An Intelligent Agriculture Network Security System Based on Private Blockchains

Hsin-Te Wu and Chun-Wei Tsai

Abstract: **Countries around the world are nowadays actively promoting development in intelligent agriculture. Each of them must develop a specific plan tailored to environmental farming indices of each individual farm, and such information would be both important and sensitive. This is why information in intelligent agriculture requires protection from network security to ensure data privacy and integrity. This study proposes applying dark web technology to ensure the privacy of blockchains and servers. The study will monitor packet transmission frequency in intelligent agriculture to prevent distributed denial-of-service (DDOS) attacks. The main features of system include: (1) An identity authentication mechanism, (2) secure transmission of information, (3) establishment of private blockchains, (4) a faster, improved authentication system for blockchain information, and (5) resistance against DDOS attacks. The proposed scheme can safeguard network security for the IoT as well as the servers by way of applying dark web technology, which can avoid exposure of blockchains and server ID addresses and thus in turn lower the risks of DDOS attack damages. Experiment results indicate that the application of lightweight encryption of proposed scheme does indeed improve the authentication speed while also satisfying requirements of network security.**

Index Terms: **Blockchain, intelligent agriculture, internet of things, network security, privacy.**

I. INTRODUCTION

FOOD and energy are indispensable to human beings, and we can see from this study [1] how, as countries around the globe experience increased population and economic development, the demand of human for crops are bigger than ever. According to this study [2], the global population is expected to grow from 1.8 billion in 2009 to 4.9 billion in 2030; subsequently, demand for dairy products will rise as well. This study [3] mentions that the human demand for farm crops will increase drastically by 2050 and, therefore, agriculture production must be doubled. However, the agriculture labor force of today is facing the problem of ageing; moreover, the growingly extreme climate of today is causing damage towards crops that has led to a global food crisis – a problem to be faced by countries all around the world [4]. In particular, crisis in water resources will cause graver and graver water shortage in the decades to come [5]. Intelligent agriculture can effectively monitor the grow of crops; meanwhile, its use of sensors to aid in procedures such as water irrigation and spreading can help reduce labor costs. Intelligent agriculture is also capable of determining and adjusting the amount of water need for irrigation based on environmental factors such as soil condition, which reduces waste of water resources.

The proposed scheme applies bilinear pairings technology to create a network security system that satisfies the following requirements. (1) It has an intelligent agriculture identity authentication mechanism. Given that intelligent agriculture systems are established in outdoor environments, in order to prevent tampering from malicious parties, the system has added an authentication mechanism to verify legitimacy of any identity. (2) It guarantees privacy and integrity in information transmission – in order to prevent information exposure during sensor data transmission in intelligent agriculture, the study has applied symmetric encryption and hash technology to ensure information privacy and integrity. (3) It has established a blockchain system that warrants information preservation and accuracy. (4) Its application of dark web technology can avoid exposure of blockchains and server location that could lead to malicious distributed denial-of-service (DDOS) attacks. (5) It boasts a blockchain information authentication mechanism – the study has established a rapid authentication mechanism that improves the authentication speed while reducing its computational burden. (6) An intelligent agriculture system needs to fend off DDOS attacks and, because an intelligent agriculture system collects data at fixed hours, the server will calculate the transmission frequency of system, and if the frequency is too high, it will discard the packet and alert the administrator. (7) The proposed intelligent agriculture system keeps track of environmental cultivation factors of a farm, which would include cultivation techniques of a farmer as well as coefficient data such as the soil electrical conductivity specific to an individual farm. Our proposed main contribution of scheme is establishing network security for IoT networks.

II. RELATED WORK

First of all, we wish to examine network security issues in IoT networks. This study [6]–[8] mentions that most IoT networks do not possess any network security mechanism and are therefore susceptible to Linux.Darlloz or DDOS attacks; consequently, many IoT networks face the problem of breach of important data. The main reason for such problem is that IoT networks lack authentication mechanisms – as mentioned in studies [9] and [10], when intelligent healthcare or intelligent furniture lack authentication mechanism, they fall prey to malicious attacks such as data breach or even bigger disasters. While on the topic of IoT network security, this study [11] refers to the 2015

Manuscript received May 5, 2019.

H. Wu is with the Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Penghu, Taiwan, email: wuhsinte@gms.npu.edu.tw.

C.-W. Tsai is with the Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, email: cwtsai@cse.nsysu.edu.tw.

C.-W. Tsai is the corresponding author.

Digital Object Identifier: 10.1109/JCN.2019.000043

1229-2370/19/$10.00 © 2019 KICS

remark of federal trade commission (FTC) that IoT shall encounter grave issues in privacy and network security to remind us of the necessity to emphasize IoT network security. On that note, study [12], [13] posits that an IoT network should meet the following criteria: lightweight encryption, data integrity and access control, as well as secure middleware and cyber physical system.

For instance, this study [9], [14] uses a PKI mechanism to authenticate an IoT identity of user; however, PKI requires the use of certificates to authenticate validity and origin of a key, and since certificates call for certificate authorities to confirm validity and origin, it demands significant time for authentication and computational burden. This study [15] aims at creating an Internet of Vehicles network security system by applying elliptic curve cryptography to enable establishment of symmetric encryption keys between vehicles and gateways; additionally, it applies symmetric encryption to encrypt data because symmetric encryption calls for computation of low complexity, which helps relieve the computational burden of IoT network. For instance, this study [16] works on protocol definition and security design of protocol of each transport layer in the IoT network, resolving network security issues for all transport layers. The network layer is encrypted using secure sockets layer (SSL) while the application layer uses advanced encryption standard for encryption that ensures network security. Meanwhile, this study [17] relies on the security of communication protocols to guarantee message integrity. This study [18] utilizes the characteristic value of email and machine learning to identify the sender of spams in order to minimze spam attacks.

Since blockchains can be utilized in authenticating message integrity as well as identity legitimacy, many studies have proposed integrating blockchains with IoT technology in order to provide data protection. Adopting this approach, this study [19] discusses how blockchains can help authenticate message origin and security while PKI encryption can be used to ensure message security in order to effectively resist DDOS attacks. This study [20] proposes applying the blockchain architecture towards IoT networks and using smart contracts to safeguard information legitimacy and security. This study [21] suggests using blockchains to solve privacy and security issues in IoT networks; the study uses bilinear pairing to create an encryption system that covers from system registration to data transmission and can authenticate identity legitimacy and data privacy in the IoT network.

III. BACKGROUND

A. Bilinear Pairings

The features of bilinear pairing are as follows:

- Bilinear: $e = (aP, bP) = e(P, P)^{ab}$, $a, b \in Z_q^*$.
- Non-degeneracy: $Q \in G_1$ such that $e\left(Q, Q\right) \neq 1$.
- Computable: There exists an efficient algorithm to compute $e\left(Q, Q\right)$ for all $Q \in G_1$.

Bilinear pairings cryptography is realized in this study [22], with G_1 and data volume being of q, respectively, 161 bits and 160 bits. This study applies ID-based cryptography (IBC) [23] that emphasizes bilinear pairings technology.

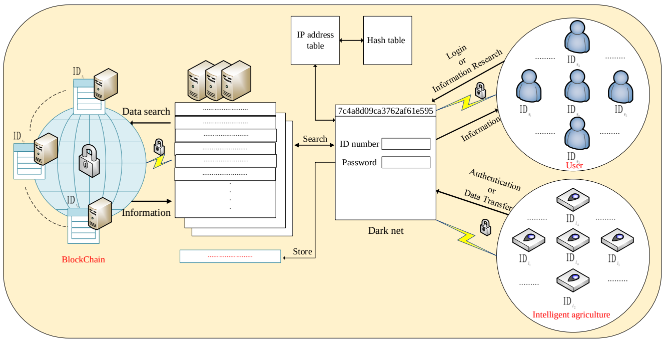


Fig. 1. System illustration.

B. Blockchains

Blockchain has become a hot topic in the finance industry as well as the tech industry. The concept of blockchains stemmed from Bitcoin of 2018. In blockchain technology, data is distributed and stored in each node; it also applies the concept of distributed ledgers or shared ledgers and distributes the ledgers in each node. Since blockchains are widely applied in industries such as medicine and finance, information of which require privacy protection, this study [24] established an identity managing system to safeguard access rights of its user to data in order to prevent breach of blockchain data. This study [25] employs anonymity to secure the identity of a Bitcoin owner. Our study employs blockchains to protect access rights of a user and avoid DDOS attacks from hackers. This study also conducted a performance analysis comparison against studies [24], [25].

C. Systems Model

The proposed system is shown in Fig. 1. This study uses stationary intelligent agriculture equipment ($I_1 \sim I_n$), all of which employ 4G mobile communication. $I_1 \sim I_n$ equipped with sensors for keystroke authentication and GPS; they also come with solar power devices that do not require additional power support. The proposed system also has a dark net mechanism (TA); when anyone attempts to access data from the blockchains ($S_1 \sim S_n$), they must undergo mutual identity authentication and establish a common session key. Each time, the common session key between the TA and $S_1 \sim S_n$ will be different so as to prevent hackers from obtaining secret key of TA through malicious attacks. Data transmission between blockchains, $I_1 \sim I_n$, and TA rely on symmetric encryption; the authentication mechanism of blockchain employs bilinear pairings cryptography to verify data origin, utilizes hash-based message authentication code (HMAC) to ensure message integrity, and uses symmetric encryption to ensure message privacy.

IV. THE PROPOSED SCHEME

A. System Initialization

The proposed system first computes TA and security coefficients including the public key as well as private key of $I_1 \sim I_n$ and $S_1 \sim S_n$. Symbols used in this study are shown in Table 1. TA is computed as follows:

- TA selects a random number $s \in Z_q^*$ as the master key, in which r is a public value while s is secret value of TA.

Table 1. Summary of notations and symbols.

Symbol	Meaning of the symbol
P	The generator of G_1.
Q	The generator of G_1.
$\mathbb{ID}_{\approxeq}$	The real ID of the user u.
G_1	The additive group.
G_2	The multiplicative group.
s, k	A random number $s, k \in Z_q^*$ chosen as the master key where Z_q^* is a finite field of order q.
$\mathcal{SK}$	The common session key.
$\mathcal{SYE}_{\mathbb{ID}_{\approxeq}}$	The symmetric encryption of user u.
e	The bilinear map.
H	The hash function.
M	The message or smart contract.
$\mathcal{G}_{\mathbb{ID}_{\approxeq}}$	The GPS message of user u.
$\mathcal{D}_{\mathbb{ID}_{\approxeq}}$	The sensor information of user u.
$\mathcal{PR}_{\mathbb{ID}_{\approxeq}}$	The private key of user u.
$\mathcal{PK}_{\mathbb{ID}_{\approxeq}}$	The public key of user u.
$\mathcal{PU}_{\mathbb{ID}_{\approxeq}}$	The public value of user u.
$\mathcal{T}_{\mathbb{ID}_{\approxeq}}$	The timestamp of user u.

- The ID of TA is $\mathbb{ID}_{\mathbb{TA}}$; the public key is $\mathcal{PK}_{\mathbb{ID}_{\mathbb{TA}}} = \mathbb{ID}_{\mathbb{TA}} \cdot \mathbb{P}$ while the private key is $\mathcal{PR}_{\mathbb{ID}_{\mathbb{TA}}} = r^s \cdot \mathbb{ID}_{\mathbb{TA}} \cdot \mathbb{P}$.
- The public value of TA is $\mathcal{PU}_{\mathbb{ID}_{\mathbb{TA}}} = r^s \cdot P$.

Following the above, the system computes security coefficients such as the public key and private key of $I_1 \sim I_n$, as follows:

- TA sets public key of I_n as $\mathcal{PK}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}} = \mathbb{ID}_{\mathbb{I}_{\ltimes}} \cdot \mathbb{P}$.
- TA sets private key of I_n as $\mathcal{PR}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}} = r^s \cdot \mathbb{ID}_{\mathbb{I}_{\ltimes}} \cdot \mathbb{P}$.

Next, the system computes security coefficients such as the public key and private key of $S_1 \sim S_n$, as follows:

- TA sets public key of S_n as $\mathcal{PK}_{\mathbb{ID}_{\mathbb{S}_{\ltimes}}} = \mathbb{ID}_{\mathbb{S}_{\ltimes}} \cdot \mathbb{P}$.
- TA sets private key of S_n as $\mathcal{PR}_{\mathbb{ID}_{\mathbb{S}_{\ltimes}}} = r^s \cdot \mathbb{ID}_{\mathbb{S}_{\ltimes}} \cdot \mathbb{P}$.

B. Authentication

When the administrator has set up the stationary intelligent agriculture equipment, they will proceed to use the keyboard of equipment to input the password of administrator and activate the program. The intelligent agriculture equipment comes with a GPS sensor that detects the longitude and latitude of the location ($\mathcal{T}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}}$) of equipment. Following that, $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$ will perform identity authentication with $\mathbb{ID}_{\mathbb{TA}}$. First, both parties establish a common session key ($\mathcal{SK}$) using their own private key and the public key of other party. $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$ must compute session key of $\mathbb{ID}_{\mathbb{TA}}$ with the equation $\mathcal{SK}_{\mathcal{I}_{\setminus} \leftrightarrow \mathcal{TA}} = \rceil \left(\mathcal{PR}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}}, \mathcal{PK}_{\mathbb{ID}_{\mathbb{TA}}}\right)$; meanwhile, $\mathbb{ID}_{\mathbb{TA}}$ can also compute session key of $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$, so the two parties can utilize the session key to conduct private communication. $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$ and $\mathbb{ID}_{\mathbb{TA}}$ will compute secret value of HMAC and transmit the GPS location of equipment, mainly relying on HMAC to authenticate message origin and integrity. Additionally, the system will verify the GPS location to prevent the equipment from being moved around or suffering other malicious behavior. The algorithm for identity authentication is as follows:

$\mathbb{ID}_{\mathbb{I}_{\ltimes}}$ computes k and $\mathcal{T}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}}$, and proceeds to encrypt them using $\mathcal{SK}_{\mathcal{I}_{\setminus} \leftrightarrow \mathcal{TA}}$ before transmitting the data to $\mathbb{ID}_{\mathbb{TA}}$. $\mathbb{ID}_{\mathbb{TA}}$ will then compute $\mathcal{PU}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}} = \nabla^{\frac{\infty}{\int}} \cdot \mathbb{ID}_{\mathbb{TA}} \cdot \mathbb{ID}_{\mathbb{I}_{\ltimes}} \cdot \mathbb{P}$ and encrypt the data before transmitting to $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$. Upon reception, $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$ generates key of HMAC, encrypts it, and then transmits it to $\mathbb{ID}_{\mathbb{TA}}$. Each time $\mathbb{ID}_{\mathbb{TA}}$ and $\mathbb{ID}_{\mathbb{I}_{\ltimes}}$ exchange messages, a different key is used for data encryption and transmission to prevent exposure of private keys. Meanwhile, there will be frequent communication between blockchains and TA; hence, establishing a common session key allows for the identity authentication and private communication . This study proposes using symmetric encryption for message transmission in order to effectively reduce the computational burden of equipment.

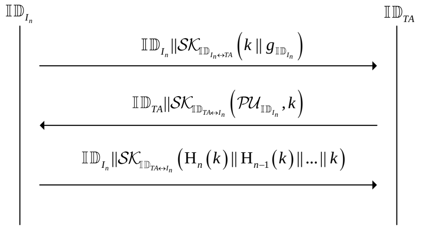

$\mathbb{ID}_{I_n}$
$\mathbb{ID}_{TA}$
$\mathbb{ID}_{I_n} \| \mathcal{SK}_{\mathbb{ID}_{I_n \leftrightarrow TA}} \left(k \,\|\, g_{\mathbb{ID}_{I_n}}\right)$
$\mathbb{ID}_{TA} \| \mathcal{SK}_{\mathbb{ID}_{TA \leftrightarrow I_n}} \left(\mathcal{PU}_{\mathbb{ID}_{I_n}}, k\right)$
$\mathbb{ID}_{I_n} \| \mathcal{SK}_{\mathbb{ID}_{TA \leftrightarrow I_n}} \left(\mathrm{H}_n(k) \,\|\, \mathrm{H}_{n-1}(k) \,\|\, ... \,\|\, k\right)$

Fig. 2. Encryption/decryption algorithm 1: Identity authentication.

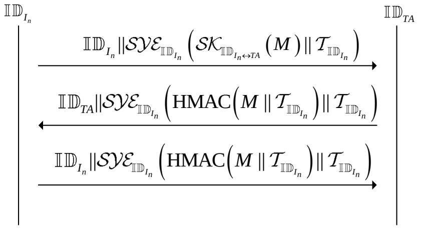

$\mathbb{ID}_{I_n}$
$\mathbb{ID}_{TA}$
$\mathbb{ID}_{I_n} \| \mathcal{SYE}_{\mathbb{ID}_{I_n}} \left(\mathcal{SK}_{\mathbb{ID}_{I_n \leftrightarrow TA}}(M) \,\|\, \mathcal{T}_{\mathbb{ID}_{I_n}}\right)$
$\mathbb{ID}_{TA} \| \mathcal{SYE}_{\mathbb{ID}_{I_n}} \left(\mathrm{HMAC}\left(M \,\|\, \mathcal{T}_{\mathbb{ID}_{I_n}}\right) \| \mathcal{T}_{\mathbb{ID}_{I_n}}\right)$
$\mathbb{ID}_{I_n} \| \mathcal{SYE}_{\mathbb{ID}_{I_n}} \left(\mathrm{HMAC}\left(M \,\|\, \mathcal{T}_{\mathbb{ID}_{I_n}}\right) \| \mathcal{T}_{\mathbb{ID}_{I_n}}\right)$

Fig. 3. Encryption/decryption algorithm 2: Message transmission and authentication.

C. Message Transmission and Authentication

For message transmission between TA and $I_1 \sim I_n$, this study employs a total number of n sets of HMAC keys; each message transmission uses a different key for privacy encryption. The proposed advantage of scheme is that TA can monitor whether any packet has been lost during message transmission between $I_1 \sim I_n$. In addition, the message is attached with the GPS location and timestamp to prevent DDOS attacks and other hardware attacks. The message transmission and authentication between $I_1 \sim I_n$ and TA is computed with the following algorithm:

When I_n and TA have completed identity authentication, both parties will have obtained the k value to compute n sets of HMAC secret keys. If In wishes to transmit a message to TA, it must first compute the GPS location and sensor data, $M = \left(\mathcal{G}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}} || \mathcal{D}_{\mathbb{ID}_{\mathbb{I}_{\ltimes}}}\right)$; In then encrypts the data using its common session key with TA, followed by computing the timestamp and utilizing the nth set of key of k value to encrypt and transmit the message to TA. Upon reception, TA deciphers the message and then determines whether the GPS location has changed and whether the time difference between the timestamp and that of the previous set of data falls within reasonable range. The computation is as follows:

The equipment used in this study are placed outdoors and are therefore in risk of malicious attacks; for instance, a ma-

Algorithm 1 GPS location determination.

```
if $\mathcal{G}_{\mathbb{ID}_{\mathbb{I}_\ltimes}} \neq \mathcal{G}'_{\mathbb{ID}_{\mathbb{I}_\ltimes}}$ or $\left(\mathcal{T}_{\mathbb{ID}_{\mathbb{I}_\ltimes}} - \mathcal{T}_{\mathbb{ID}'_{\mathbb{I}_\ltimes}}\right)$ >Range then
    Discard packet
else
    Proceed with message transmission
end if
```

licious party might hack into the IoT development board or even physically remove the board at once. With this in mind, the system requires identity authentication whenever anyone attempts to implant a program; moreover, if the equipment is physically moved, then the server will consider any attempt as an external force and reject any packets. TA utilizes Algorithm 1 to determine equipment of I_n has been moved around. It means that this system will determine whether the time difference between the timestamp of packet and that of the previous packet is greater than the established range. Also, it determines whether packets have been continuously transmitting within a short period of time; if so, then it signifies the possibility of a DDOS attack, and it will discard the packet; if not, then TA will compute HMAC value of I_n message and timestamp, and then use the nth set of key of k to encrypt and transmit to I_n. After receiving and confirming the message, I_n will transmit the same message back to TA; TA will then encrypt $\mathcal{SK}_{\mathcal{I}_\backslash\leftrightarrow\mathcal{TA}}(\mathcal{M})||\mathcal{T}_{\mathbb{ID}_{\mathbb{I}_\ltimes}}||\mathcal{HMAC}||\mathcal{PU}_{\mathbb{ID}_{\mathbb{I}_\ltimes}}||||\backslash$ using the common session key and transmit it to the blockchain.

D. Dark Web

This study employs dark web technology to ensure the privacy of blockchains. The study has also established a web browser; any user must first undergo identity authentication before conducting any information search. In the dark web, the address bar of browser will only show the hash value and not the real IP of blockchain. The dark web has a correspondence chart that contains the correspondence between real IP of a blockchain and its hash value. The study employs dark web technology for the following advantages: (1) It guarantees access of legitimate users to blockchains; (2) it prevents hackers from obtaining the real location of blockchain to launch DDOS attacks; and (3) it uses the dark web to create private blockchains that can prevent malicious breach of data. In the proposed scheme, the dark web (TA) also runs identity authentication with equipments of $I_1 \sim I_n$. When the authentication goes through, the packets of $I_1 \sim I_n$ will be distributed in the blockchains. As shown in illustration of Fig. 1 of roles, the dark web plays the role of a mediator. The dark web establishes the browser and provides the network program; $I_1 \sim I_n$ and legitimate users can enter and access data; identity and message authentication between the dark web and $I_1 \sim I_n$ are illustrated in Subsections IV.B and IV.C. Users can complete identity authentication via the dark web and search for user information using the following dark web message encryption computation:

The user uses IBC and TA to authenticate their identity; the user then encrypts the searched data and transmits it to TA, who, upon reception, will decipher the message using the common session key. TA then transmits the data to $S_1 \sim S_n$ for data search; $S_1 \sim S_n$ will encrypt their searched data using the common session key before transmitting it to TA, who will then decipher the message using the common session key before transmitting the data to users. During the above procedure, the common session key is used in authenticating the identity legitimacy and privacy of all different parties. Meanwhile, the user is unaware of the real location of $S_1 \sim S_n$, which reduces the risk of malicious cyberattacks.

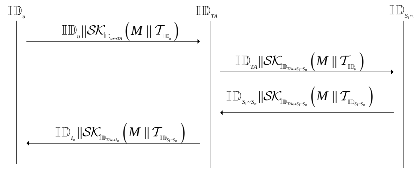

$\mathbb{ID}_u$
$\mathbb{ID}_{TA}$
$\mathbb{ID}_{S_1\sim S_n}$
$\mathbb{ID}_u||\mathcal{SK}_{\mathbb{ID}_{u\leftrightarrow TA}}\left(M \,||\, \mathcal{T}_{\mathbb{ID}_u}\right)$
$\mathbb{ID}_{TA}||\mathcal{SK}_{\mathbb{ID}_{TA\leftrightarrow S_1\sim S_n}}\left(M \,||\, \mathcal{T}_{\mathbb{ID}_u}\right)$
$\mathbb{ID}_{S_1\sim S_n}||\mathcal{SK}_{\mathbb{ID}_{TA\leftrightarrow S_1\sim S_n}}\left(M \,||\, \mathcal{T}_{\mathbb{ID}_{S_1\sim S_n}}\right)$
$\mathbb{ID}_{I_n}||\mathcal{SK}_{\mathbb{ID}_{TA\leftrightarrow I_n}}\left(M \,||\, \mathcal{T}_{\mathbb{ID}_{S_1\sim S_n}}\right)$

Fig. 4. Encryption/decryption algorithm 3: Dark web message encryption.

E. Blockchain Message Authentication

When the blockchain ($S_1 \sim S_n$) receives from TA a message $\mathcal{SK}_{\mathcal{I}_\backslash\leftrightarrow\mathcal{TA}}(\mathcal{M})||\mathcal{T}_{\mathbb{ID}_{\mathbb{I}_\ltimes}}||\mathcal{HMAC}||\mathcal{PU}_{\mathbb{ID}_{\mathbb{I}_\ltimes}}||||\backslash$, it will store the message in the block. If another server wishes to authenticate the message, it will first compute $\mathrm{HMAC}'_{k_n} = \mathcal{SK}_{\mathcal{I}_\backslash\leftrightarrow\mathcal{TA}}(\mathcal{M})$, and then proceed to determine whether HMAC'_{k_n} and HMAC are identical; if they are identical, then it signifies message integrity. Following that, it computes the message origin using $e\left(\mathbb{ID}_{\mathbb{I}_\ltimes} \cdot P, \mathbb{ID}_{\mathbb{TA}} \cdot P\right) = e\left(\mathcal{PU}_{\mathbb{ID}_{\mathbb{TA}}}, \mathcal{PU}_{\mathbb{ID}_{\mathbb{I}_\ltimes}}\right)$; if the results are identical, then the message is from I_n. In addition, the message is encrypted using TA and common session key of I_n, so that other users are unable to access contents of the message. This proposed of study authentication method can effectively authenticate blockchain integrity and origin while strengthening the privacy of message. The proposed scheme does not require any additional certificate to authenticate the validity and legitimacy of key, which in turn improves the authentication speed of blockchain.

When a user (U_n) locates (I_1) message of another equipment, they can only authenticate said integrity and origin of message. This is because U_n is incapable of obtaining the common session key between I_1 and TA. Even if U_n attempts to utilize their common session key with TA ($\mathcal{SK}_{\mathcal{U}_\backslash\leftrightarrow\mathcal{TA}}$) to obtain secret key of TA, it would still hardly succeed; for because on the Bilinear Diffie-Hellman (BDH) assumption, there exists computation hardness for U_n to obtain s from the private key. Therefore, our proposed blockchain method can ensure message privacy.

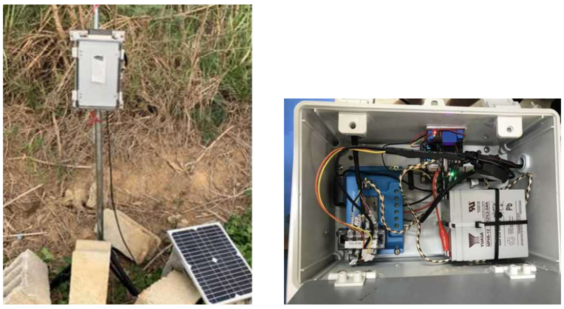
V. RESULTS

In Table 2, we suggest using encryption/decryption computation time to run method analysis; the encryption/decryption computation time is based on experiment results of studies [26], [27].

Table 3 is a comparison result of our proposed method against Studies [24], [25]. For identity authentication, our study employs IBC for authentication while this study [24] opts for elliptic curve cryptography to authenticate identity legitimacy, which means they need to compute whether the certificate of other

Table 2. Execution time in milliseconds.

Notation	Description	Execution time (ms)
T_p	Pairing operation	≈ 4.5
T_m	Point multiplication	≈ 0.6
T_e	Field exponentiation	≈ 0.45
H	HMAC	0.002
S_e	AES encryption	< 0.19
S_d	AES decryption	< 4.65



(a) (b)

Fig. 5. The equipments of the proposed system: (a) Intelligent agriculture equipment and (b) the interior of the intelligent agriculture equipment.

party is authentic. This study [25] adopts a share secret key method to authenticate legitimacy; from the results, we can see that our proposed method is superior to the other approaches. For message authentication, this study employs symmetric encryption to ensure message integrity and origin; by contrast, this study [24] authenticates the legitimacy and uses PKI of certificate for signatures as well as authentication of message integrity. This study [25] must collect the share secret key from each node and compute the master secret key before it may conduct deciphering. Experiment results indicate that our proposed approach surpasses other methods. Under our proposed blockchain system, the origin of each and every piece of information outperforms those of other approaches. All our proposed encryption methods fall under lightweight encryption; we employ symmetric encryption to effectively reduce computational burden.

The IoT equipment used in this proposed of study intelligent agriculture system includes temperature and humidity sensors, Grove Barometer Sensors, and soil sensors. IoT equipment in intelligent agriculture usually relies on 4G network for data transmission. The farm is about 0.4 acres in size and its main crop is radish. This study employs intelligent agriculture equipment in the hands-on experiment, as shown in Fig. 5. Fig. 5(a) shows the intelligent agriculture equipment conducting detection, while Fig. 5(b) illustrates the IoT development board of intelligent agriculture equipment and a GPS sensor. This study utilizes development boards and servers to implement and realize bilinear pairings network security, dark web, and blockchains.

VI. CONCLUSION

Given that IoT networks are not protected by network security, they are susceptible to cyberattacks or data breaches by hackers or other malicious parties. This study has created an intelligent agriculture network security mechanism; we have also employed dark web technology to construct a private blockchain environment. It is true that blockchains run of today on a distributed architecture and can run mutual authentication of message integrity and origin; nevertheless, in intelligent agriculture, relevant information is considered intellectual property of individual farmers, therefore warranting privacy protection. Moreover, once a blockchain server is exposed, it becomes easily attacked by hackers. The highlights of our contribution of study include the following. (1) The application of IBC technology in identity authentication mechanism ensures that only legitimate users can access blockchain information. (2) All data transmission between equipment or users are performed via symmetric encryption – the secret key of which is known to only the two parties – and therefore ensures privacy; moreover, symmetric encryption bears low computational complexity, making it perfect for IoT networks. (3) Our proposed private blockchain authentication mechanism of system not only helps authenticate message integrity and origin, but also prevents illegitimate users from accessing any data. (4) Our application of system of dark web technology protects physical servers and blockchains from location exposure that can lead to DDOS attacks; the real IP address is safe from exposure because all IP addresses are mapped using hash functions. (5) Our application of bilinear pairing in constructing the blockchain message authentication mechanism can effectively authenticate message integrity and origin. (6) Our use of dark web technology and identity authentication mechanism protects the system from cyberattacks.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions on the paper. This work was supported in part by the Ministry of Science and Technology of Taiwan, R.O.C., under Contracts MOST107-2221-E-005-029 and 108-2221-E-005-021-MY3. This work was also partially supported by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU) and was financially supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan.

REFERENCES

[1] M. Taniguchi, N. Masuhara, and K. Burnett, "Water, energy, and food security in the asia pacific region," *J. Hydrology: Regional Studies*, vol. 11, pp. 9–11, June 2015.

[2] C. Kulatunga, L. Shalloo, W. Donnelly, E. Robson, and S. Ivanov, "Opportunistic wireless networking for smart dairy farming," *IT Professional*, vol. 19, no. 2, pp. 16–23, 2017.

[3] F. Y. Narvaez, G. Reina, M. Torres-Torriti, G. Kantor, and F. A. Cheein, "A survey of ranging and imaging techniques for precision agriculture phenotyping," *IEEE/ASME Trans. Mechatron.*, vol. 22, no. 6, pp. 2428–2439, 2017.

[4] R. Gebbers and V. I. Adamchuk, "Precision agriculture and food security," *Science*, vol. 327, no. 5967, pp. 828–831, 2010.

[5] H. Navarro-Hellin *et al.*, "A wireless sensors architecture for efficient irrigation water management," *Agricult Water Manage*, vol. 151, pp. 64–74, 2015.

[6] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[7] Y. Agarwal and A. K. Dey, "Toward building a safe, secure, and easy-to-use internet of things infrastructure," *Computer*, vol. 49, no. 4, pp. 88–91, 2016.

[8] J. Margulies, "Garage door openers: An internet of things case study," *IEEE Security Privacy*, vol. 13, no. 4, pp. 80–83, 2015.

[9] M. Shahzad and M. P. Singh, "Continuous authentication and authorization for the internet of things," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 86–90, 2017.

[10] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1899–1909, 2017.

Table 3. Effectiveness analysis.

Property/method	**Chao Lin. et al. [24]**	**Qi Wang et al. [25]**	**The proposed scheme**
Identity authentication	Signing: T_p+ T_m+ T_e Verification: T_p+ T_m+ T_e Spending time: 11.28 (ms)	Signing: n* T_m Verification: n* T_m Spending time: 2*n*0.6 (ms)	Signing: T_p+ T_e Verification: T_p+ T_e Spending time: 10.08 (ms)
Private communication	Signing: N/A Verification: N/A	Signing: Se Verification: Sd Spending time: 4.84 (ms)	Signing: Se Verification: Sd Spending time: 4.84 (ms)
Message authentication	Signing: 2*T_p+ T_m+ T_e Verification: 2*T_p+ T_m+ T_e Spending time: 20.28 (ms)	Signing: n*T_p+ n*T_m Verification: n*T_p+ n*T_m Spending time: 2*n* 4.5 +2*n* 0.6 (ms)	Signing: Se+H Verification: Se+H Spending time: 4.844 (ms)
Blockchain message authentication	Signing: 2*T_p+ T_m+ T_e Verification: 2*T_p+ T_m+ T_e Spending time: 20.28 (ms)	Signing: n*T_p+ n*T_m Verification: n*T_p+ n*T_m Spending time: 2*n* 4.5 +2*n* 0.6 (ms)	Signing: T_p+T_e Verification: T_p+T_e Spending time: 10.08 (ms)

[11] V. A. Almeida, D. Doneda, and M. Monteiro, "Governance challenges for the internet of things," *IEEE Internet Comput.*, vol. 19, no. 4, pp. 56–59, 2015.

[12] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet of things: Research challenges and opportunities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3567–3569, 2018.

[13] T. Qiu, R. Qiao, and D. O. Wu, "Eabs: An event-aware backpressure scheduling scheme for emergency internet of things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, 2018.

[14] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Access*, vol. 25, no. 6, pp. 12–18, 2018.

[15] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2526–2536, 2018.

[16] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tut.*, vol. 17, no. 3, pp. 1294–1312, 2015.

[17] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[18] T. Qiu *et al*, "Sigmm: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, 2019.

[19] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[20] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, 2018.

[21] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24 639–24 649, 2018.

[22] M. Scott, "Computing the tate pairing," in *Proc. CT-RSA*, Feb. 2005.

[23] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Crypto*, Aug. 2001.

[24] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 25, pp. 28 203–28 212, 2018.

[25] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12 336–12 341, 2017.

[26] M. Scott, "Efficient implementation of cryptographic pairings," 2007. [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf

[27] A. J. Devegili, M. Scott, and R. Dahab, "Implementing cryptographic pairings over barreto-naehrig curves," in *Proc. ICPBC*, July 2007.

[28] J. Liu, Y. Chai, Y. Xiang, X. Zhang, S. Gou, and Y. Liu, "Clean energy consumption of power systems towards smart agriculture: Roadmap, bottlenecks and technologies," *CSEE J. Power Energy Syst.*, vol. 4, no. 3, pp. 273–282, 2018.

[29] M. Bacco, A. Berton, A. Gotta, and L. Caviglione, "IEEE 802.15.4 air-ground uav communications in smart farming scenarios," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1910–1913, 2018.

[30] M. Roopaei, P. Rad, and K.-K. R. Choo, "Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 10–15, 2017.

[31] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported internet of things," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 269–284, 2016.

[32] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "SDN-based data transfer security for internet of things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 257–268, 2018.

Hsin-Te Wu is an Assistant Professor of Department of Computer Science and Information Engineering from National Penghu University of Science and Technology, Taiwan. He received the Ph.D. Degree in Department of Computer Science and Engineering from National Sun Yat-Sen University, Taiwan, in 2013. His research interests include computer networks, wireless network, speech compression, network security and Internet of things.

Chun-Wei Tsai received the Ph.D. degree in Computer Science and Engineering from National Sun Yat-sen University, Kaohsiung, Taiwan, in 2009. He was a Postdoctoral fellow with the Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan before joining the faculty of the Applied Geoinformatics and the Information Technology, Chia Nan University of Pharmacy & Science, Tainan, Taiwan in 2010 and 2012, respectively. He joined the faculty of the Department of Computer Science and Information Engineering, National Ilan University, Yilan, Taiwan, in 2014, the Department of Computer Science and Engineering, National Chung-Hsing University, Taichung, Taiwan, in 2017, and then the Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, in 2019, where he is currently an Assistant Professor.