Peer-to-Peer Networking and Applications (2018) 11:1230–1239
https://doi.org/10.1007/s12083-018-0635-3

Enhanced secure device authentication algorithm in P2P-based smart farm system

Cheol-Joo Chae[1] · Han-Jin Cho[2]

Received: 10 April 2017 / Accepted: 15 January 2018 / Published online: 31 January 2018

Abstract
The application of ICT technology to agriculture has raised interest in smart farm systems that can remotely manage growing environments. Data transmission in smart farm systems uses wireless networks such as ZigBee and Wireless LAN and TCP/IP based wired networks. And also use the P2P network to share smart farm system data with other smart farm systems. There are security vulnerabilities that may arise in information communication environment in smart farm system unlike traditional farms, the smart farm system automatically stores and manages data for growth environments such as temperature, humidity, and CO_2. Therefore, an attacker can use a security vulnerability to manage temperature, humidity, and Co_2, which can cause significant damage. In this paper, we propose an authentication method that performs minimum encryption and decryption operations by combining session key and public key to securely control smart farm system. The proposed authentication method reduces the encryption/decryption time, the registration time, and facilitates the use of the smart card with low computing performance by using the session key compared with the existing authentication method.

Keywords Smart farm device authentication · P2P-based smart farm · Certificate · Security · Authentication

1 Introduction

Recently, smart farms that can manage the growing environment of crops by applying ICT technology to greenhouses have been widely used. Smart farm technology is being developed around Europe, and smart farming in the Netherlands is at the top of the world. In Korea, the RDA is focusing on the development of Korean smart farm models suitable for domestic environment [1]. The smart farm is a farm where ICT technology can be used to properly maintain and manage the growth environment of crops and livestock. In smart farm, devices are installed in specific locations and extract data such as temperature, humidity, CO_2, etc. and transmit them to other devices or gateways through the network. The devices used in smart farm are RFID, sensors, smart devices, and the gateway sends and receives collected data from the devices. Data send and receive in smart farm uses wireless networks such as ZigBee and Wireless LAN as well as TCP/IP based wired network [2]. And also use P2P networks to share data from each farm with other farms. To share farm data, use a hybrid P2P or pure P2P network depending on the farm type.

In smart farm environment, there are security vulnerabilities that can occur in information communication environment. Unlike traditional farm management, smart farm automatically stores and manages data on the growth environment such as temperature, humidity, and CO_2. Therefore, an attacker can use security vulnerabilities to control the temperature, water supply, and it can cause damage. In recent years, there have been attempts to hack smart farm facilities and attack smart farm environment control facilities in Europe. Security vulnerabilities in such a smart farm can cause serious security problems because once an attacker has successfully authenticated, attacker can take advantage of all services in the smart farm.

Therefore, we propose an authentication algorithm that performs minimum encryption and decryption operations by

This article is part of the Topical Collection: *Special Issue on Convergence P2P Cloud Computing*
Guest Editor: Jung-Soo Han

✉ Han-Jin Cho
hanjincho@hotmail.com

Cheol-Joo Chae
chae.cheoljoo@gmail.com

[1] Korea National College of Agriculture and Fisheries, Kongjwipatjwi-ro, Wansan-gu, Jeonju, Republic of Korea

[2] Department of Smart Mobile, Far East University, Eumseong, Republic of Korea

combining session key and public key in order to secure control device in smart farm. The proposed authentication method reduces the number of encryption/decryption times and reduces the registration time compared with the previous authentication algorithm. We also used session keys to improve the utilization of smart farm devices with low computing power. This paper is organized as follows. In the section 2, analyze P2P network and smart farm structure. And the section 3, describes the design part of the proposed system. In the section 4, describes the performance evaluation of the proposed system. In section 5, a conclusion is given.

2 P2P-based smart farm system

2.1 P2P networks

P2P is a network in which peers share some of the hardware resources such as processing power, storage space, and content. In a client/server network, clients can't share resources, but in a p2p network they can share peer resources. Therefore, P2P network is a network in which the peer can act as a server or a client. The method of classifying the P2P network can be divided into a file sharing model and a CPU sharing model according to the shared resources, and can be divided into a pure P2P and a hybrid P2P according to a sharing method. Since pure P2P does not have a central management server, the traffic is not concentrated in one place and the P2P network is formed firmly. However, efficiency is low in data transmission or peer search. Most P2P applications use pure P2P or hybrid P2P [3–5]. Figure 1 shows configuration of P2P networks.

Hybrid P2P is a method to control users' shared file list and so on at the central server in order to communicate with each other efficiently and communicate necessary information. The central server only provides the name of the peer that is already connected to the connecting peer, and connection establishment and communication are performed by the peers. The computer only acts as a server and client for file transfer. This method can increase search speed and search success rate. However, if the number of concurrent users increases, central server expansion should be considered, and the load on the central server is also increased. In addition, the characteristics of the hybrid P2P model require a system account manager for index management for search.

2.2 Network-based smart farm system

In smart farm, IoT technology can be used to monitor the growth environment information such as temperature, humidity, and CO_2 and to control the environment that can be optimized for the growth environment [6–8]. Sensors attached to the smart farm acquire the growth environment data and transmit it to the gateway that manages the sensors through the wired and wireless network. The wired and wireless networks used by the sensor to transmit the growth environment data in the smart farm use IEEE802.3, PLC, RS-232C in case of wire, IEEE802.15.4, IEEE802.15.4e, IEEE802.15.4 in case of wireless, .11n. In order to control the growth environment in smart farms, there are control facilities for each facility, and an information management system is included to provide optimal growth environment. Figure 2 shows smart farm configuration [9–13].

The ITU-T SG13 Group, which is responsible for the standardization of the future network and cloud sector, has developed a standard (ITU-T Y.2238) for network-based smart agriculture outline from 2012. The purpose of the standard development is to define the convergence between agriculture and ICT and the essential considerations for applying IT to agriculture. Applying information and communication technology and automation technology to agriculture has been applied to the production stage such as greenhouse automation mainly because of increase of production quantity and improvement of quality. However, in recent years, there has been a demand for expanding the field of smart agriculture as the interest in the whole cycle process from the production to the distribution and consumption stages has increased. Therefore,

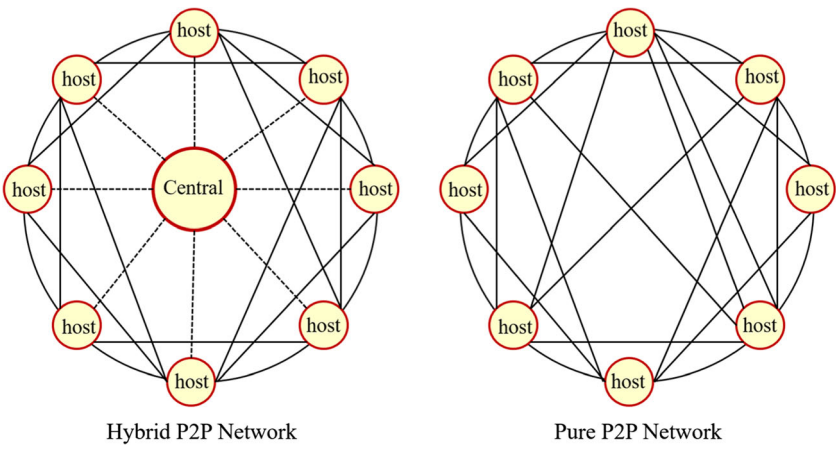

Fig. 1 Configuration of P2P networks

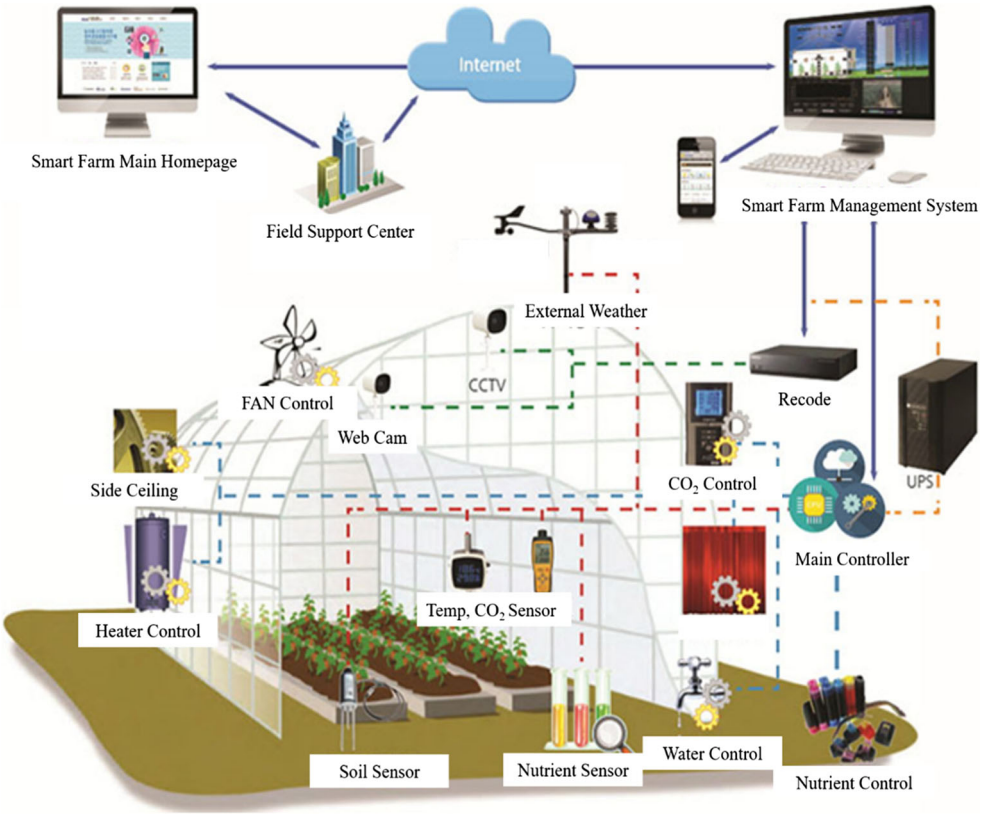

Fig. 2 Example of smart farm

as shown in Fig. 3, the standard has been developed to consider interactions with various entities related to the entire field of agriculture.

Agricultural producers produce agricultural products and supply them to consumers. Methods for producing agricultural products can be divided into land, greenhouse, and plant. Smart farm services provide services at the production, consumption and distribution stages. It can be divided into content service and remote automation service depending on the type of service. The content service provides the optimum growth conditions of the big data base and the forecast of the agricultural product price information, and the remote automation service provides the environment to cultivate agricultural products remotely. The logistics agent provides the consumers with the agricultural products harvested by the agricultural producers. Depending on the method of providing

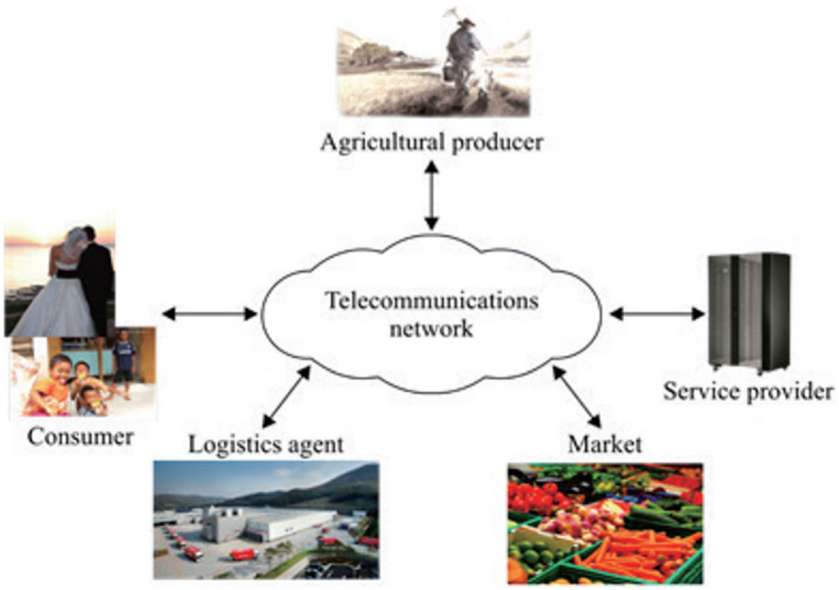

Fig. 3 Network-based smart agriculture overview

agricultural products, it can be subdivided into direct deal, wholesale, and online. Consumers are the final consumers who consume agricultural products through methods such as distributors, producers and direct dealers, and can be divided into general individual and group consumers, and consumers for business purposes according to the purpose of consumption [14–18].

ITU-T Y.2238 defines a network-based smart farm and defines the smart farm reference model, services and network functions required for the smart farm. Since the network enables participation of various service objects, the network-based smart farm service defines a reference model that can involve various objects as well as producers as shown in Fig. 4.

3 Design of smart farm device authencitciaon in P2P-based smart farm system

3.1 Enhanced secure device authentication method

Device authentication is required to monitor and control growth environment data in smart farms. In smart farms, device authentication can be exploited by an attacker. In smart farm, authentication information attacks can create a security problem because they can use sensors and controllers installed in a smart farm with authentication information. Therefore, we proposes a new authentication method that combines public key based authentication method and minimum public key based authentication method. This is a method of indirectly authenticating the contents authenticated by the internal smart farm device($F_{Device1}$) by delivering the device advertisement sent from the external smart farm device($F_{Device2}$) to the internal smart farm device($F_{Device1}$). The user sends an electronic signature to the internal smart farm device, and the internal smart farm device verifies the validity of the public key by accessing the authentication authority and authenticates the digital signature. In this method, internal smart farm devices can authenticate users and external smart farm devices. The digital signature of the user provides a non-repudiation function for the location information registered by the user, thereby managing and controlling the use of network resources. In the case of an internal smart farm device, it is authenticated by sending an electronic signature to the external smart farm device and creating a MAC for the user. Therefore, all participants involved in the new location registration process can be authenticated. The authentication procedure for the proposed method is shown in Fig. 5.

The user and the internal smart farm device share a secret key. Then, the external smart farm device advertises the external smart farm device using the electronic signature signed with its own private key and the certificate of the external smart farm device. In order for the user to register with the external smart farm device, M_2, the electronic signature signed with the user's private key, and the user's certificate are transferred to the external smart farm device. M_2 includes the request, the external smart farm device IP address, the internal smart farm device IP address, the user IP address, the user temporary address, the internal smart farm device random number, and the user random number. The external smart farm device transmits to the internal smart farm device including M_2 received from the user, electronic signature signed with the user's private key, user certificate, and user random number. The internal smart farm device verifies the user certificate

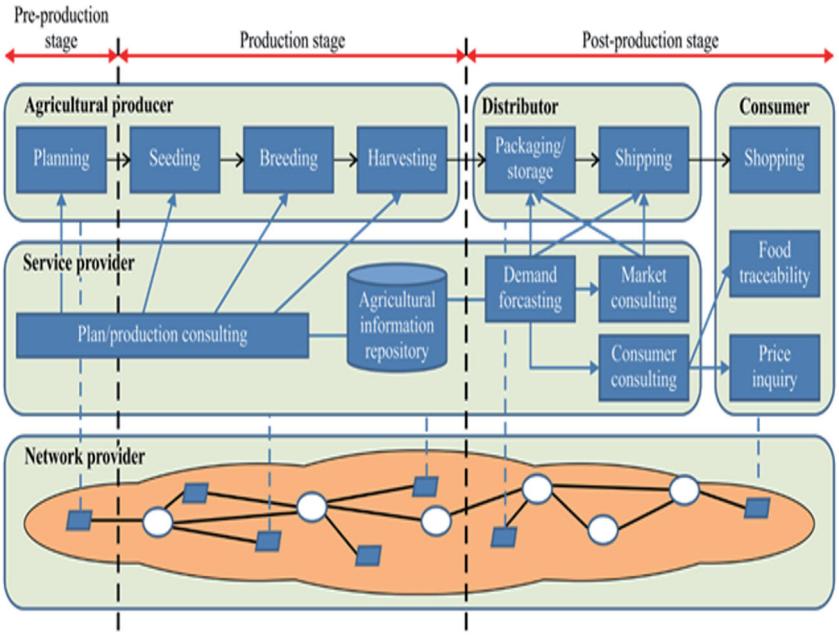

Fig. 4 Smart agricultural reference model

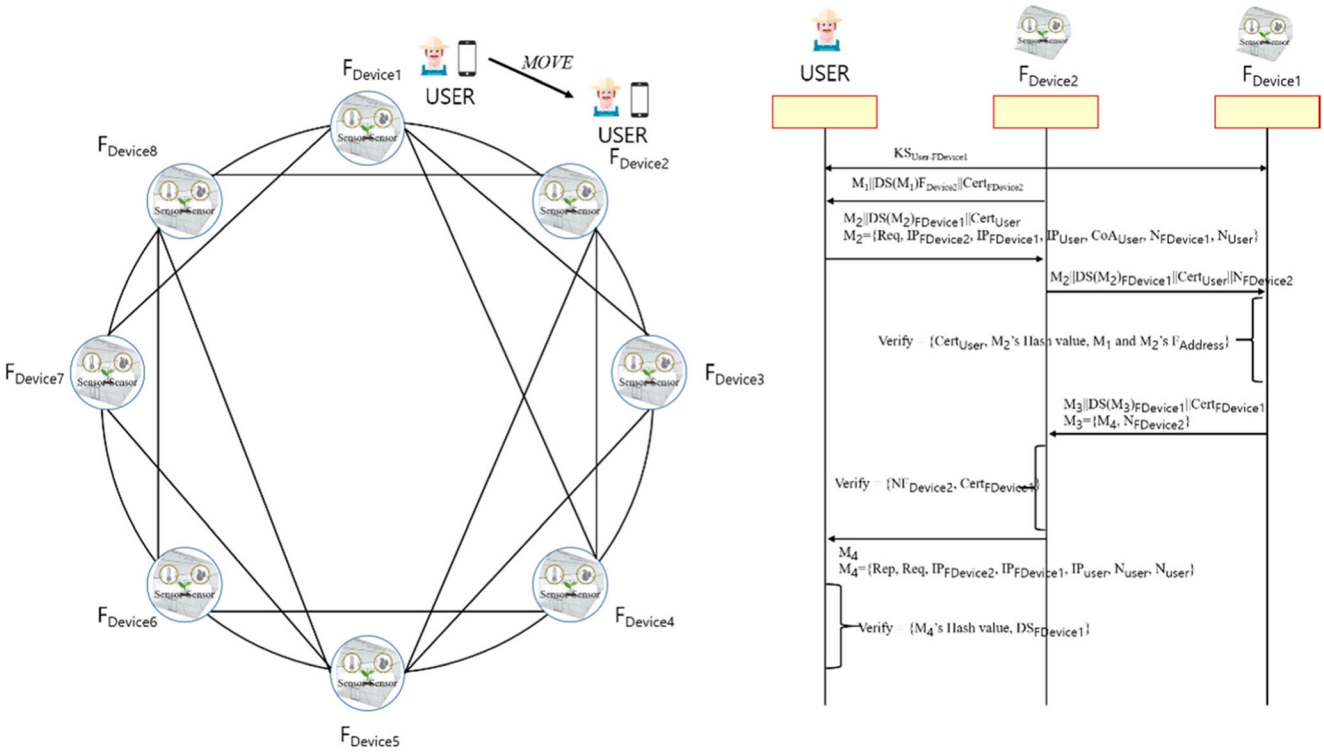

Fig. 5 Proposed system configuration and authentication method

using information received from the external smart farm device and verifies the hash value of M_2. Then, it verifies whether the addresses of the external smart farm device included in M_1 and M_2 are matched and verifies the certificate and digital signature of the external smart farm device. If the verification is successful, the internal smart farm device sends the external smart farm device an electronic signature signed by the M_3, internal smart farm device private key, and internal smart farm device certificate to the external smart farm device. M_3 includes M_4 and external smart farm device random numbers. The external smart farm device verifies its random number among the contents received from the internal smart farm device and verifies the internal smart farm device certificate and digital signature. When the verification is successfully completed, the external smart farm device sends the M_4 to the user. Then, the user verifies the hash value of M4 and verifies the digital signature value of the internal smart farm device.

In the proposed method, the user generates a digital signature using private key and includes the digital signature in the registration request. The user includes a digital signature and a certificate in the original text. However, because you have issued certificates in advance, you do not need to access the authentication authority when signing. The internal smart farm device receives the digital signature and prove it and preserves it as proof of the user's service request. The registration request uses digital signature, but the registration response depends on the MAC, so even when the user receives the registration response, it does not need to access the authentication authority when authenticating by authenticating with the secret key. This method can increase the utilization by minimizing the user's public key usage.

3.2 Device certificate issuance method

Authentication systems such as authentication server, security service, and LDAP were used by IBM compatible PCs for smart farm device authentication. The system configuration was constructed using Windows Server and Linux. And implemented API and interface using Java. The certificate profile related to the standard items and extensions of certificates for smart farm device authentication service is defined in accordance with IETF PKI X.509 working group recommendation RFC3280 as shown in Fig. 6, and the details of each item are as follows [19].

- Version: The version of the certificate
- Serial Number: The unique identifier of the certificate associated with the certificate.
- Signature: An object identifier of the algorithm used to compute the digital signature for the certificate, an identifier of the algorithm.
- Issuer: The Designated Name of the issuing CA that is named according to the X.500 recommendation. Since it can't be registered as a public issuer, it is designated as "Smart Farm DN" and processed.

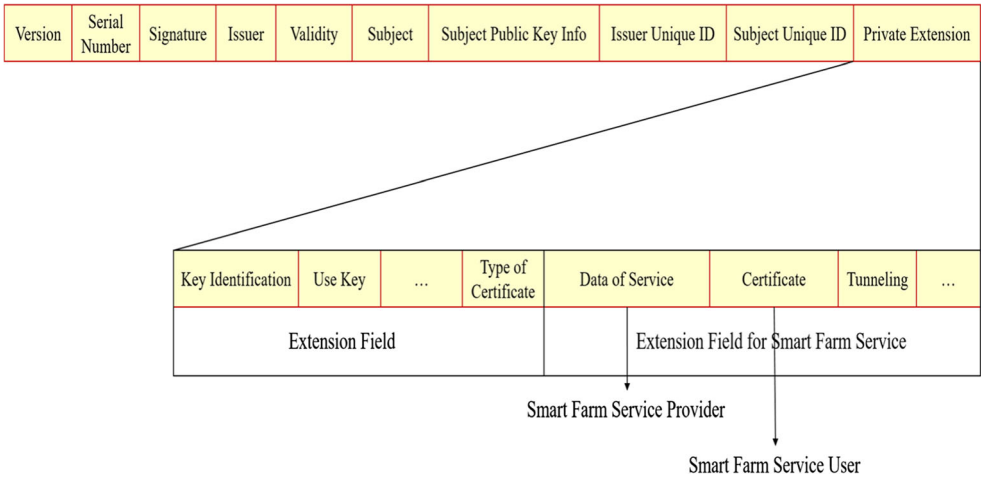

Fig. 6 Configuring X.509 public key certificates for smart farm services

- Validity: The validity period of the certificate for which the certificate is not revoked, expressed as International Coordinated Time.
- Subject: Must be entered if the DN of the certificate owner does not define an individual name referring to the extension. Enter and process information about smart farm devices or users.
- Subject Public Key Info: The encryption algorithm identifier of the subject public key.
- Issuer Unique ID: Can be omitted as the unique identifier of the issuer of the certificate. Skip for smart farm authentication.
- Subject Unique ID: The unique identifier of the certificate owner. Handled by smart farm device user ID.
- Private Extension: Additional information needed to configure other certificates is added to add key and policy related information such as key identifier, key usage, private key usage period, CRL distribution point, certificate policy, basic constraint information, etc.,

4 Evaluating the performance of the proposed system

The authentication system proposed in this paper satisfies the information security factor required for providing smart farm services. Digital signatures and data exchange confidentiality attack security is as follows. There is no attack method for RSA commonly known for attacking digital signatures. When an attacker has e and n values, n must be factorized to get d values. Even if NFS is used as the fastest factorization method in large numbers larger than 110 digits, Brute Force attack on RSA requires time as shown in Table 1.

For a hash function such as SHA-1, the degree of security is determined by whether it has randomness and no collision. The attacker will try to find m for m satisfying H(m) = H(m'), but no specific attack method has been found. A Brute Force attack takes 1.08E22 years to find a digest value conflict in SHA-1 for a machine that processes 1,000,000,000 messages per second.

To generate a hash value, an average of 0.20 *ms* is required. To prove the hash value, 0.15 *ms* is required. Since the mechanism for generating and verifying the hash value is the same, there is no difference. Encryption/decryption operations are the same. In the case of digital signatures, it takes 8 *ms* to generate the digital signature and 1 *ms* to prove it, so it is more necessary than the time to generate and verify the hash value. The reason why the digital signature takes at least 51 times and the maximum of 48 times as compared with the hash value making process is because the public key function itself has a complicated structure as compared with the hash function. Public key computation is computationally expensive and requires a lot of resources and consumes power. In addition, since the encryption/decryption time is long and the process of issuing the public key of the user and storing it in the key store and issuing the other party's public key and using it for decryption is required, the calculation cost is higher than the secret key calculation.

The total registration time is the time when the user moves from the internal smart farm to the external smart farm and registers the location information with the internal smart farm device using the external smart farm device. The total registration time consists of the registration request, the registration response time, the node processing time including the smart farm device table update time, the encryption/decryption time

Table 1 Brute Force RSA Factoring MIPS

Key size	MIPS-year
512	30,000
768	200,000,000
1024	300,000,000,000
2048	300,000,000,000,000,000,000

required to generate the hash value or digital signature, and the message delivery time between the user and the smart farm device.

Figure 7 shows the total authentication time per authentication mechanism and the authentication time in the proposed system. The total registration time is 37 times in the case of the public key method and takes 134 *ms* in comparison with the secret key method. This time is considerably longer if the handoff service or service at the TCP/UDP layer is followed after the new registration process is done at the network layer. It can be seen that the public key is difficult to use despite the fact that it increases security. The minimum public-key-based approach that minimizes the use of public keys while maintaining security is only 51% less than the public key-based approach. However, since there is no anti-repudiation service in this case, the proposed method allows smart farm device to perform digital signature. In the proposed scheme, the registration time is reduced by 58% compared to the public key based method, and the performance is improved. The digital signature added for the non-repudiation service is increased by 119% compared to the minimum public key. Provide necessary services while providing non-repudiation services while minimizing efficiency.

Figure 8 shows the total authentication time, host process time, and encryption time according to the authentication method. In a secret key based scheme, most registration time is due to the propagation delay time between devices. Encryption/decryption time using secret key is very short. In the public key based scheme, the time required for encryption/decryption using the public key is increased by 980 times as compared with the secret key, so that the public key process cost is high. However, the proposed method reduces authentication, processing, and encryption/decryption time by about 50% compared to the public key method.

Figure 9 compares the processing time and the encryption/decryption time when the public key method and the proposed method are applied to the existing registration method and the proposed local registration method. The overall registration time can be divided into authentication time, registration time, and session key distribution time. Therefore, we show that the performance is improved

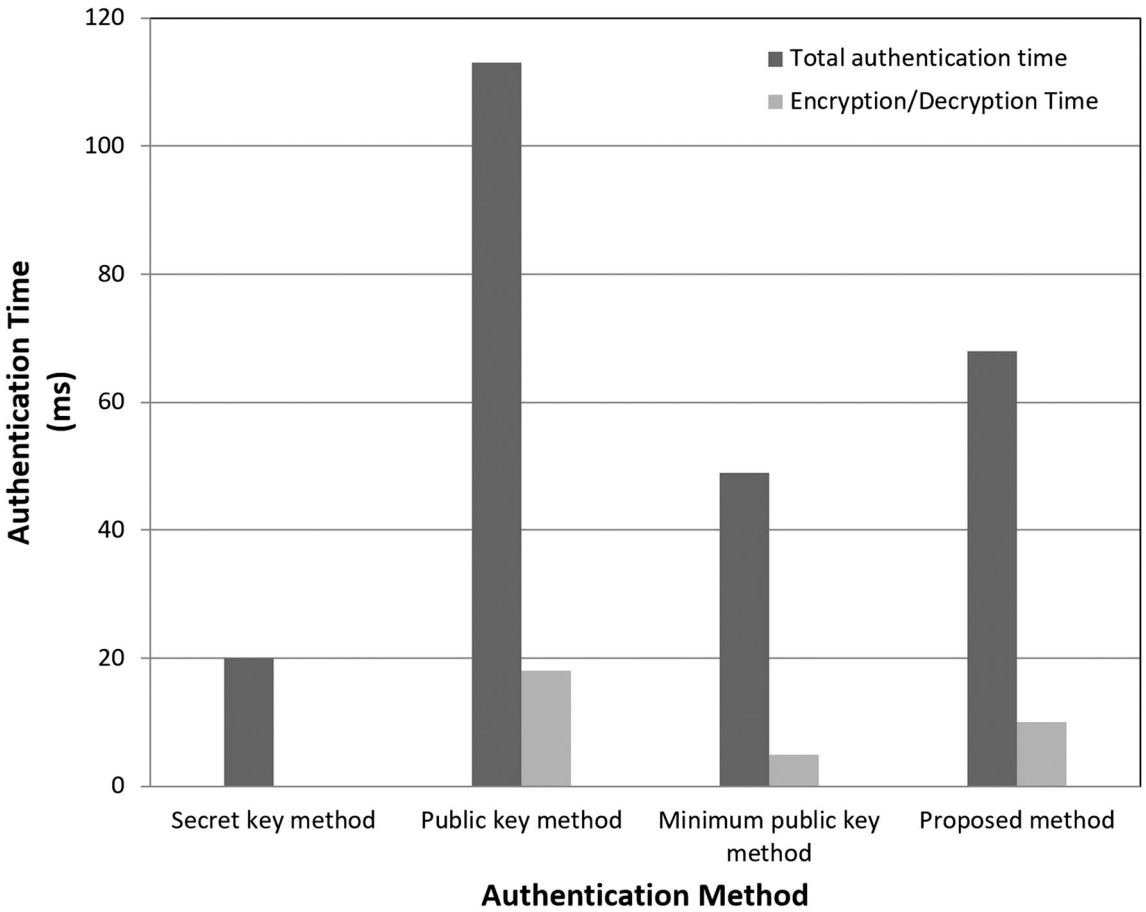

Fig. 7 Total registration time and authentication time

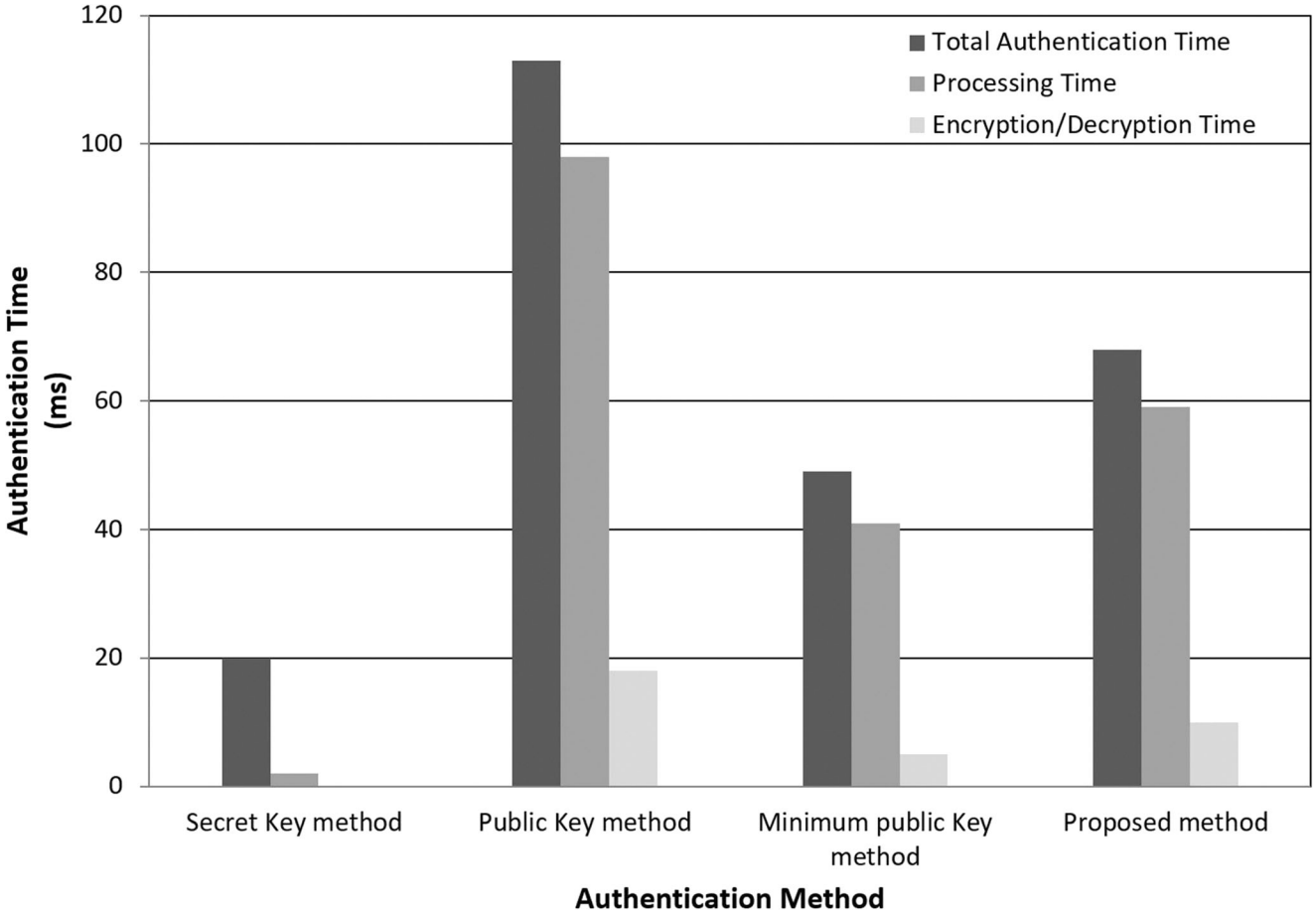

Fig. 8 Authentication, processing, and encryption/decryption time comparison results

compared to the existing authentication and registration method. In addition, it can be confirmed that the proportion of encryption/decryption and digital signatures in the entire registration time is relatively small.

In addition, the performance of the cryptographic security required for the information protection service is examined in order to evaluate the performance of the proposed authentication method, and the performance of the proposed authentication method is analyzed as follows

- Authentication: In this paper, the key distribution problem is solved by issuing and managing the certificates needed for mutual authentication through the authentication server. The public key algorithm is capable of authenticating the owner of the key because of its mathematical relationship and having the characteristics of the key pair, and can perform a denial-blocking function to prevent denial of the digital signature through public key encryption.
- Confidentiality: In the proposed authentication method, Secure Random value for key, data and session key synchronization is encrypted by using certificate-based private/public key and temporary secret key. In other words, the Secure Random value generated by the smart farm device and the server is combined to generate a 16-byte session key for synchronization. The synchronized session key is used for digital signature and message encryption after authentication.
- Non-repudiation: Since the authentication method in the proposed authentication method uses the existing authorized certificate method, it can be authenticated to the key owner because of the mathematical relationship and the characteristics of the key pair. The digital signature through the key encryption can perform a denial-blocking function which does not deny the digital signature.
- Access Control: Access control means to allow only selected recipients to access the information. Access control in the public key infrastructure allows access information to be sent only to the intended recipient by using the public key/secret key, so that the access information from the recipient can be checked to select only authorized users and control access to the information is. The access control service can provide smooth information service and can protect the system from external illegal access threats.

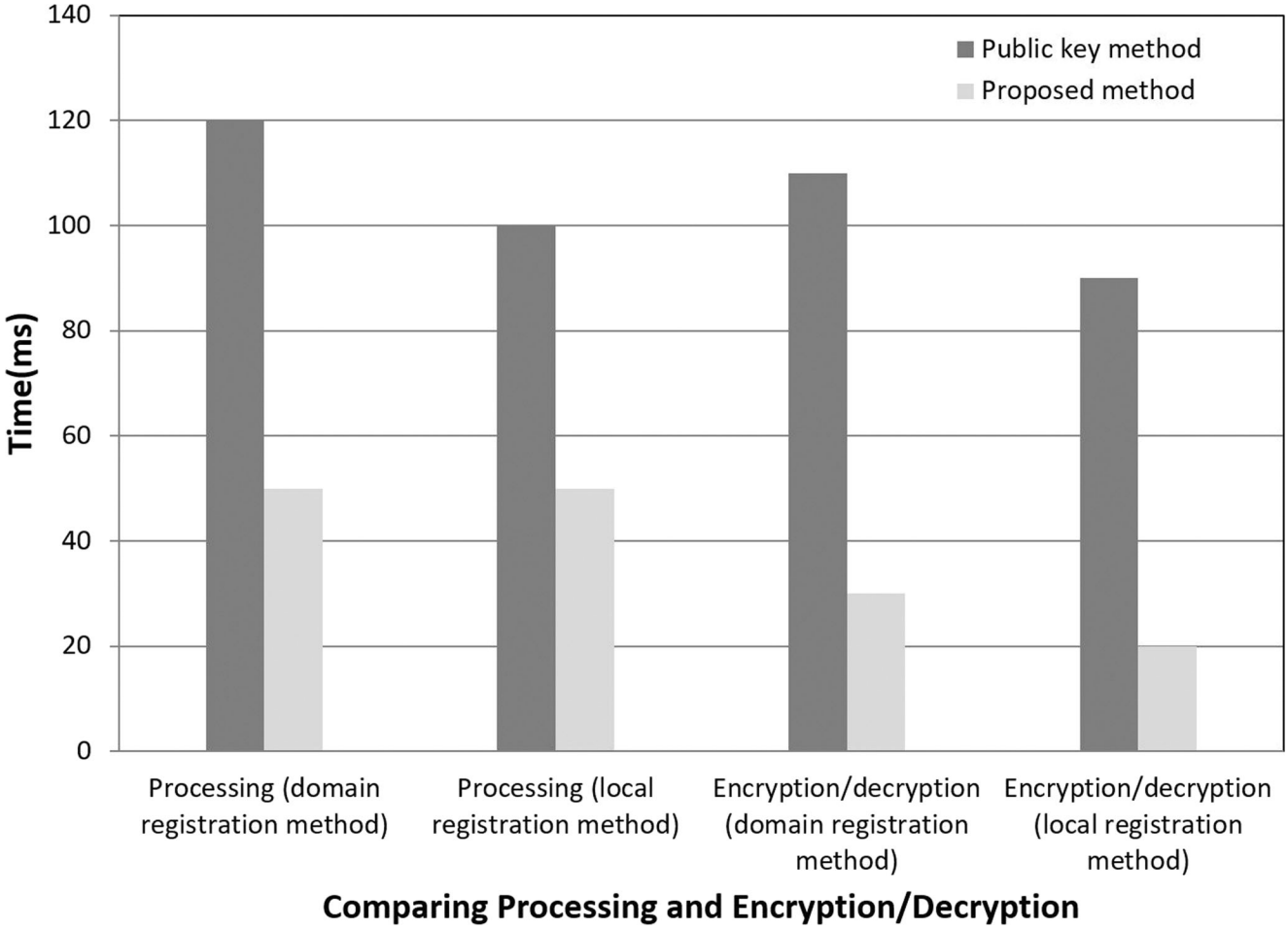

Fig. 9 Comparison of processing time and encryption/decryption time

5 Conclusions

In Smart Farm, ICT technology is used to acquire and control data on the growth environment. In this paper, we propose smart farm authentication method to securely control smart farm, and solve the problem in existing smart farm environment. To accomplish this, we propose an authentication scheme that minimizes the encryption / decryption operation by combining the session key and the public key in order to break the existing heavy authentication scheme, and modified the authentication scheme by the registration scheme for faster throughput. The proposed smart farm authentication method reduces the number of encryption/ decryption times, reduces the registration time, and uses the session key to make it easier to use in a smart farm that has low computing capability compared to the existing authentication method.

The proposed method reduces the performance degradation of smart palm devices by including the MAC using the secret key in the registration response sent from the internal smart farm. The benefit of hash functions is great in environments where compute is reduced to a minimum such as smart farm devices. The internal smart farm device does not need to prove the external smart farm when receiving the smart farm and does not have to directly authenticate with the external smart farm device during the registration process. The internal smart farm device receives the registration request and authenticates the external smart farm device. If authentication is successful, it sends the registration reply to the user. The smart farm user indirectly authenticates the content of the external smart farm device by receiving the registration reply. This authentication method is expected to prevent security and authentication problems in smart farm environment.

Acknowledgements This work was supported by the 2017 Far East University Research Grant (FEU2017S05).

References

1. Yong-Byum L (2016) Smart farm policy and trend of technology in Korea. Institute of Control, Robotics and Systems 22(3):58–64

2. Dong-Hee K (2013) The security for IoT service. Korea Institute of Communication Sciences 30(8):53–59
3. Park H-s (2006) ProposalofHybridP2P-basedOn-LineLearningMode. Graduate School of Education Chosun Universiy, Major in Information and Computer Science Education
4. Cheol-Joo C et al (2016) A privacy data leakage prevention method in P2P networks. Peer-to-Peer Networking and Applications 9(3): 508–519
5. Gary Chan S-H, Mea W (2015) Email author. Jacob Chakareski, Bin Wei, "Special Issue on P2P Cloud Systems" 8(2):241–243
6. Hyun-Woo Je OY (2012) Remote monitoring system of photovoltaic inverter using Zigbee communication. Korean institute of information. Technology 10(2):94–101
7. Kang M (2014) Design of Multi-Node Real-Time Diagnostic and Management System Using Zigbee Sensor Network. Institute of Electronics Engineers of Korea 51(6):1280–1289
8. Chenyan Zhang, et al. (2013) Topology performance analysis of Zigbee network in the smart home environment. 2013 5th IHMSC international conference
9. Kaewmard, Nattapol, and Saiyan Saiyod (2014) Sensor data collection and irrigation control on vegetable crop using smart phone and wireless sensor networks for smart farm." Wireless Sensors (ICWiSE), 2014 I.E. Conference on IEEE
10. Kanjilal D et al (2014) Smart farm: Extending automation to the farm level. International Journal of Scientific & Technology Research 3:7
11. Jindarat, Siwakorn, and Pongpisitt Wuttidittachotti (2015) Smart farm monitoring using Raspberry Pi and Arduino." Computer, Communications, and Control Technology (I4CT), 2015 International Conference on IEEE
12. Ryu, Minwoo, et al. (2015) Design and implementation of a connected farm for smart farming system. SENSORS, 2015 IEEE
13. Hwang SI, Ju SY, Ju JM (2015) A study on ICT-based smart farm factory integration platform. Proc Korea Inst Commun and Inf Sci Winter (2015):225–226
14. Young PJ (2016) Smart agricultural standardization trend. The Journal of The Korean Institute of Communication Sciences 34(1):70–75
15. ITU-T Y.2238 (2015) Overview of Smart Farming based on networks
16. ITU-T Y.PSF (2015) Functional model for production service of Smart Farming
17. ITU-T Y.POPS (2015) Postproduction Service of Smart Farming on the Network
18. ITU-T Y.ISG-FR (2016) Framework of IoT-based Smart Greenhouse Service
19. http://www.ietf.org (2002) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

Cheol-Joo Chae received his Ph.D. degree in computer engineering from Hannam University, Daejeon, Korea, in 2009. From 2009 to 2013 he was a senior member of the research staff in the ETRI, Daejeon, Korea, where he did research on network communication system. From 2013 to 2016 he was a senior member of the research staff in the KISTI, Daejeon, Korea, where he did research on information system. Since then, he has been a Professor with Korea National College of Agriculture and Fisheries.

Han-Jin Cho received the B.S., M.S. and Ph.D. in Computer Engineering from Hannam University, Korea in 1997, 1999 and 2002. Since then, he has been a Full Professor with the Department of Energy IT Engineering, Far East University, Korea. He was awarded a certificate from the Ministry of Knowledge Economy, Korea in 2012. His main research interests include Mobile Applications and Network Security.