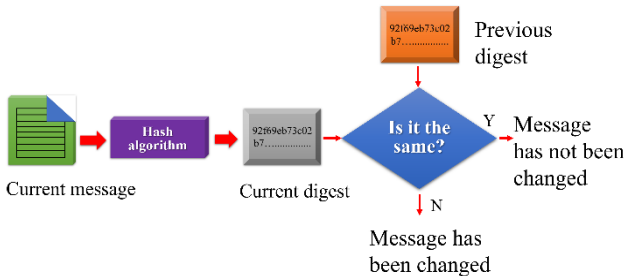


FIGURE 6. A schematic of file check integrity.

fingerprints at the bottom of the document, and others will not be able to modify the content of the document or create a fake document because people's fingerprints cannot be forged. To ensure that the document has not been changed, the user can compare the fingerprint on the document with the fingerprint on the file. If the comparison results are different, it means that this document is different [37], [38].

The system usually treats the input information as a document file. When the message is calculated using the hash function, it becomes a unique message digest, which can be regarded as another kind of fingerprint, because fingerprints are also unique. Figure 5 shows the message, password hash function, and message digest.

Even though these messages are regarded as documents, and message digests are regarded as fingerprints, there are some divergences. The most important thing is that the message digests must be protected from modifiers. When the system is to verify whether the message digest has been changed, the system can once again input the original message content through the calculation of the hash function. The final message digest can be compared with the previous message digest. Figure 6 shows the schematic of file check integrity.

A cryptographic hash function must meet three criteria: preimage resistance, second preimage resistance, and collision resistance, as shown in Figure 7.

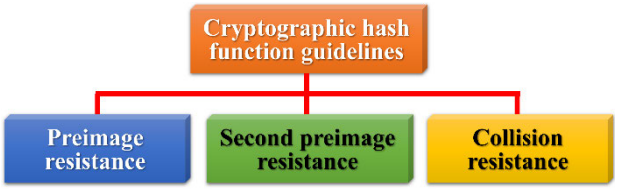


FIGURE 7. Basic principles of a typical cryptographic hash function.

A. PREIMAGE RESISTANCE

The cryptographic hash function must be capable of preimage resistance. Given a hash function h and $y = h(M)$, it is difficult for the system to find information, in this case, M', such that $y = h(M')$.

B. SECOND PREIMAGE RESISTANCE

The system ensures that the information cannot be easily forged. That is, given a specific message and its digest, it is impossible (or at least very difficult) to create another message with the same digest. From the perspective of calculation, it is impossible to find any secondary input value that has the same output as the specific input value. For example, at a given x, it makes it difficult to satisfy $h(x) = h(x')$ Secondary image $x' \neq x$.

C. COLLISION RESISTANCE

Ensure that no other system can find two messages that can hash together the same digest. This attack means that other systems can create two messages (without limits) and hash the same digest. Of course, this is a situation that does not want to be attacked.

The random oracle model, proposed by Bellare and Rogaway in 1993, is an ideal mathematical model for hash functions. A function based on this model behaves as follows:

a. When a new message of any length is sent, the oracle creates and responds with a fixed-length message digest composed of random 0s and ls, and the oracle records this message and the message digest.

b. When a message is sent and its message digest exists, the oracle only responds to the record digest.

c. The digest of a new message must have nothing to do with all previous digests, which means that Oracle cannot use a formula or algorithm to calculate the digest.

Assume an oracle has a table and a fair coin. The table has two fields. The first field shows the messages that the oracle has sent a digest, and the second field lists the digest created for these messages. The digest is assumed to be 16 bits regardless of the size of the message. Table 2 shows an example of this kind of table, where the message and the message digest are expressed in hexadecimal form. In the table, Oracle has created three digests.

This oracle can be thought of as a similar automatic dialogue device. When an oracle receives a query message, it truthfully responds to related things. For example, when a random oracle receives an inquiry message, it truthfully

TABLE 2. Oracle response to the table after the first three digests.

Message	Message digest
4523AB1352CDEF45126	13AB
723BAE38F2AB3457AC	02CA
AB45CD1048765412AAAB6662BE	A38B

TABLE 3. The table after the fourth digest issued by oracle.

Message	Message digest
4523AB13 52CDEF4 5126	13AB
723BAE38F2AB3457AC	02CA
AB1234CD8765BDAD	DCB1
AB45CD1048765412AAAB6662BE	A38B

responds with a random number. It is assumed that the digest is 16 bits regardless of the size of the message. Table 1 shows an example of such a table, in which the message and the message digest are expressed in hexadecimal. In Table 2, Oracle created three digests. These message digests are randomly generated. According to another example of the content of the paper, we can also regard the message digest as the positive and negative situation of tossing coins (positive=1=H, negative=0=L). Assuming 13AB (16) = 0001001110101011(2), we can regard it as the result of tossing coins 16 times as LLLHLLHHHLHLHLHH.

We now assume two situations to occur:

a. Given the message ABl234CD8765BDAD to request the oracle to calculate the digest, oracle checks its table and finds that there is no such message in the table, so Oracle flips a coin 16 times.

If the result is HHTHHHTTHTHHTTTH, the letter H represents the front side, and the letter T represents the backside. Oracle interprets H as bit 1 and T as bit 0 and responds with binary 1101110010110001 or hexadecimal DCB1 as the message digest of the message. Then, this message and message digest are added to Table 3.

b. Given the message 4523AB1352CDEF45126, to request oracle to calculate the digest, oracle checked its table and found a digest of the message in the table (the first column). Oracle responded only to the corresponding digest (13AB).

IV. DECENTRALIZED SHARED TRANSMISSION DATA STRUCTURE

Fabric is an implementation of blockchain technology and a distributed shared ledger technology based on transaction calls and digital events. Compared with other blockchain technologies, Fabric uses a modular architecture to support the development of pluggable components. In this research, we studied the book as a record of data transmitted by the sensor [39], [40].

The aggregation of ordering service nodes in the network forms a consensus service, which can be considered an organization of delivery assurance communication. The consensus service provides a shared communication channel for the client and peer nodes and a broadcast service for messages

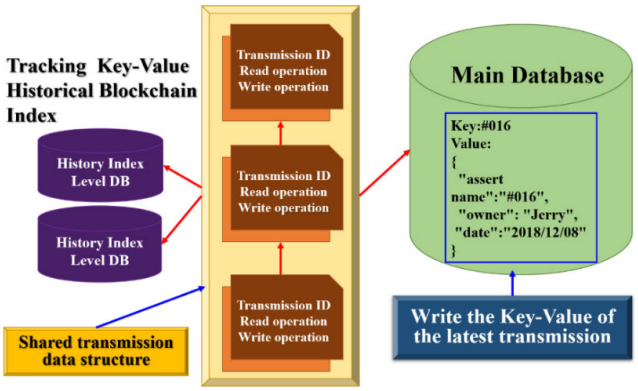


FIGURE 8. The market decentralized shared transmission data structure.

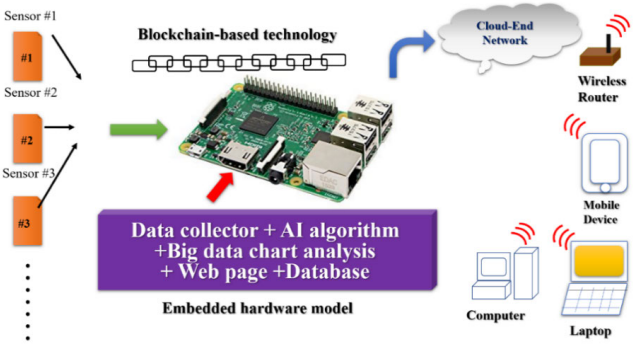


FIGURE 9. Raspberry Pi was used to integrate the data collector, database storage, and web server services.

containing transmitted data. After the client connects to the channel, the message can be transmitted to all peer nodes through the consensus service broadcast message. The consensus service in Fabric ensures that message communication is serialized and reliable. In other words, the consensus service outputs the same message to all peer nodes connected to the channel, keeping the logical order of the outputs the same [41], [42].

Based on the underlying structure of blockchain technology, the method of blockchain can be defined as a shared ledger technology. A ledger is a core component of the blockchain, in which all historical transactions and status change records are stored. In Fabric, each channel corresponds to a shared ledger, and each peer node connected to the shared ledger can participate in the network and view the ledger information. The information in the ledger is publicly shared, and a copy of the ledger is maintained on each peer node. Figure 8 shows the decentralized shared transmission data structure. Figure 9 uses a Raspberry Pi to integrate the data collector, database storage, and web server services.

V. USING SYSTEM FUSION ALGORITHM

The sensing data measured by multi-point sensors need to be integrated, which is usually called the ''fusion method''. When the system measures some data from different sensors, the system must perform data fusion processing. Usually, the system performs automatic analysis and comprehensive information processing according to customized standards. Such results make remote sensing data easy to observe. Information fusion technology is used in the air environment monitoring system. The calculation of the system can process the sensing data provided by multiple sensors at multiple levels. Such results will have many benefits. For example, multi-sensor data fusion has better accuracy in sensing data than single-sensor data fusion, and the data level of multi-sensor data fusion is also wider. The information collected by a group of similar sensors is redundant, while the appropriate fusion of such redundant information can reduce the uncertainty of the information. The information collected by various types of environment-sensors has obvious complementarity. After proper processing, this complementarity can compensate for the uncertainty of a single sensor and the limitations of the measurement range. Multiple sensors can increase the reliability of the system. For example, when one or several sensors fail, the system can still work normally.

For example, when the system contains many air environment detection sensors, and these sensors are widely distributed. In the process of system transmission and calculation, to reduce the burden of communication lines and reduce the calculation amount of the fusion center, the system is divided into many subsystems to perform analysis and calculation. Then the analysis results are combined to obtain the fusion output of the entire system. In simple terms, the system is to perform fusion calculations on the two scattered parts, and finally integrate them into a complete output result, as shown in Figure 10.

This data fusion method allocates sensors to air detection points according to design requirements and uploads data after each air detection point has completed feature extraction. The relay station of the system performs partial fusion; the total detection station performs global fusion and generates auxiliary decision-making.

A. LOCAL FUSION ALGORITHM

In the example of this paper, the number of system air detection points is not too much, that is, the dimensionality of the subsystem is not high, so the local fusion method can be performed by the classic vector Kalman filter algorithm. Assuming that there is a total of q air detection points, the signals from each air detection point form a q-dimensional vector $\mathbf{X}(k) = [x_1(k)\, x_2(k) \cdots x_q(k)]^T$. Process noise is a sequence of independent white noise $\omega(k) = [\omega_1(k)\omega_2(k) \cdots \omega_q(k)]^T$; then, the mathematical model of the multidimensional random signal can be expressed as

$$\mathbf{X}(k) = A\mathbf{X}(k-1) + \omega(k-1) \tag{1}$$

where A= diag $(a_1 a_2 \cdots a_q)$ is the coefficient matrix.

Running optimal filter, the q-dimensional random signal X(k), the first r components of X(k) (r < q) are measured simultaneously at time k, and an r-dimensional measurement

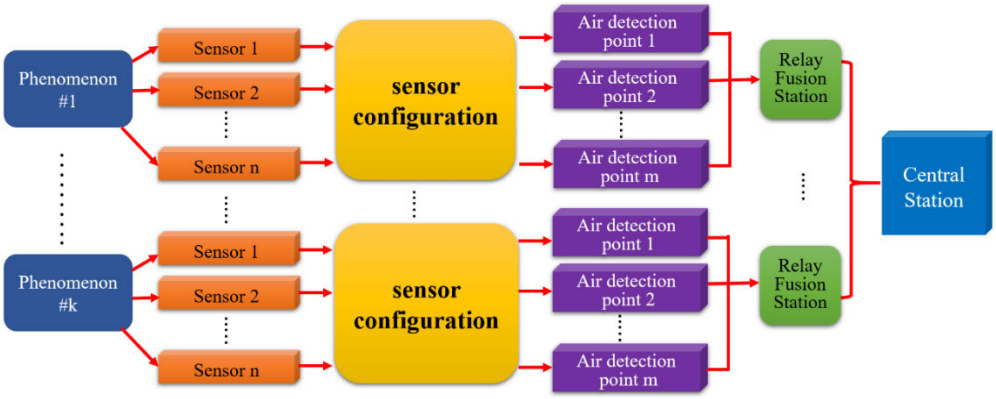


FIGURE 10. The structure of the system fusion model.

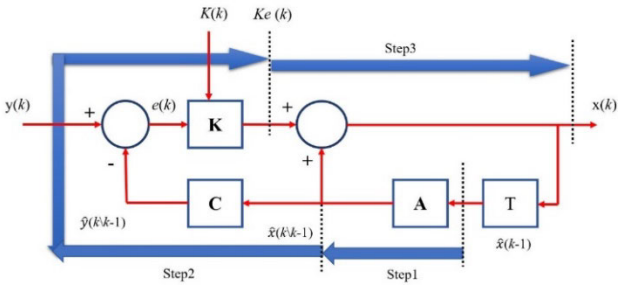


FIGURE 11. The main program of vector Kalman filtering.

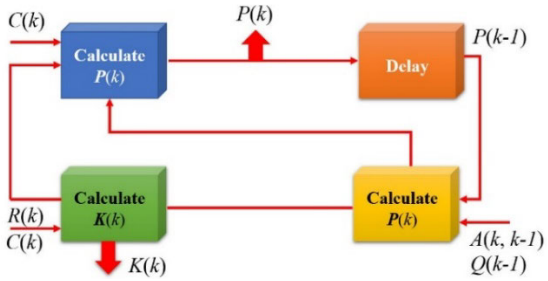


FIGURE 12. The subroutine of the vector Kalman filtering.

data vector Y(k), its mathematical model can be expressed as

$$\mathrm{Y(k)} = \mathrm{CX(k)} + \mathrm{V(k)} \tag{2}$$

where $\mathrm{C} = \mathrm{diag}\,(c_1 c_2 \cdots c_r)$ is the observation matrix,

$\mathrm{V(k)} = [\upsilon_1(k)\upsilon_2(k)\cdots\upsilon_r(k)]$ is an additional measurement noise sequence.

So there is the vector Kalman filter algorithm

$$\hat{x}(k) = \boldsymbol{A}\hat{x}(k-1) + K(k)[\boldsymbol{Y}(k) - \boldsymbol{CA}\hat{x}(k-1)] \tag{3}$$

$$\mathrm{K(k)} = P_1(k)\boldsymbol{C}^T[\boldsymbol{CP_1}(k)\boldsymbol{C}^T + R(k)]^{-1} \tag{4}$$

$$\mathrm{P(k)} = P_1(k) - \mathrm{K(k)}\boldsymbol{C}P_1(k) \tag{5}$$

where (3) is the filter estimation equation, (4) is the filter gain equation, where $P_1\,(k) = \boldsymbol{A}P\,(k-1)\,\boldsymbol{A}^T + \boldsymbol{Q}\,(k-1)$, and (5) is the filter covariance equation.

Generally, the vector Kalman filter with prediction plus rectification uses a recursive method as a typical filter algorithm. When the system employs this feature, it is easy to apply a micro-controller to filter the real-time signal transform. Figure 11 and Figure 12 show the algorithm block diagrams of the main program and the subprogram of the vector Kalman filter, respectively.

B. GLOBAL FUSION ALGORITHM

The fusion station filters and processes these air data by multi-sensors measurement will make known the air environment more precisely. Each relay fusion station uploads these sensing data to the total inspection center station that can be regarded as a system sensor data transfer. Then, the global fusion algorithm uses a forward neural network model, such as the single hidden layer neural network shown in Figure 13.

The output situation of each relay fusion station forms a vector $\mathrm{X(k)} = [x_1(k)x_2(k)\cdots x_n(k)]^T$, as the input group of the neural network, the output group is $\mathrm{Y(k)} = [y_1(k)y_2(k)\cdots y_n(k)]^T$, which depends on actual engineering needs.

The activation function of the hidden unit is taken as the sigmoid function

$$g(\mathrm{z}) = \frac{1}{1+e^{-x}} \tag{6}$$

The implicit output is

$$x_{ni} = g(\sum\nolimits_{j=1}^{N} \omega_{ij}\mathrm{z}_j + \theta_i) \tag{7}$$

Taking the excitation function of the output node as a linear function, the output of the entire network is

$$\mathrm{Y} = \sum\nolimits_{j=1}^{N} \omega_{IJ}^2 x_{ni} = f(x_1, x_2, \cdots, x_n) \tag{8}$$

For training the forward neural network weight matrix, the backpropagation (BP) algorithm is generally used. However, the traditional BP algorithm is essentially a least-squares estimation, robustness is poor and very sensitive to outliers, so this article uses the robust BP (RBP) algorithm.

$$W_{IJ}\,(k+1) = W_{ij}(k) + \eta\delta_j O_I + \alpha[W_{ij}(k) - W_{ij}(k-1)] \tag{9}$$

$$\theta_j\,(k+1) = \theta_j + \eta\delta_j + \alpha[\theta_j(k) - \theta_j(k-1)] \tag{10}$$

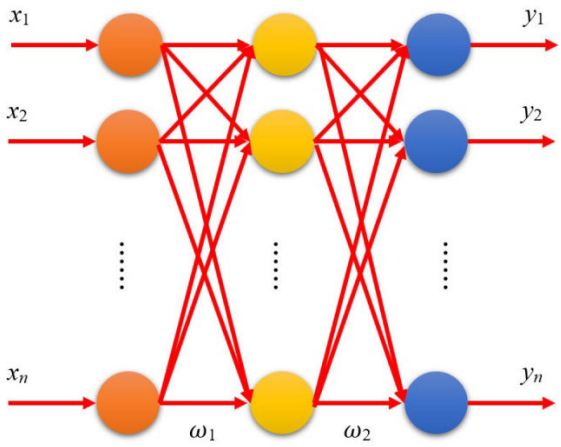


FIGURE 13. The single hidden layer neural network structure.

where η is the learning rate; α is the inertia term constant, $\Psi(e) = \rho'(e)$, $\rho(e)$ is the Hampel function.

$$O_i = f_i(net_i) = 1 + exq(-\sum_j W_{ij}O_j - \theta_i)^{-1} \quad (11)$$

$$\delta_j = O_j(1 - O_j)\varphi(e)(\text{output layer}) \quad (12)$$

$$\delta_j = O_j(1 - O_j)\sum_k \delta_k W_{kj}(\text{hidden layer}) \quad (13)$$

where f(x) is the Sigmoid function.

VI. PLANNING OF BLOCKCHAIN-BASED TECHNOLOGY FOR WSNs

Each block sends data that is not rewritable, and thus, its level of security is extremely high. This security is especially beneficial when applied to the secret WSNs. A new WSN is built utilizing the latest blockchain [13], [14].

Building a WSN is often impeded by the budget or difficulties encountered during operation. The issues usually start from small regions and gradually expand to larger regions. To report these problems, the present important blockchain technique for Bitcoin is the most suitable for this research [15].

Each primary node links to several sensor devices. Furthermore, each of those nodes has a serial number to present the order of blockchain connection. Except gathering its own sensor data, each blockchain gathers measurement data from the nodes of other blocks besides. That is, when a new block is created for each node block, the primary node also obtains identical sensor data.

Consequently, each node maintains sensor data for its own and for other nodes, and no single node is the central node, thus demonstrating the application of decentralization. All the blockchain nodes are linked by the P2P network and with the safest encryption determined based on network cryptography computations conducted by the team.

In addition, renewing functions are increased to the ensemble to permit the blockchain to renew links. The order of making links may not be the same, but the correctness of the measurement data is guaranteed. The initial condition in the system initiates a blockchain reset every 30 minutes. Nevertheless, the team still requires to produce a suitable restart series according to practical analysis. In the condition of fault in any of the block nodes during the testing phase, or if new block nodes are established, the automatic mechanism of the system polishes the impeding node or adds the new nodes. This is controlled by the approach program using AI machine learning to manage the blockchain link and improve the defects of the mining approaches at first utilized by bitcoin. The linking approach of blockchain nodes on the WSNs is presented in Figure 8.

The node orders labeled in Figure 14 are linked by the asymmetric cryptographic algorithm, which prevents mining time and increases performance efficiency. Each blockchain is linked to a preceding and subsequent opposite side as the system lets each newly established block experience encryption and cryptography with keys. Each new block efficiently connects to the former block according to the mechanism established in this system. This characteristic is different from the Bitcoin blockchain approach.

The method proposed in this research improves the security of the block connecting approach by deciding which block to connect first in chronological sequence. The key is still to go by the hash function and password key-related authentication technique before successful connecting. In addition, no efficiency problem involving Bitcoin mining has been met. Figure 15 shows the present blockchain node connection. Each node includes the hash function that is the last block and itself. In effect, hash functions are long strings of words, but they are shown as four single-digit numbers in this figure. Figure 16 presents an order of blocks with incorrect hash functions; that is to say, the values of the nodes in order are different, which signifies erroneous connecting. When such erroneous connecting is detected, the system directly terminates the connection and transfer of data in that blockchain.

Furthermore, it is ensured that the measurement data for each blockchain node are unanimous. The content in any subblock of the subjected blockchain presents the accurate unanimous measurement content for the entire WSNs. This is the distributed file system (DFS) architecture, which effectively lowers the hazard of data storage. Blockchain applications are new research in WSNs and must be written to the microcontroller utilizing software code, which is different from the structure of traditional WSNs. Besides the advantages of the blockchain, our study also utilizes the Web platform to carry out the system, which reduces the standards of various communication protocols and thus greatly ameliorates efficiency. Every block node has complete sensing data, therefore, data privation caused by node failure is not an issue.

VII. PRIVATE BLOCKCHAIN IMPLEMENTATION

For messages of any length, SHA256 generates a 256-bit hash value, which is called a message digest. This digest is equivalent to an array of 32 bytes length, usually represented by a hexadecimal string of 64 bytes length. The SHA256 algorithm uses 8 initial hash values and 64 hash

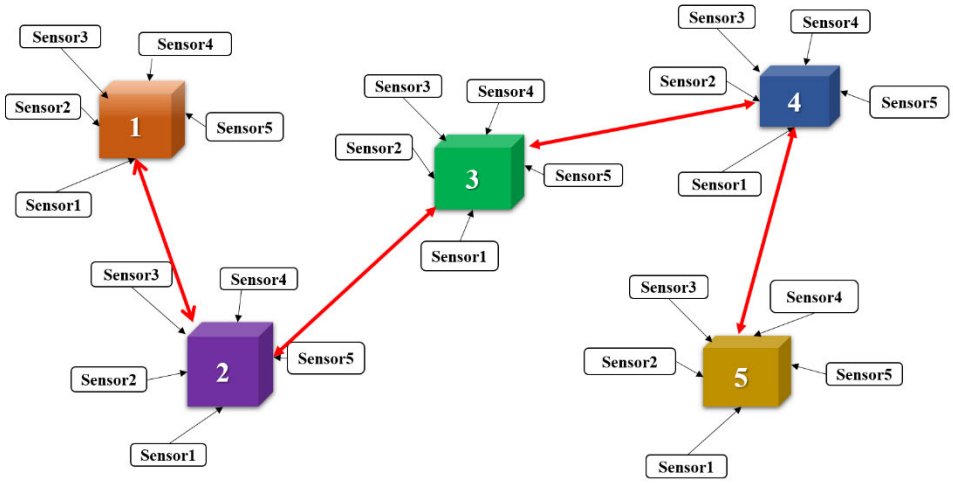


FIGURE 14. Integration of blockchain approach in a WSNs structure.

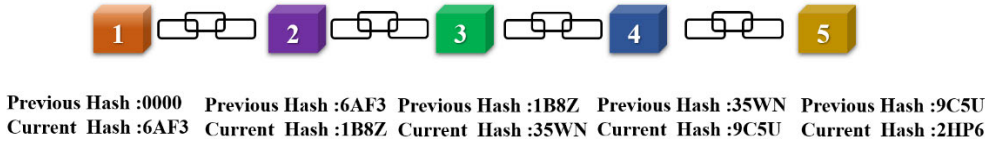


FIGURE 15. Blockchain planning sample for the partial nodes in a normal WSNs.

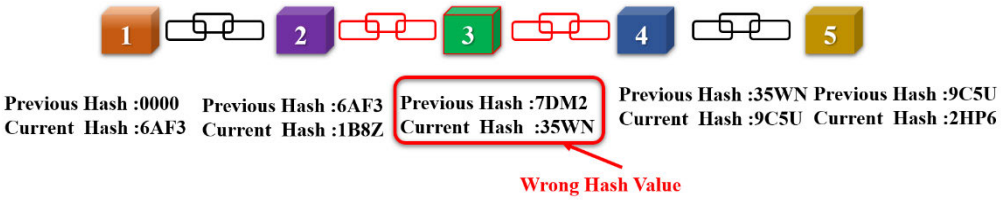


FIGURE 16. Blockchain planning sample for the partial nodes in an abnormal WSNs.

constants. Among them, the initial values of the 8 hashes of the SHA256 algorithm are as follows:

h0:= 0 × 6.09e667
h1:= 0x bb67ae85
h2:= 0 × 3.6ef372
h3:= 0x a54ff53a
h4:= 0 × 510.527f
h5:= 0 × 9.05688c
h6:= 0 × 1.83d9ab
h7: = 0 × 5be0cd19

These initial values are derived from the decimal part of the square root of the first 8 prime numbers (2,3,5,7,11,13,17,19) in natural numbers. For example, the fractional part of $\sqrt{2}$ is approximately 0.414213562373095048 and $0.414213562373095048 \approx 6*16^{-1}+a*16^{-2}+0*16^{-3}+\ldots$. Therefore, the decimal part of the square root of prime number 2 takes the first 32 bits to correspond to $0 \times 6.09e667$. In the SHA256 algorithm, the 64 constants used are shown in Table 4.

Like the initial value of 8 hash-functions, these constants are the first 64 prime numbers of natural numbers (2,3,5,7,11,13,17,19,23,29,31,37,41,43,47, and the decimal part of the cube root of 53,59,61,67,71,73,79,83,89,97...) is taken from the first 32 bits. Steps to implement wireless sensing network blockchain. Each block in this study contains the block number, sensing the data, timestamp, and hash value of the previous block (Figure 17).

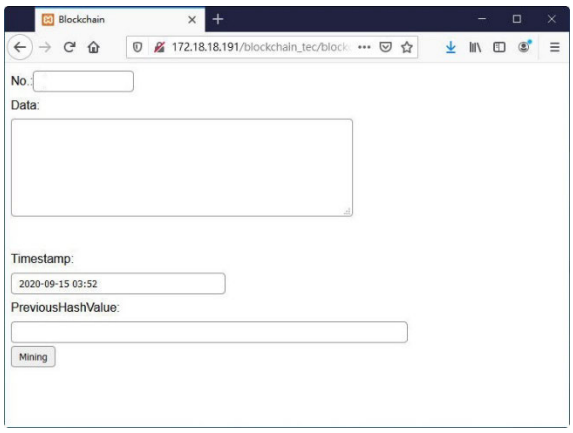


FIGURE 17. Block content unit of the proposed method.

TABLE 4. The 64 constants in the SHA256 algorithm.

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
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

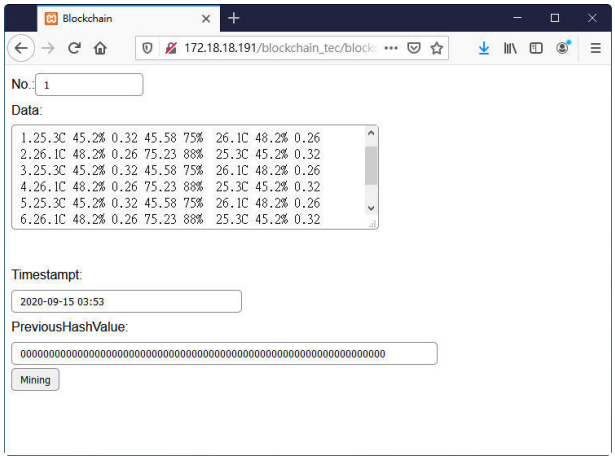


FIGURE 18. The use of each unit's data to calculate the hash value of each block.

Each block is the basic unit of the blockchain. The message content of each block includes the number of the block, a timestamp, measurement data of each sensor, the hash value of the previous block, and the random Nonce value. When the first block of Genesis is generated, the hash value of the previous block is "0".

The first block implementation is created. The proposed method calculates the block number, sensor data, timestamp and the hash value of the previous block, as listed below. The hash value is:

"No." + "Data" + "Timestamp" + "PreviousHashValue",

where the PreviousHashValue value of the first block is 64 "0"s, as shown in Figure 18. In a general situation, a user presses the data mining button, and the system begins to mine the sensor data. The hash-function value of this block is the hash value format designed by our system, and the first four values are "0000". The random nonce value generated by the

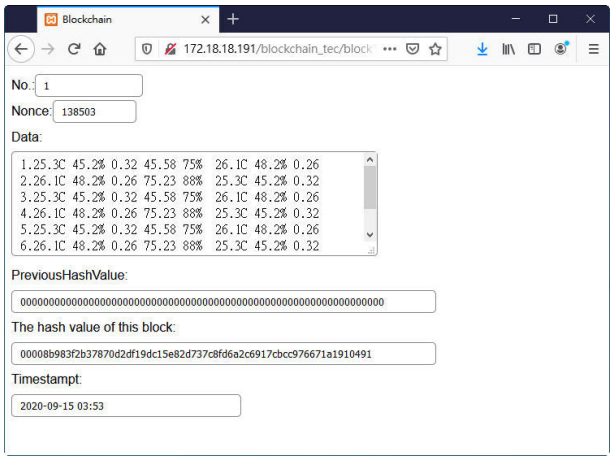


FIGURE 19. The random nonce safety value is calculated through mining technology.

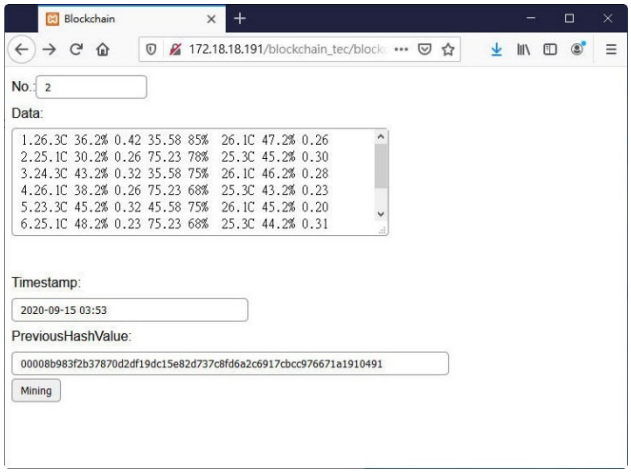


FIGURE 20. The data is filled in to calculate the second block hash value and the nonce value.

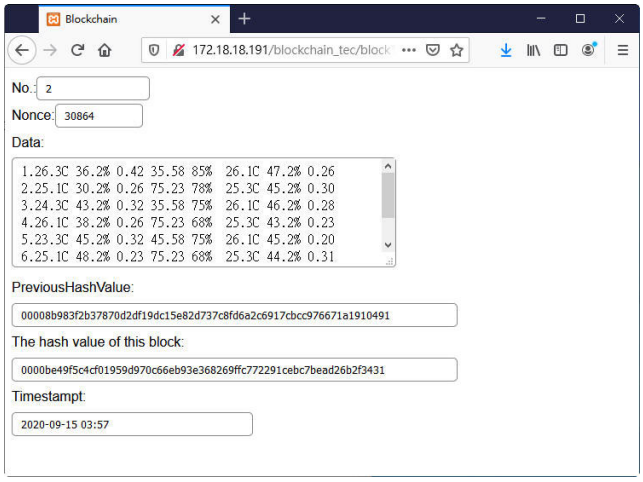


FIGURE 21. Calculation of the hash value and nonce value of block number 2.

hash value of the block we signed is the safe value we mined. If data are tampered with, the system generates different nonce values, as shown in Figure 19. The user continues

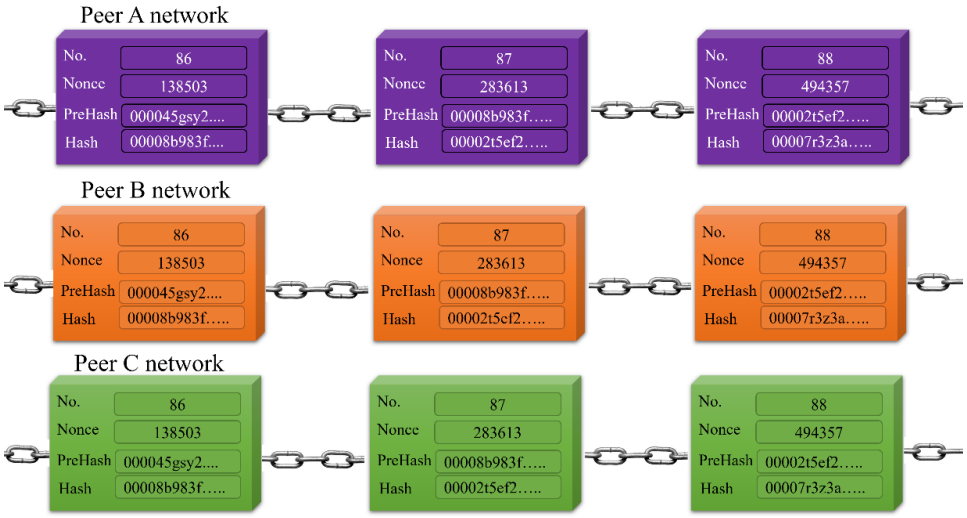


FIGURE 22. Blockchain connection in the normal condition.

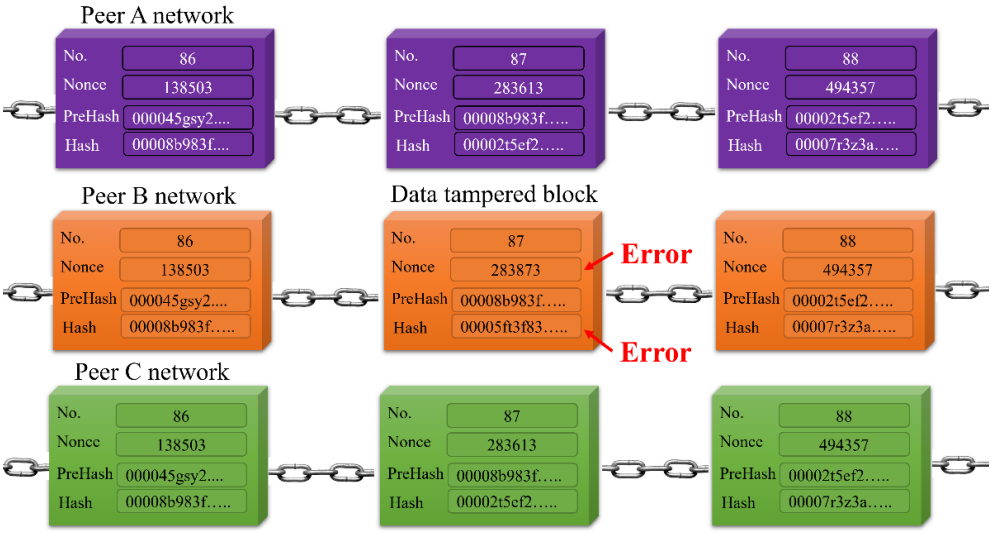


FIGURE 23. The 87th block data after being tampered with.

to compute the hash value and nonce value of the second block. The No. text-box is filled with 2. The text-box of the sensor field is filled with new data, such as the data grid. The timestamp is automatically generated by the system. Next, the hash value of the first block is filled, and then, the mining button of the data is shown to calculate the hash value and the nonce value of the second block. The screen is shown in Figure 20.

The hash value of block number 2 is displayed in the box of the hash value of this block. Currently, the nonce value is ''30864'', as shown in Figure 21.

This implementation example uses a distributed network structure to employ the wireless sensor network of the blockchain. The blockchain-based structure in this study uses a decentralized network structure. Suppose when each block is generated every 30 minutes, then the proposed system will have three peer-to-peer networks at the same time when it is generated from the first blockchain. In the peer network blockchain structure, a block is generated every 30 minutes.

Figure 22 shows the normal connection of the blockchain network. When a block of data is tampered with, the system immediately finds the tampered place. As shown in Figure 23, in the peer B Network, the nonce and hash values of the 87th block are tampered with. When the system compares the peer A and peer C networks, the system finds that the data in the 87th block of the peer B network are different from those of other blocks.

VIII. USING JAVASCRIPT AND NODE.js

At present, the popular blockchain technology is a kind of cryptocurrency application, which is very popular among

```
main.js          main-v2.js          package.json
const SHA256 = require("crypgo-js/sha256");

class Block {
    designer(index, timestamp, data, previousHash = '') {
        this.index = index;
        this.previousHash = previousHash;
        this.timestamp = timestamp;
        this.data = data;
        this.hash = this.computeHash();
    }

    computeHash() {
      return SHA256(this.index + this.previousHash
        + this.timestamp + JSON.stringify(this.data)).toString();
    }
}
```

FIGURE 24. Definition of a block class and writing of a fundamental component element for every block node.

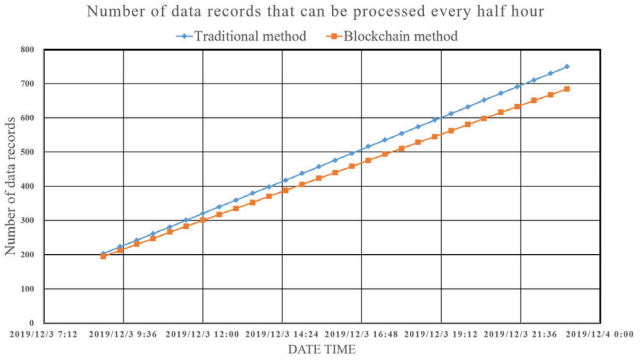


FIGURE 25. A comparison of traditional methods and blockchain methods.

researchers and is specifically used in various information fields, such as VR, AI, and big data.

For a better understanding and perception of this technology, let us consider Google Earth as an analogous example. When Ajax, which is not a new technology, is connected with other technologies, something exceptional, such as Google Earth, can be established. When the blockchain approach is combined with other devices, such as encryption and deciphering technologies and P2P networking, bitcoin emerges.

The coding presented in Figure 24 shows a definition of a block class and the writing of the fundamental component element for every block node. Designer symbols such as the ''index'' component represent the index sequence for linking, ''previousHash'' represents the hash functional value for the previous node, ''timestamp'' represents the record for the timestamp, ''data'' represents the location of data storage, and ''hash'' stands for the subroutine that calls for the calculation of the hash function.

After defining the block data part style, the connections for blockchains are carried out. Starting from nothing, the initial genesis block is established, and corresponding programs are performed for each step taken.

When the latest block is established, the system must compute the length of the blockchain as programmed. This research proposes a contrast between the blockchain approach and the traditional approach in the WSNs structure access sensor data records. Figure 25 presents the comparison

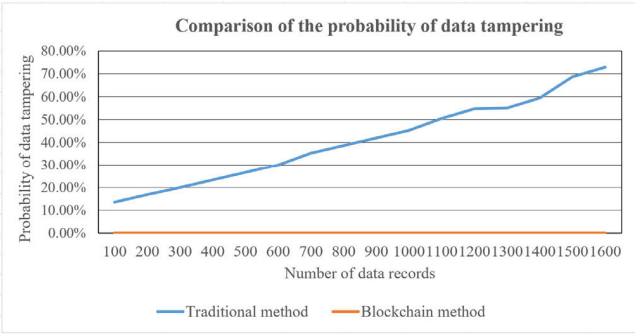


FIGURE 26. Comparison of the probability of data tampering.

of the number of data records that can be performed every half hour between the traditional approach and the blockchain approach. The figure clearly indicates that the approach of utilizing the blockchain has a worse number of records than the traditional approach. Although, it is only a small gap, and its show execution is nearly as good as that of other systems. This gap can still be accepted by operators. Improving the security of wireless sensor networks was the primary focus of our research.

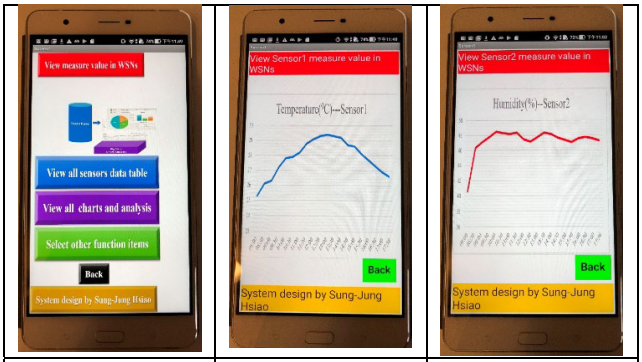
The genesis blockchain, i.e., the first block, has an index key value of ''0'', and the next block has a value of ''1''. To add a new block, it is important to compute whether the previous hash function has been duplicated successfully.

Figure 24 presents the system proposed by us, which consists of a number of program files, each of which is our subsystem. Figure 25 is a comparison of sensing data transfer analysis. When the data are more than the number, the system simplifies the data format of different agreements because of the use of the Web platform, so the overall efficiency of the system is better. However, microcontrollers choose built-in memory because we use software to overcome many problems of transferring data, such as data format conversion, or different protocol platforms.

Figure 26 presents the comparison of the probability of data tampering when the system uses general technology and has blockchain technology. Obviously, when the amount of sensed data is larger, the proposed system uses the traditional wireless sensor network method, and the data transmitted by it is more likely to be tampered with. Under the same data transmission conditions, when the proposed system with blockchain method processes a large amount of data, the data transmitted by the wireless sensor network is difficult to be secretly modified, which will be the application of the blockchain method benefit.

IX. RESULTS ANALYSIS

This section presents the mobile device operation display. First, on the system login frame, and the system app presents button options such as those presented in Figure 27(a). Upon pressing the first button, labeled ''view all sensors data table,'' the mobile device presents the whole and present data the sensors gather in a table mode. The next selection allows



(a)Login system main screen	(b)Temperature data	(c)Humidity data

FIGURE 27. Actual mobile device display showing how the proposed blockchain-based system operates in WSNs.

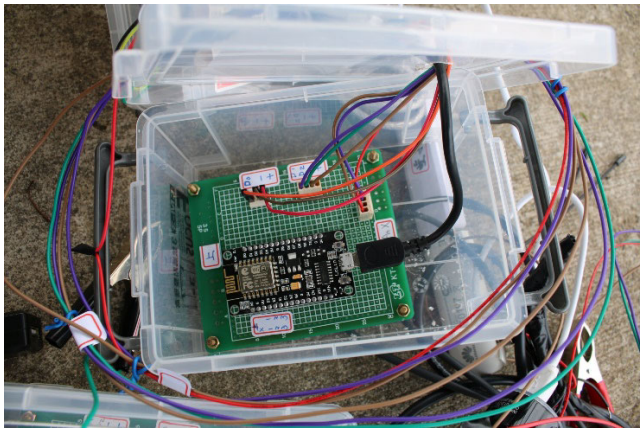


FIGURE 28. Actual microcontroller and sensor device.

the setting of the scope of the show to focus on the changing figure. The second button, named ''view all charts and analysis,'' shows a visual analysis utilizing multiple modes of data figures and charts. Figure 27(b) presents the figure analysis of the temperature measurements in the whole WSNs structure. This figure presents that the values for temperature measurements tend to be higher at about noon and lower in the morning and evening. Figure 27(c) shows the analysis of the humidity measurements; the humidity is lower in the morning and higher in the evening. A tarry in the data delivered from the sensors is detected because the data must go by blockchain sharing. This subject requires to be resolved. The WSNs in this research has evolved from the earlier ZigBee chip link to the present long-distance low-consumption LoRa chip link. Our laboratory utilizes the most up-to-date NB-IoT technique to enhance transfer efficiency and widen the scope for WSNs. Moreover, our study hopes to integrate the future network with 4G or 5G to carry out easy connections for all things on earth.

Our team uses a wireless sensing network and blockchain integration technology to conduct various farmland environmental sensing analyses of rice growth. The items observed include temperature and humidity in the air, illuminance, ultraviolet light, average speed of the wind, maximum speed

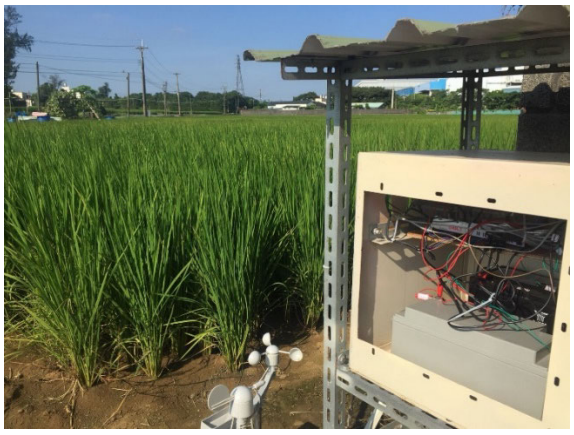
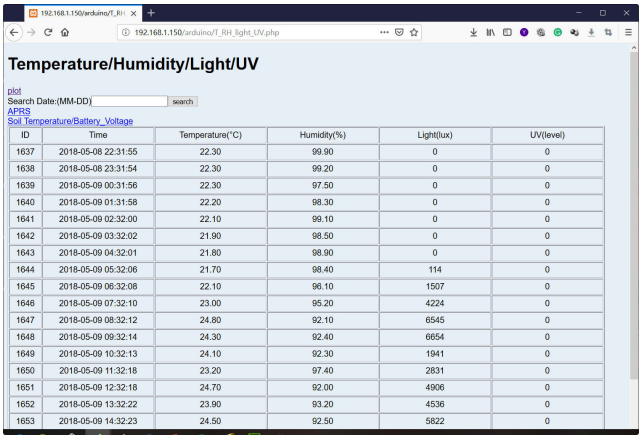
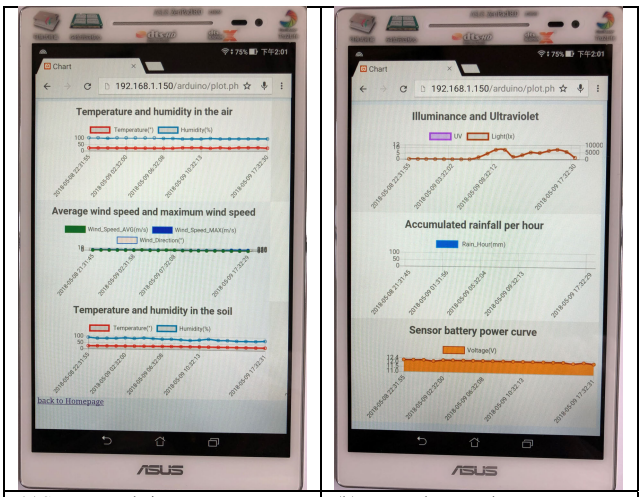


FIGURE 29. Sensor node device and router device.



ID	Time	Temperature(°C)	Humidity(%)	Light(lux)	UV(level)
1637	2018-05-08 22:31:55	22.30	99.90	0	0
1638	2018-05-08 23:31:54	22.30	99.20	0	0
1639	2018-05-09 00:31:56	22.30	97.50	0	0
1640	2018-05-09 01:31:58	22.20	98.30	0	0
1641	2018-05-09 02:32:00	22.10	99.10	0	0
1642	2018-05-09 03:32:02	21.90	98.50	0	0
1643	2018-05-09 04:32:01	21.80	98.90	0	0
1644	2018-05-09 05:32:06	21.70	98.40	114	0
1645	2018-05-09 06:32:08	22.10	96.10	1507	0
1646	2018-05-09 07:32:10	23.00	95.20	4224	0
1647	2018-05-09 08:32:12	24.80	92.10	6545	0
1648	2018-05-09 09:32:14	24.30	92.40	6654	0
1649	2018-05-09 10:32:13	24.10	92.30	1941	0
1650	2018-05-09 11:32:18	23.20	97.40	2831	0
1651	2018-05-09 12:32:18	24.70	92.00	4906	0
1652	2018-05-09 13:32:22	23.90	93.20	4536	0
1653	2018-05-09 14:32:23	24.50	92.50	5822	0

FIGURE 30. The system receives sensing data from remote sensors.



(a)System real-time temperature and humidity curve analysis chart	(b) UV and sensor battery inventory data display

FIGURE 31. The actual mobile device instantly displays the sensing curve.

of the wind, accumulated rainfall per hour, temperature and humidity of the soil, and power curves of the sensor battery. Figure 28 shows the microcontroller and sensor hardware. Figure 29 shows the placement of the sensor and the base station. Our team placed 20 sensor nodes around the rice fields.

Figure 30 shows the system receiving data from remote sensors. Our system uses the MySQL database system. Figure 31 shows that the farmland sensor device transmits data to each node in real-time, and the farmland observation data can be immediately displayed by logging into the system using the mobile device.

The daily temperature and humidity changes are relatively small, but the temperature and humidity in the soil change due to water irrigation. Ultraviolet light will also change due to sunrise time. This experiment focuses on the correct delivery of remote sensing data.

X. CONCLUSION

For the integration of blockchain technology into WSNs, the following aspects need to be discussed further.

A. BLOCKCHAIN CAUSES DATA TRANSMISSION DELAY

Every blockchain requires cryptography processing and public key deciphering to achieve linking. Moreover, creating a new blockchain requires confirmation of the link's previous and latter sequences beforehand to transmit data. Therefore, to achieve instantaneous data update and storage, some issues need to be fixed.

B. ISSUES RELATED TO AN INCREASE IN THE MEASUREMENT DATA AMOUNT

With the proposed approach using blockchain technology, the hash function and encryption key compute cannot be avoided. However, as the quantity of data increases, the time needed for the calculation process increases, thus reducing the data transfer efficiency. Therefore, large-scale computations will increase the data deal with time.

Our team continues to improve the abovementioned shortcomings using approaches such as the resetting mechanism of blockchains, which will constantly update data transfer to the most current status. Another method that may contribute is the use of a system control mechanism and a simplified process of hash function calculation. Additionally, to simplify blockchain security, encryption will be switched from asymmetric to symmetric.

Adding blockchain technology to many information applications will produce many benefits. Blockchain technology uses a decentralized and general consensus mechanism to maintain the integrity of the data, and can effectively prevent the risk of data tampering when the data is transmitted. The ledger that originally used blockchain technology in finance can be regarded as the sensory database of WSN. Based on blockchain technology, a block has a more reserved record database, and each block contains a time-stamp that cannot be forged.

REFERENCES

[1] S.-Y. Wang, Y.-J. Hsu, and S.-J. Hsiao, "Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation," in *Proc. Int. Symp. Comput., Consum. Control (ISC)*, Dec. 2018, pp. 149–152.

[2] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, Mar. 2018.

[3] L. Thomas, C. Long, P. Burnap, J. Wu, and N. Jenkins, "Automation of the supplier role in the GB power system using blockchain-based smart contracts," *CIRED-Open Access Proc. J.*, vol. 2017, no. 1, pp. 2619–2623, Oct. 2017.

[4] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[5] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.

[6] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.

[7] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[8] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[9] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

[10] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[11] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[12] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[13] H. Jang and J. Lee, "An empirical study on modeling and prediction of bitcoin prices with Bayesian neural networks based on blockchain information," *IEEE Access*, vol. 6, pp. 5427–5437, 2018.

[14] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov. 2017.

[15] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Comput.*, vol. 4, no. 4, pp. 84–90, Jul. 2017.

[16] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[17] M. E. Peck, "Blockchain world–do you need a blockchain? This chart will tell you if the technology can solve your problem," *IEEE Spectr.*, vol. 54, no. 10, pp. 38–60, Oct. 2017.

[18] M. E. Peck and S. K. Moore, "The blossoming of the blockchain," *IEEE Spectr.*, vol. 54, no. 10, pp. 24–25, Oct. 2017.

[19] P. Fairley, "Blockchain world–feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectr.*, vol. 54, no. 10, pp. 36–59, Oct. 2017.

[20] A. Nordrum, "Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything," *IEEE Spectr.*, vol. 54, no. 10, pp. 54–55, Oct. 2017.

[21] M. E. Peck and D. Wagman, "Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectr.*, vol. 54, no. 10, pp. 56–61, Oct. 2017.

[22] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[23] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.

[24] A. Islam, M. B. Uddin, M. F. Kader, and S. Y. Shin, "Blockchain based secure data handover scheme in non-orthogonal multiple access," in *Proc. 4th Int. Conf. Wireless Telematics (ICWT)*, Jul. 2018, pp. 1–5.

[25] K. Kotobi and S. G. Bilen, "Blockchain-enabled spectrum access in cognitive radio networks," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2017, pp. 1–6.

[26] X. Feng, J. Ma, T. Feng, Y. Miao, and X. Liu, "Consortium blockchain-based SIFT: Outsourcing encrypted feature extraction in the D2D network," *IEEE Access*, vol. 6, pp. 52248–52260, 2018.

[27] Z. Wang, Y. Tian, and J. Zhu, "Data sharing and tracing scheme based on blockchain," in *Proc. 8th Int. Conf. Logistics, Informat. Service Sci. (LISS)*, Aug. 2018, pp. 1–6.
[28] Q. He, Y. Xu, Y. Yan, J. Wang, Q. Han, and L. Li, "A consensus and incentive program for charging piles based on consortium blockchain," *CSEE J. Power Energy Syst.*, vol. 4, no. 4, pp. 452–458, 2018.
[29] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: A survey," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2205–2224, Apr. 2019.
[30] S. A. Sert, E. Onur, and A. Yazici, "Security attacks and countermeasures in surveillance wireless sensor networks," in *Proc. 9th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2015, pp. 201–205.
[31] A. Sharma and S. Chauhan, "Sensor fusion for distributed detection of mobile intruders in surveillance wireless sensor networks," *IEEE Sensors J.*, vol. 20, no. 24, pp. 15224–15231, Dec. 2020.
[32] A. Yazici, M. Koyuncu, S. A. Sert, and T. Yilmaz, "A fusion-based framework for wireless multimedia sensor networks in surveillance applications," *IEEE Access*, vol. 7, pp. 2169–3536, Jul. 2019.
[33] X. Gou, C. Zhao, T. Yang, L. Zou, Y. Zhou, Y. Yan, X. Li, and B. Cui, "Single hash: Use one hash function to build faster hash based data structures," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Jan. 2018, pp. 278–285.
[34] M. Kidon and R. Dobai, "Evolutionary design of hash functions for IP address hashing using genetic programming," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jun. 2017, pp. 1720–1727.
[35] N. Veeraragavan, L. Arockiam, and S. S. Manikandasaran, "Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud," in *Proc. Int. Conf. Algorithms, Methodol., Models Appl. Emerg. Technol. (ICAMMAET)*, Feb. 2017, pp. 1–6.
[36] A. Mustafa and Hendrawan, "Calculation of encryption algorithm combination for video encryption using two layers of AHP," in *Proc. 10th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2016, pp. 1–7.
[37] A. A. Moldovyan, N. A. Moldovyan, A. N. Berezin, and P. I. Shapovalov, "Randomized pseudo-probabilistic encryption algorithms," in *Proc. 20th IEEE Int. Conf. Soft Comput. Meas. (SCM)*, May 2017, pp. 14–17.
[38] F. S. Wu, "Research of cloud platform data encryption technology based on ECC algorithm," in *Proc. Int. Conf. Virtual Reality Intell. Syst. (ICVRIS)*, Aug. 2018, pp. 125–129.
[39] B. T. Baker, R. F. Silva, V. D. Calhoun, A. D. Sarwate, and S. M. Plis, "Large scale collaboration with autonomy: Decentralized data ICA," in *Proc. IEEE 25th Int. Workshop Mach. Learn. Signal Process. (MLSP)*, Sep. 2015, pp. 1–6.
[40] K. Xie, W. Luo, X. Wang, D. Xie, J. Cao, J. Wen, and G. Xie, "Decentralized context sharing in vehicular delay tolerant networks with compressive sensing," in *Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2016, pp. 169–178.
[41] K. Nomura, M. Mohri, Y. Shiraishi, and M. Morii, "Attribute revocable attribute-based encryption for decentralized disruption-tolerant military networks," in *Proc. 3rd Int. Symp. Comput. Netw. (CANDAR)*, Dec. 2015, pp. 491–494.
[42] Y. He, M. Yan, M. Shahidehpour, Z. Li, C. Guo, L. Wu, and Y. Ding, "Decentralized optimization of multi-area electricity-natural gas flows based on cone reformulation," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4531–4542, Jul. 2018.

SUNG-JUNG HSIAO received the B.S. degree in electrical engineering from the National Taipei University of Technology, Taiwan, in 1996, the M.S. degree in computer science and information engineering from National Central University, Taiwan, in 2003, and the Ph.D. degree from the Department of Electrical Engineering, National Taipei University of Technology, in 2014. He is currently working with the Department of Information Technology, Takming University of Science and Technology, as an Assistant Professor. He has had the work experience of research and design at the famous computer company of Acer Universal Computer Company, Mitsubishi, and FIC.

WEN-TSAI SUNG (Member, IEEE) received the M.S. and Ph.D. degrees from the Department of Electrical Engineering, National Central University, Taiwan, in 2000 and 2007, respectively. He is currently working with the Department of Electrical Engineering, National Chin-Yi University of Technology, as a Distinguished Professor, and the Dean of Research and Development. His research interests include the artificial intelligence Internet of Things (AIoT) and wireless sensors networks. He has won the 2009 JMBE Best Annual Excellent Paper Award and the Dragon Thesis Award that sponsor is Acer Foundation.