This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things

Pengfei Hu, *Student Member, IEEE,* Huansheng Ning, *Senior Member, IEEE,* Tie Qiu, *Senior Member, IEEE,* Houbing Song, *Senior Member, IEEE,* Yanna Wang, and Xuanxia Yao

***Abstract*—Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification and resolution raises the demands of computation, communication and storage capabilities. Therefore, we have proposed the fog computing based face identification and resolution framework to improve processing capacity and save the bandwidth. However, there are some security and privacy issues brought by the properties of fog computing based framework. In this paper, we propose a security and privacy preservation scheme to solve above issues. We give an outline of the fog computing based face identification and resolution framework, and summarize the security and privacy issues. Then the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are proposed to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution. Finally, we implement a prototype system to evaluate the influence of security scheme on system performance. Meanwhile, we also evaluate and analyze the security properties of proposed scheme from the viewpoint of logical formal proof and the CIA (confidentiality, integrity, availability) properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation.**

***Index Terms*—Internets of Things (IoT), fog computing, face identification, face resolution, security, privacy preservation.**

I. Introduction

THE Internets of Things (IoT) realizes the interconnection and intercommunication among ubiquitous things, and promotes the natural and seamless convergence of physical space and cyber space[1-3]. More and more physical objects, including humans, sensors, mobile devices, are connected into Internet to be an element of IoT in various applications[4, 5]. As a special physical object, humans are also frequently interacting with cyber space[6]. Currently, Internet of people (IoP) based applications are attracting even more attention[7]. The identification and resolution of human is the crucial technology for ensuring the identity consistency between physical space and cyber space in these applications[8].

The traditional identification and resolution applications are mainly based on ID code, for example, electronic product code (EPC)[9], ubiquitous identification (uID)[10], European article number (EAN), etc. However, in some IoT scenarios, there are some physical objects which are unattached ID or attached unreadable and un-trusted ID[11]. In this situation, some properties (e.g., biometric, space-time information) can be used as identifier of physical object[12, 13]. Face is widely used for identification and resolution of human. The face identification process refers to generating face identifier and associating personal identity information with the identifier. The face resolution process refers to searching personal identity information or obtaining related personalized service by face identifier. Different from ID code which mainly consists of numbers and alphabets, face identifier needs to be generated by performing some facial image processing algorithms, including face detection, preprocessing, feature extraction and face identifier generation. In the face resolution process, face identifier matching algorithm need to be performed[14]. In addition, the size of face identifier is larger and its structure is more complex than ID code. Therefore, the processes of face identification and resolution need more computation, communication and storage capabilities[15].

Some researchers have adopted cloud computing to improve processing and storage capacity[16, 17]. However, in cloud computing architecture, various applications need to request services on cloud. Bandwidth will become a bottleneck in this centralized processing architecture with the increase of applications and users[18, 19]. Fog computing is an emerging computational and service model[20]. It makes full use of the computation capability of network edge devices to provide efficient service[21]. We have proposed a face identification and resolution scheme based on fog computing[22]. By applying the task partitioning, some computing tasks are offloaded from cloud to fog nodes[23]. While powerful computation and storage capabilities are provided, fog computing model can notably reduce network transmission load and save bandwidth.

Though fog computing properly meets the requirements of the computation, communication and storage in face identification and resolution, there are some security and privacy issues that need to be solved urgently[24-27]. Face identification and resolution applications usually refer to personal privacy

P. Hu, H. Ning, Y. Wang, X. Yao are with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China (e-mail: hupf7721@126.com; ninghuansheng@ustb.edu.cn; wang_yan_na@sina.com; yaoxuanxia@163.com).

T. Qiu is with the School of Software, Dalian University of Technology, Dalian 116024, China (e-mail: qiutie@ieee.org).

H. Song is with the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136, USA (e-mail: Houbing.Song@mail.wvu.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

information which is crucial to users. Different from ID code, once face identifier or personal registration information is stolen, these applications based on face identification will be confronted with huge security threat. So research on the security and privacy preservation scheme for face identification and resolution has important application value.

Fog node devices which are close to end users are usually deployed in some places where protection and surveillance are relatively weak. So they are vulnerable to security challenges[28]. Some traditional attack methods become available to fog computing framework in order to realize malicious purposes, such as, man-in-the-middle attack[29], eavesdropping, and data hijack[30], etc. Our fog computing based face identification and resolution scheme is mainly comprised of fog nodes, data transmission between cloud and fog, cloud. We will analyze and research security and privacy issues on these three places.

In our framework, face identifier and personal identity information, which are sensitive data, need to be transmitted frequently on fog and cloud. So we discuss the security and privacy issues of this framework from confidentiality, integrity and availability. And identity authentication scheme among devices, data encryption scheme, and data integrity checking scheme are designed to solve these security and privacy issues. With the help of proposed scheme, our framework can provide efficient and secure face identification and resolution service.

This paper proposes a security and privacy preservation scheme for fog computing based face identification and resolution framework in IoT. The main contributions of this paper are as follows:

1) The security and privacy issues faced in fog computing based face identification and resolution framework are analyzed and summarized according to the characteristic of this framework.
2) The identity authentication scheme, data encryption scheme, and data integrity checking scheme are proposed to meet the demands of confidentiality, integrity, and availability in the processes of face identification and face resolution.
3) The prototype system using proposed security and privacy preservation scheme is implemented to demonstrate that the computation and communication overhead is small. And formal proof with the BAN (Burrows-Abadi-Needham) logic and security properties analysis are presented to verify and analyze the security of the proposed scheme.

The rest of this paper is structured as follows. Section II reviews the related works on security and privacy preservation issues and solutions in face identification and resolution applications. Section III presents the security and privacy issues of fog computing based face identification and resolution framework. Section IV proposes the security and privacy preservation scheme for fog computing based face identification. Section V proposes the security and privacy preservation scheme for fog computing based face resolution. Section VI presents the experiment and performance analysis for proposed security and privacy preservation scheme. Section VII concludes this paper.

II. Related Work

The security and privacy issues of face identification and resolution play a significant role in ensuring cyber security about human in IoT scenario. Researchers have already conducted some research work in this field. Some security and privacy-preservation schemes have been presented.

Osadchy et al.[31] proposed a secure and privacy-preserving face identification system (SCiFI). A secure face identification protocol was presented by using homomorphic encryption and oblivious transfer. Though it could run in the situation of near real-time, this scheme was suitable for face identification with few number of face data. For a relative large database, the computational cost would increase linearly.

Huang et al.[32] presented a novel matching protocol for biometric identification. It used a more efficient protocol based on the ciphertexts packing and additive homomorphic encryption to compute the Euclidean distances of vectors. This scheme could improve identification efficiency, while disclosed any private biometric data. However, this scheme need to transmit whole encrypted database from server side to client to perform biometric identification. With the increase of database size, the computation and communication costs would increase linearly.

In above work, researchers proposed some security and privacy-preservation schemes for face and other biometric identification to ensure the system security. However, the common problem facing in these schemes were that the computation and communication costs would grow linearly with the increase of database size. So some researchers considered to solve this problem by cloud computing.

Haghighat et al.[33] proposed a cloud computing-based and cross-enterprise biometric identification system (CloudID) with privacy-preservation. The confidential information of users was linked with their biometrics and stored by encryption. A k-d tree structure in the searchable encryption algorithm was proposed to implement encrypted search query. This scheme not only met the demands of computation and storage capabilities, but also provided a privacy-preserving and trustworthy biometric identification scheme.

Bommagani et al.[34] presented a secure face recognition framework based on cloud computing. Some recognition tasks were performed on cloud, and they were divided into multiple tasks to be executed in parallel. Meanwhile, based on Local Binary Pattern (LBP) feature template generation model, a cancelable face template generation algorithm was proposed to preserve the privacy and security of biometric data.

Yuan et al.[35] proposed a novel biometric identification scheme with privacy preservation to securely move most of the identification operations to cloud servers. The cloud servers implemented identification service in encrypted database by using the credential which was generated by database owner. This could ensure that the private biometric data was confidential to cloud.

Xia et al.[36] proposed a privacy-preserving content-based image retrieval (CBIR)scheme in cloud computing to prevent the leakage of sensitive images, e.g., personal images. The extracted feature vector of image was protected by the secure

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

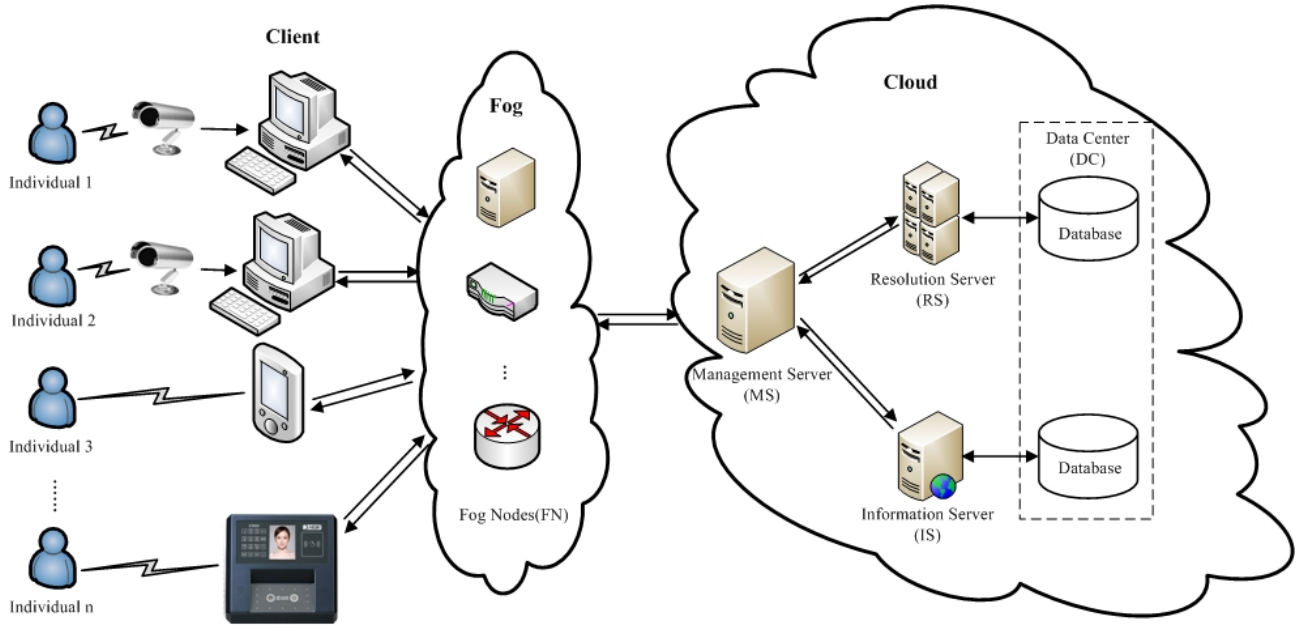

Fig. 1. The fog computing based face identification and resolution framework

kNN algorithm, and image pixels were encrypted by a standard stream cipher. In addition, a watermark-based protocol was proposed to prevent illegally copy and distributions.

These security and privacy-preservation schemes of face and biometric identification based on cloud computing remarkably improved the processing capacity of system, while ensuring the security. But the problem of bandwidth was still not resolved. So we proposed a fog computing based face identification and resolution framework. The characteristics of fog computing architecture determined that it faced new security and privacy challenges.

Lee et al.[37] analyzed and surveyed the potential security and privacy problems in fog computing. It mainly included man-in-the-middle attack, intrusion detection, malicious detection technique, malicious fog node problem, data protection, data management issues. But specific solutions were not presented in the article. Yi et al.[38] surveyed the security challenges of fog computing, for example, authentication, network security, secure data storage and computation. They also analyzed the privacy issues in data, usage, and location.

Stojmenovic et al.[39] thought that the main security issues were authentication at different levels of fog nodes. The public key infrastructure (PKI) and authentication techniques based on Diffie-Hellman key exchange protocol could be used to solve the authentication problem. They took the man-in-the-middle attack as an example to study and discuss the security problems of fog computing. By examining the memory consumption and CPU utilization of gateway, it was proofed to be a stealthy attack and difficult to address.

III. Security and Privacy Issues of Fog Computing Based Face Identification and Resolution Framework

In this section, we introduce the fog computing based face identification and resolution framework. The schedules of face identification and face resolution are presented in detail. In addition, we focus on the analysis of security and privacy issues in the processes of face identification and face resolution based on this framework.

A. Fog Computing Based Face Identification and Resolution Framework

We combine fog computing with face identification and resolution application to provide efficient service in our scheme. The advantages of fog computing are made fully useable to provide powerful computing power and storage capacity. And most importantly, the amount of network transmission is reduced notably and the bandwidth is saved effectively.

In this scheme, some computational overhead is offloaded from cloud to fog nodes by applying the strategy of task partitioning. The algorithms of face detection, facial image preprocessing, feature extraction and face identifier generation are performed to generate face identifier on fog nodes. The face identifier matching algorithm and data storage are performed on cloud which can make full use of the advantage of powerful computation and storage capability. Furthermore, face identifier and personal identity information are independently managed by different servers on cloud. This strategy is convenient for distributed deployment and improves system flexibility.

The framework consists of three parts: client, fog, and cloud. Client is composed of computers, mobile phones, smart terminals, etc. Fog comprises many fog nodes (FN), for example, exchange board, router, gateway, or dedicated server. Cloud is composed of management server (MS), resolution server (RS), information server (IS), and data center (DC). Fig. 1 shows the fog computing based face identification and resolution framework.

The process of face identification refers to transforming the face of an individual in physical space into identifier in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

TABLE I
LIST OF SYMBOLS DEFINITION FOR FACE IDENTIFICATION AND RESOLUTION SCHEME

Symbol	Description
F	The raw facial image of registered individual
inf	The personal information of registered individual
V	The face identifier of of registered individual
ID_{inf}	The identifier of *inf*
F'	The raw facial image of test individual
inf'	The personal information of test individual
V'	The face identifier of test individual
$ID_{inf}{}'$	The identifier of *inf*'

Algorithm 1 The procedure of face identification

Begin

Step 1. Client requests the face identification service.

Step 1.1. Camera acquires facial image of an individual, and sends the raw facial image *F* to client.

Step 1.2. Client registers needful personal information *inf* of the individual.

Step 1.3. Client requests the face identification service to FN and establishes network connection.

Step 1.4. Client sends *F* and *inf* to FN.

Step 2. FN receives *F* and *inf*, and implements face identifier generation.

Step 2.1. For the raw facial image *F*, the algorithms of face detection, facial image preprocessing, feature extraction and face identifier generation are performed to generate the face identifier *V*.

Step 2.2. FN sends *V* and *inf* to MS in cloud.

Step 3. MS receives *V* and *inf*, and respectively sends them to RS and IS to implement identity registration.

Step 3.1. MS allocates an identifier ID_{inf} for *inf*.

Step 3.2. MS sends *V* and ID_{inf} to RS, and sends ID_{inf} and *inf* to IS.

Step 4. RS stores *V* and ID_{inf} into DC, and returns the sign of successful registration to MS.

Step 5. IS stores ID_{inf} and *inf* into DC, and returns the sign of successful registration to MS.

Step 6. MS returns the sign of successful registration to FN. FN also returns this sign to client.

End

cyber space. This identifier is used for ensuring the consistency between the individual in physical space and his/her identity information in cyber space. In this process, face image is acquired firstly. Then the face image identification is performed by these operations of face detection, preprocessing, feature extraction and face identifier generation to generate face identifier. Finally, the face identifier is stored into data center together with personal identity information. The detailed procedure of face identification is shown in Algorithm 1. The list of symbols definition and description for face identification and resolution scheme is shown in Table I.

The process of face resolution refers to finding and obtaining identity information of an individual in cyber space with his/her face in physical space. The face identifier is still used as the bridge to realize seamless convergence between physical space and cyber space. In this process, face image is still converted into face identifier firstly, which is similar to face identification process. Then the identifier is singly matched with all the enrolled identifiers by performing face identifier matching algorithm. Finally, according to the matching result, the personal identity information will be found. The detailed procedure of face resolution is shown in Algorithm 2.

Algorithm 2 The procedure of face resolution

Begin

Step 1. Client requests the face resolution service.

Step 1.1. Camera acquires facial image of test individual, and sends the raw facial image *F'* to client.

Step 1.2. Client requests the face resolution service to FN and establishes network connection.

Step 1.3. Client sends *F'* to FN in fog.

Step 2. FN receives *F'*, and implements face identifier generation.

Step 2.1. For the raw facial image *F'*, the algorithms of face detection, facial image preprocessing, feature extraction and face identifier generation are performed to generate the face identifier *V'*.

Step 2.2. FN sends *V'* to MS in cloud.

Step 3. MS receives *V'*, and retransmits it to RS to execute identity resolution.

Step 4. RS receives *V'*, and implements face resolution.

Step 4.1. The identifier *V'* of test individual is seriatim matched with the identifiers stored in DC by performing face identifier matching algorithm. After successful matching, the corresponding ID'_{inf}, which is paired with the face identifier matched successfully, will be obtained.

Step 4.2. RS returns the ID'_{inf} to MS.

Step 5. MS receives ID'_{inf} and establishes network connection with IS. MS requests the personal information acquisition service to IS.

Step 6. IS acquire the personal information *inf'* about test individual by ID'_{inf}, and return it to MS in specific way, for example, PML document, web service, data file, and so on.

Step 7. MS returns the personal information *inf'* of test individual to FN.

Step 8. FN returns *inf'* to client, and displays it to end users.

End

In our previous work, we have presented the face identifier generation model based on Local Binary Pattern (LBP) feature and face identifier matching algorithm based on Euclidean Distance in detail[40-42]. In addition, Haar face detection algorithm and histogram equalization algorithm have been adopted to perform face detection and facial image preprocessing[43]. In this paper, we still use these algorithms to implement face identification and face resolution.

B. Security and Privacy Issues of Fog Computing Based Face Identification and Resolution Framework

The fog computing based framework provides a novel face identification and resolution scheme. However, there are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

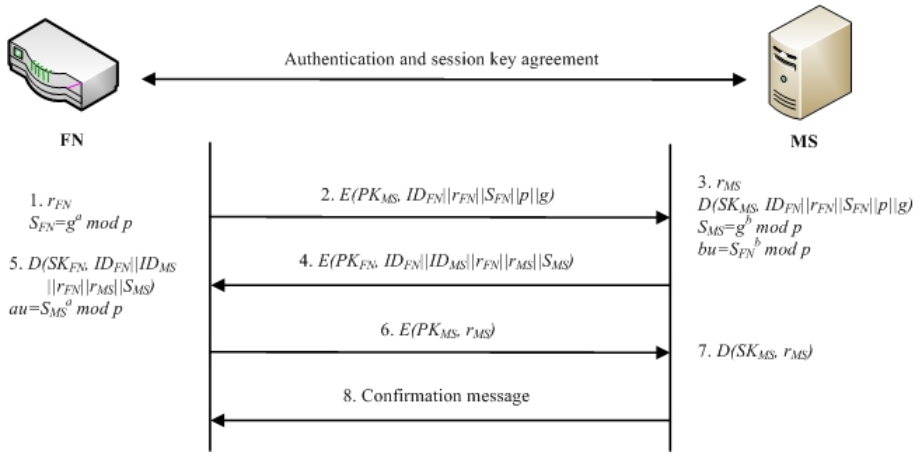

Fig. 2. The authentication and session key agreement process between FN and MS

some potential security threats in practical application. These security and privacy issues are analyzed and discussed from the following three aspects:

1) Confidentiality of data transmission and storage

The function of our framework is to realize the identification and resolution with facial image. These facial and personal identity data, which is sensitive and vulnerable, will be transmitted between fog and cloud, and among servers in cloud. Once the information is disclosed, various applications based on this identification and resolution system will be in an insecure situation. So the associated information should be encrypted during transmission process. In addition, data center is vulnerable. These sensitive data should also be stored by encryption.

2) Integrity of transmitted data

In our fog computing framework, FN, MS, RS and IS need to connect and communicate with each other to transmit data. During transmission process, these data may be modified and destroyed by illegal authorized attacker. In addition, the data stored in database need to be prevented from being tampered by attacker. In order to solve this problem, the mechanism of data integrity checking should be designed to ensure the consistency between sent data and received data.

3) Identity validity of functional participants

Fog nodes are usually deployed at the edge of network, which is a place out of rigorous protection and surveillance. They may become available for attacker to compromise overall system in order to achieve malicious purpose. This security threat mainly includes man-in-the-middle attack and identity forgery. In cloud, though the security is more powerful than fog nodes, unauthorized attacks also need to be bewared. Therefore, the authentication and authorization schemes for each function modules need to be designed to ensure that legitimate users will not be improperly rejected to use the information and resources. What's more, it should prevent illegal users from obtaining access authority.

In order to solve these problems, we will design detailed security and privacy preservation scheme for the processes of face identification and face resolution in the following section.

TABLE II
LIST OF SYMBOLS DEFINITION FOR SECURITY AND PRIVACY PRESERVATION SCHEME

Symbol	Description
r_{FN}, r_{MS}	Random number generated by FN and MS
S_{FN}, S_{MS}	Intermediate result generated in session key agreement process between FN and MS
p	Prime number
g	A primitive root of p
a, b	Random number generated by FN and MS, and $a < p, b < p$
ID_{FN}, ID_{MS}	The identification of FN and MS
PK_{FN}, PK_{MS}	Public key of FN and MS
SK_{FN}, SK_{MS}	Private key of FN and MS
au, bu	The key generated by FN, The key generated by MS
$K_{FN,MS}, K_{MS,RS}$, $K_{MS,IS}$	Session key between FN and MS, between MS and RS, between MS and IS
K_{RS}	The key of RS to be used for encrypting the data stored in database
K_{IS}	The key of IS to be used for encrypting the data stored in database

IV. Security and Privacy Preservation Scheme for Fog Computing Based Face Identification

From the previous section, we find that there are some security and privacy issues that need to be solved in face identification process. We take the interaction process between FN and MS as an example to present the authentication scheme, data encryption scheme, and data integrity checking scheme. The processes between MS and RS, between MS and IS are similar with it. Finally, the security and privacy preservation scheme of face identification system is presented.

The list of symbols definition and description for security and privacy preservation scheme is shown in Table II.

A. The Security Scheme for the Communication between FN and MS

When the face identification system is established, IDs of all legal and interconnected FNs are stored into database of MS. Similarly, IDs of corresponding MSs are also stored into database of FN. When a new node or server is connected, their ID needs to be inserted into the other side of database. By this

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

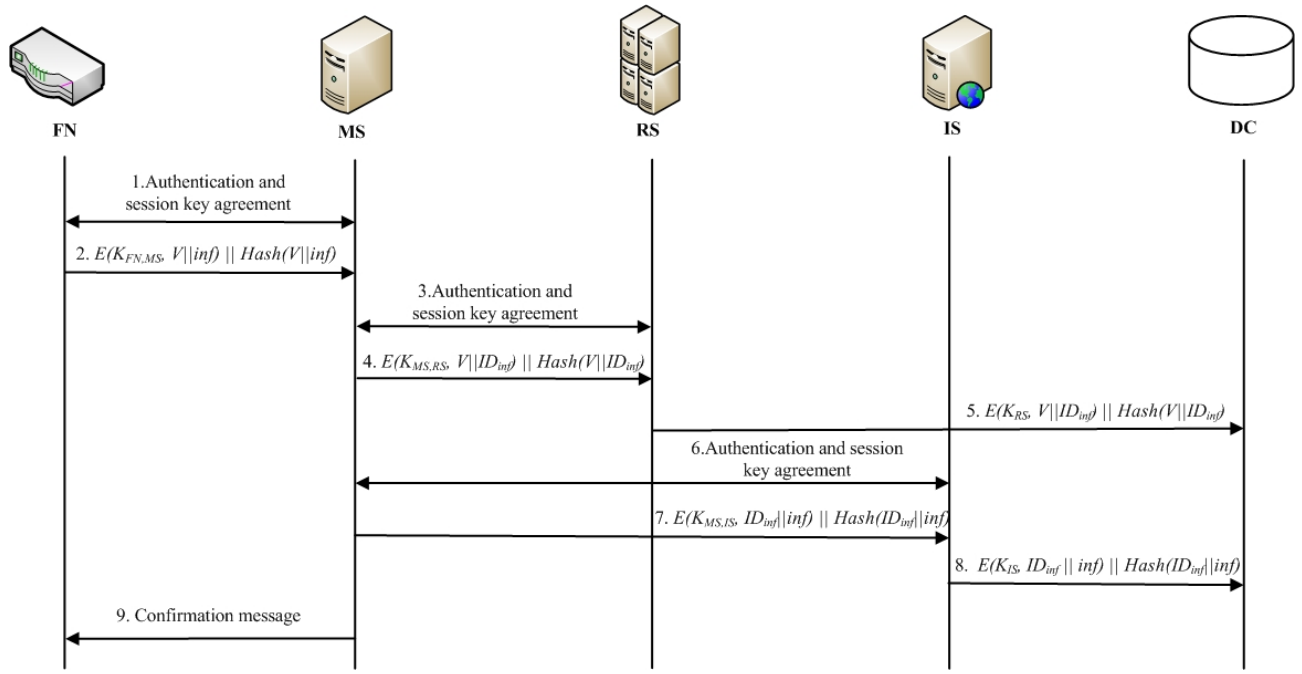

Fig. 3. The security and privacy preservation scheme of face identification process

Algorithm 3 The procedure of authentication and session key agreement between FN and MS

Begin

Step 1. FN chooses a random number r_{FN}. And $S_{FN} = g^a \ mod \ p$ is calculated according to prime number g, primitive root p, and random number a.

Step 2. FN encrypts ID_{FN}, r_{FN}, S_{FN}, p, and g with the public key PK_{MS} of MS. Then it sends the encrypted information $E(PK_{MS}, ID_{FN}||r_{FN}||S_{FN}||p||g)$ to MS.

Step 3. MS decrypts receiving messages with the private key SK_{MS} of MS to obtain $ID_{FN}, r_{FN}, S_{FN}, p$, and g. MS judges whether the identity of FN is legal by ID_{FN}. And $S_{MS} = g^b \ mod \ p$ is calculated, which b is a random number generated by MS. According to DH key agreement algorithm, $bu = {S_{FN}}^b mod \ p$ is used as the session key of MS. In addition, MS chooses a random number r_{MS}.

Step 4. MS encrypts $ID_{FN}, ID_{MS}, r_{FN}, r_{MS}$, and S_{MS} with the public key PK_{FN} of FN. Then it sends the encrypted information $E(PK_{FN}, ID_{FN}||ID_{MS}||r_{FN}||r_{MS}||S_{MS})$ to FN.

Step 5. FN decrypts receiving messages with the private key SK_{FN} of FN to obtain $ID_{FN}, ID_{MS}, r_{FN}, r_{MS}$, and S_{MS}. FN judges whether the identity of MS is legal by ID_{MS}. Meanwhile, FN judges whether current access is a replay attack by comparing returned r_{FN} with the r_{FN} sent in Step 2. In addition, $au = {S_{MS}}^a \ mod \ p$ is used as the session key of FN, and $au = bu = K_{FN,MS}$.

Step 6. FN encrypts r_{MS} with the public key PK_{MS} and sends the encrypted information $E(PK_{MS}, r_{MS})$ to MS.

Step 7. MS decrypts receiving messages with the private key SK_{MS} to obtain r_{MS}. MS judges whether current access is a replay attack by comparing returned r_{MS} with the r_{MS} sent in Step 4.

Step 8. MS sends confirmation message to FN, and the authentication and session key agreement process is accomplished.

End

way, when connection between FN and MS is established, their identity can be confirmed to each other.

Meanwhile, the session key between FN and MS need to be generated by session key agreement algorithm. The session key is used for encrypting the data to be transmitted in the subsequent process. In this paper, we adopt Diffie-Hellman (DH) key agreement algorithm to generate session key[44, 45].

The detailed authentication and session key agreement process between FN and MS is shown in Fig. 2.

In this process, the PKs of FN and MS are assigned in advance and open. And these PKs are real and available. We use public key encryption mechanism based on elliptic curve to encrypt the authentication and key agreement information[46]. The procedure of authentication and session key agreement between FN and MS is shown in Algorithm 3.

After the session key is generated, we adopt AES (Advanced Encryption Standard) symmetric key encryption mechanism to encrypt face identifier V and registered personal information *inf* of the individual[47]. In the data storage phase, we still adopt symmetric key encryption mechanism to encrypt data stored in database.

When MS receives messages transmitted from FN, it

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

Algorithm 4 The procedure of security and privacy preservation scheme for face identification system

Begin

Step 1. Bidirectional identity authentication and session key agreement algorithm between FN and MS is performed according to Algorithm 3. Then the identities of FN and MS are verified to each other. And the session key $K_{FN,MS}$ is generated and allocated to FN and MS.

Step 2. FN transmits messages to MS by adopting encryption mechanism. MS perform data integrity checking algorithm to verify integrity of data.

Step 2.1. FN encrypts face identifier *V* and personal information *inf* of the individual by using AES symmetric key encryption mechanism based on session key $K_{FN,MS}$. And the $Hash(V||inf)$ will be calculated by SHA-1 algorithm. Then FN sends $E(K_{FN,MS}, V||inf)||Hash(V||inf)$ to MS.

Step 2.2. MS decrypts receiving messages to obtain *V* and *inf*. Then MS calculates a new $Hash'(V||inf)$, which is compared with $Hash(V||inf)$ to judge whether received data is intact.

Step 3. MS and RS perform bidirectional identity authentication and session key agreement algorithm. The session key $K_{MS,RS}$ is generated and allocated to MS and RS.

Step 4. MS transmits messages to RS by adopting encryption mechanism. RS perform data integrity checking algorithm to verify integrity of data.

Step 4.1. MS encrypts face identifier *V* and identifier ID_{inf} of *inf*. And the $Hash(V||ID_{inf})$ will be calculated. Then MS sends $E(K_{MS,RS}, V||ID_{inf})||Hash(V||ID_{inf})$ to RS.

Step 4.2. RS decrypts receiving messages to obtain *V* and ID_{inf}. Then RS calculates a new $Hash'(V||ID_{inf})$, which is compared with $Hash(V||ID_{inf})$ to judge whether received data is intact.

Step 5. RS encrypts *V* and ID_{inf} with key K_{RS}, and calculates the $Hash(V||ID_{inf})$. Then RS sends $E(K_{RS}, V||ID_{inf})||Hash(V||ID_{inf})$ to DC for storing into database.

Step 6. MS and IS perform bidirectional identity authentication and session key agreement algorithm. The session key $K_{MS,IS}$ is generated and allocated to MS and IS.

Step 7. MS transmits messages to IS by adopting encryption mechanism. IS perform data integrity checking algorithm to verify integrity of data.

Step 7.1. MS encrypts identifier ID_{inf} of *inf* and personal information *inf* of the individual. And the $Hash(ID_{inf}||inf)$ will be calculated. Then MS sends $E(K_{MS,IS}, ID_{inf}||inf)||Hash(ID_{inf}||inf)$ to IS.

Step 7.2. IS decrypts receiving messages to obtain ID_{inf} and *inf*. Then IS calculates a new $Hash'(ID_{inf}||inf)$, which is compared with $Hash(ID_{inf}||inf)$ to judge whether received data is intact.

Step 8. IS encrypts ID_{inf} and *inf*. And the $Hash(ID_{inf}||inf)$ will be calculated. Then IS sends $E(K_{IS}, ID_{inf}||inf)||Hash(ID_{inf}||inf)$ to DC for storing into database.

Step 9. MS returns confirmation message of successful registration to FN.

End

will perform data integrity checking algorithm to verify the integrity of data. In this paper, we adopt hash data integrity checking algorithm based on SHA-1 (Secure Hash Algorithm-1). When *V* and *inf* are transmitted from FN to MS, the $Hash(V||inf)$ will be calculated and transmitted together with encrypted *V* and *inf*. Namely, FN will send $E(K_{FN,MS}, V||inf)||Hash(V||inf)$ to MS. After MS receives and decrypts these messages, it will calculate a new $Hash'(V||inf)$ with decrypted *V* and *inf*, and compare $Hash'(V||inf)$ and $Hash(V||inf)$. If they are equal, the received data is intact. Otherwise, it is non-intact. In data storage phase, we still adopt this integrity checking algorithm to verify the integrity of data access process and prevent data from being tampered by attacker.

B. Security and Privacy Preservation Scheme of Face Identification Process

According to the characteristics of face identification, we apply above security and privacy preservation algorithms into this process to solve the problems of confidentiality, integrity, and availability. The detailed security and privacy preservation scheme of face identification process is shown in Fig. 3.

The procedure of security and privacy preservation scheme for face identification process is shown in Algorithm 4.

V. Security and Privacy Preservation Scheme for Fog Computing Based Face Resolution

In the face resolution process, some operations are similar with face identification according to Algorithm 1 and Algorithm 2. The algorithms of face detection, facial image preprocessing, feature extraction and face identifier generation are also performed to generate the face identifier of test individual at first. Different from face identification, the generated identifier of test individual needs to be singly matched with all the enrolled face identifiers by performing identifier matching algorithm to implement face resolution. So there are some similar security and privacy issues that need to be solved.

In this process, we still adopt the public key encryption mechanism based on elliptic curve, Diffie-Hellman key agreement algorithm and AES symmetric key encryption algorithm to ensure the confidentiality of data transmission. Hash data integrity checking algorithm based on SHA-1 is adopted to ensure the integrity of data. And authentication algorithm is performed to ensure the vailability for legitimate users.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

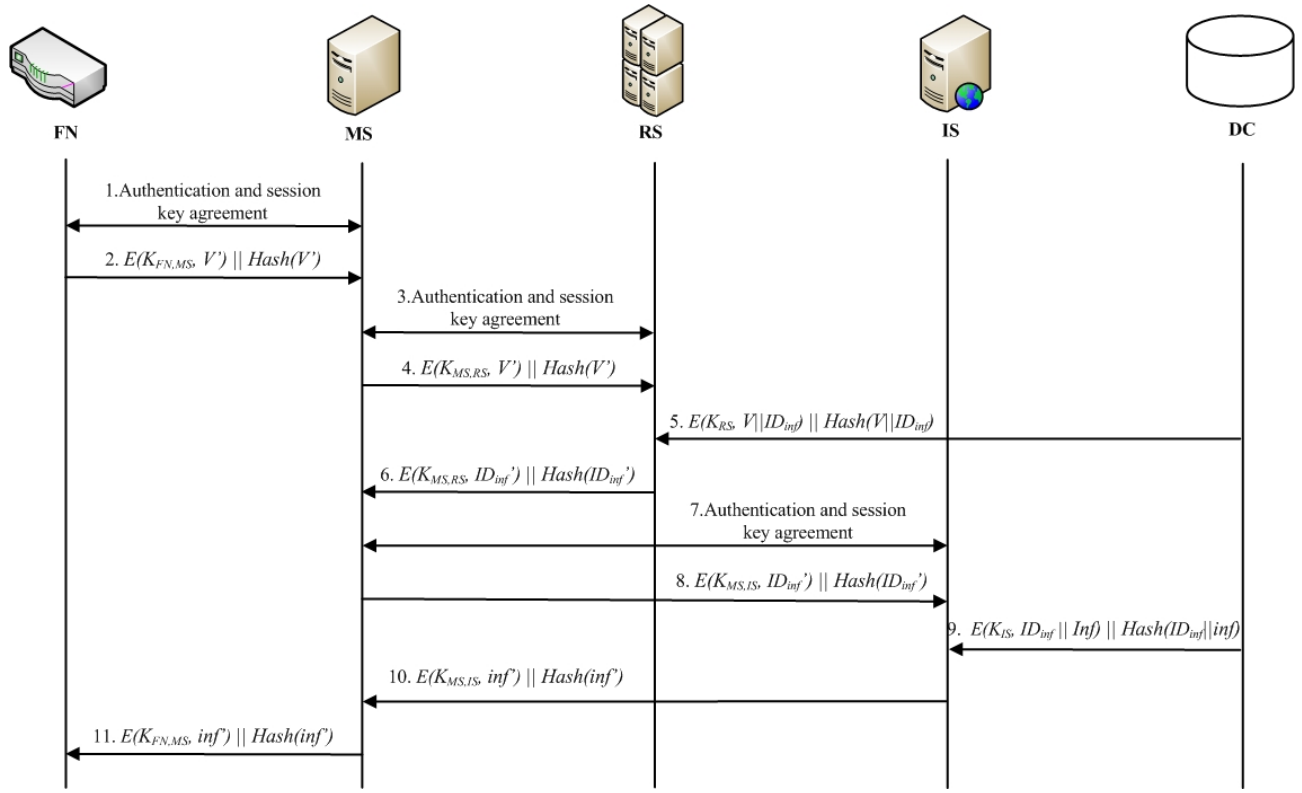

Fig. 4. The security and privacy preservation scheme of face resolution process

The detailed security and privacy preservation scheme of face resolution process is shown in Fig. 4.

The procedure of security and privacy preservation scheme for face resolution process is shown in Algorithm 5.

VI. Experiment and Performance Analysis

In this section, we evaluate and analyze the system performance and security properties of proposed security and privacy-preservation schemes for face identification and face resolution. According to the proposed scheme, we have implemented a prototype system and have evaluated the influence of security scheme on system performance. Furthermore, we have analyzed the security from the following two aspects: 1) formal proof with the BAN logic; 2) the three basic properties of information security, namely CIA (i.e., confidentiality, integrity, and availability).

A. Experimental Setup

In our previous work, we have implemented a prototype system of face identification and resolution according to Fig. 1. Based on this prototype system, we add the proposed security and privacy preservation scheme into it to implement a new system. The same algorithms of face detection, facial image preprocessing, feature extraction and face identifier generation, and face identifier matching are still executed. The proposed security and privacy preservation scheme in this paper are developed and deployed in this system.

We have deployed the new prototype system on the fog node and cloud server. The experimental environment and hardware configuration are the same with the previous system. Because the security and privacy preservation scheme of face identification process is very similar with the face resolution process, we only measure and evaluate the performance of face resolution to simplify the experiment process.

In our experiment, we measure the experimental results on three public database, including the Georgia Tech (GT) face database, the Caltech face database, and the BioID face database. We randomly choose some face images as test set and others as training set.

B. Experimental results and Performance analysis of prototype system

In general, the cost of computation and communication will increase after adding the security scheme into a system. For evaluating the influence of the proposed security scheme on system performance, we compare the changes of response time and communication overhead for the framework without security scheme and the framework with security scheme.

1) Response time for different face databases: The time consumption from sending resolution request in client to receiving the result is used as the system response time. It contains the time of face identifier generation, network transmission, and identifier matching. Fig. 5 shows the system response time of the frameworks before and after adding the security scheme for different face database. After adding the proposed security scheme, the time consumption only increases about 70ms. This indicates that the computational complexity of our proposed security and privacy preservation scheme is small and it can meet the practical application needs.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

Algorithm 5 The procedure of security and privacy preservation scheme for face resolution process

Begin

Step 1. Bidirectional identity authentication and session key agreement algorithm between FN and MS is performed according to Algorithm 3 to verify to each other's identities and generate the session key $K_{FN,MS}$.

Step 2. Like Step 2 in Algorithm 4, FN sends $E(K_{FN,MS}, V')||Hash(V')$ to MS by using AES symmetric key encryption mechanism based on session key $K_{FN,MS}$, and MS performs data integrity checking algorithm to verify integrity of data by judging whether $Hash'(V')$ and $Hash(V')$ are equal.

Step 3. MS and RS perform bidirectional identity authentication and session key agreement algorithm to verify each other's identities and generate the session key $K_{MS,RS}$.

Step 4. MS sends $E(K_{MS,RS}, V')||Hash(V')$ to RS by using encryption mechanism, and RS verifies integrity of data by judging whether $Hash'(V')$ and $Hash(V')$ are equal.

Step 5. RS implements face identifier matching.

Step 5.1. After RS decrypts receiving messages, *V'* will be obtained.

Step 5.2. All the identifiers $E(K_{RS}, V||ID_{inf})||Hash(V||ID_{inf})$ stored in database are seriatim taken out and decrypted. And a new $Hash'(V||ID_{inf})$ is calculated and compared with $Hash(V||ID_{inf})$ to verify the data integrity.

Step 5.3. The face identifier *V'* is seriatim matched with *V* by performing face identifier matching algorithm. After successful matching, the corresponding $ID_{inf}{}'$, which is paired with the face identifier matched successfully, will be obtained.

Step 6. RS transmits messages to MS by adopting encryption mechanism. MS performs data integrity checking algorithm to verify integrity of data.

Step 6.1. RS encrypts $ID_{inf}{}'$ and calculates the $Hash(ID_{inf}{}')$, then sends $E(K_{MS,RS}, ID_{inf}{}')||Hash(ID_{inf}{}')$ to MS.

Step 6.2. MS decrypts receiving messages to obtain $ID_{inf}{}'$ and calculates the new $Hash'(ID_{inf}{}')$, which is compared with $Hash(ID_{inf}{}')$ to judge whether received data is intact.

Step 7. MS and IS perform bidirectional identity authentication and session key agreement algorithm to verify their identities and generate the session key $K_{MS,IS}$.

Step 8. MS sends $E(K_{MS,IS}, ID_{inf}{}')||Hash(ID_{inf}{}')$ to IS by using encryption mechanism, and IS verifies integrity of data by judging whether $Hash'(ID_{inf}{}')$ and $Hash(ID_{inf}{}')$ are equal.

Step 9. IS acquires personal information.

Step 9.1. After IS decrypts the received messages, $ID_{inf}{}'$ will be obtained.

Step 9.2. All the $E(K_{IS}, ID_{inf}||inf)||Hash(ID_{inf}||inf)$ stored in database are seriatim taken out and decrypted. And the new $Hash'(ID_{inf}||inf)$ is calculated and compared with $Hash(ID_{inf}||inf)$ to verify the data integrity.

Step 9.3. $ID_{inf}{}'$ is seriatim compared with ID_{inf}. After successful matching, the corresponding personal information *inf'* of test individual is acquired.

Step 10. IS sends $E(K_{MS,IS}, inf')||Hash(inf')$ to MS by using encryption mechanism, and MS performs data integrity checking algorithm to verify integrity of data by judging whether $Hash'(inf')$ and $Hash(inf')$ are equal.

Step 11. MS sends $E(K_{FN,MS}, inf')||Hash(inf')$ to MS, and FN verifies integrity of data by judging whether $Hash'(inf')$ and $Hash(inf')$ are equal. Finally, FN returns the personal information *inf'* to client, and displays it to end users.

End

2) Response time for different size of face database: We set different numbers of face images in database by using the BioID face database to measure the system response time. Fig. 6 shows the average response time for different size of face databases. For the framework with the proposed security scheme, the response time will increase with the increase of size of face database, but the increment speed is relatively slow and stable. Moreover, after adding the proposed security scheme into the resolution framework, the average of consumption time only increases about 52ms for different size of face databases. This indicates that our proposed security and privacy preservation scheme can keep superiority in term of stability.

3) Amount of network transmission: We measure the amount of network transmission from fog nodes to cloud server for evaluating the communication overhead of proposed scheme. Fig. 7 shows the amount of network transmission for different face databases. Because the size of face identifier generated by LBP feature extraction algorithm is the same for different face images, the amount of network transmission is also the same on different face database for the same resolution framework. The framework with security scheme increases about 0.176KB compared with the framework without security scheme. The result indicates that the communication overhead of our scheme is small.

From these experimental results, we can find that our proposed security and privacy preservation scheme only increases a small computation and communication overhead to provide security and privacy preservation for face identification and resolution service. And it is able to keep superiority in term of stability and meet the practical application needs.

C. Security Analysis

We analyze the security properties of proposed scheme in detail from the following two aspects:

1) Formal proof with the BAN logic

As an important part of our security scheme, session key agreement algorithm of fog computing based face identifica-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

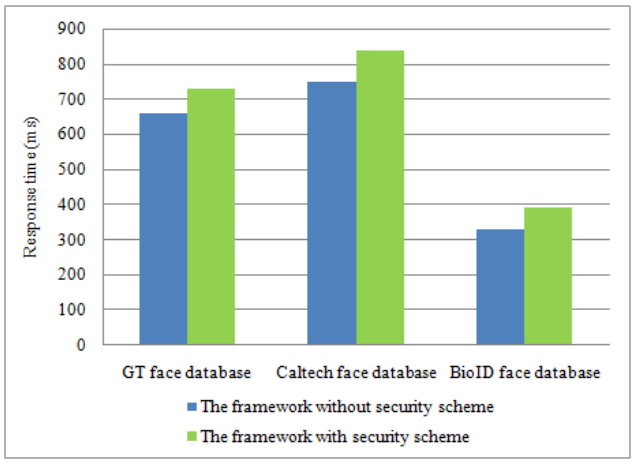

Fig. 5. Average response time for different face databases

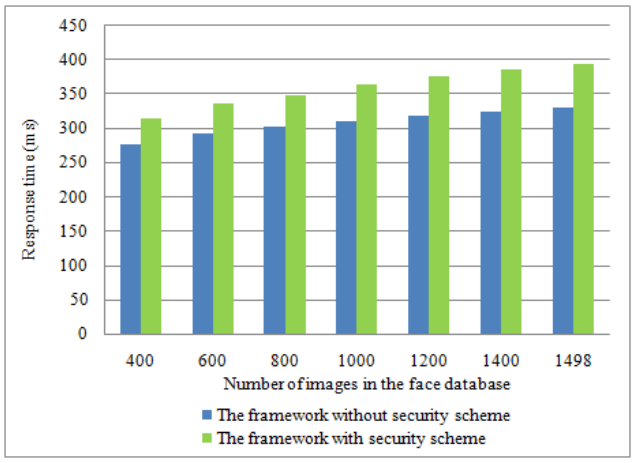

Fig. 6. Average response time for different size of face databases

tion framework has been presented in Fig. 2 and Algorithm 3. In this subsection, we adopt BAN logical formal analysis method and related rules to analyze and verify the security of this process.

Idealized model:

$$FN \rightarrow MS : \{r_{FN}, ID_{FN}, S_{FN}, p, g\}_{PK_{MS}}, \quad (1)$$

$$MS \rightarrow FN : \{r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS}\}_{PK_{FN}}, \quad (2)$$

$$FN \rightarrow MS : \{r_{MS}\}_{PK_{MS}}. \quad (3)$$

Explanation:

$$MS \lhd \{r_{FN}, ID_{FN}, S_{FN}, p, g\}_{PK_{MS}}, \quad (4)$$

$$FN \lhd \{r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS}\}_{PK_{FN}}, \quad (5)$$

$$MS \lhd \{r_{MS}\}_{PK_{MS}}. \quad (6)$$

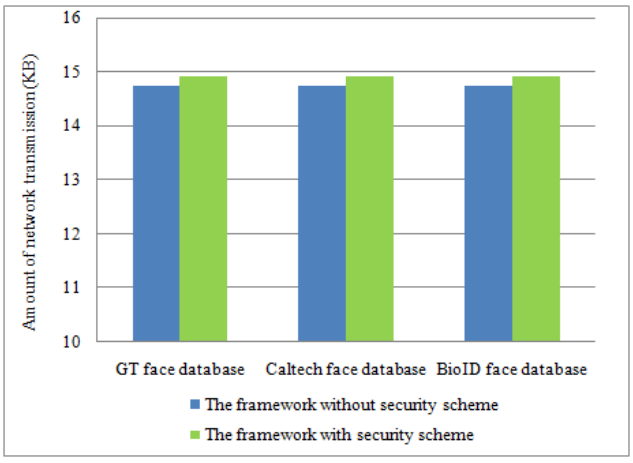

Fig. 7. Amount of network transmission for different face databases

Initial hypothesis set:

$$P_1 : FN \mid\equiv \xrightarrow{PK_{FN}} MS; \quad (7)$$

$$P_2 : MS \mid\equiv \xrightarrow{PK_{MS}} FN; \quad (8)$$

$$P_3 : FN \mid\equiv MS \mid\Rightarrow (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS}); \quad (9)$$

$$P_4 : MS \mid\equiv FN \mid\Rightarrow (r_{FN}, ID_{FN}, S_{FN}, p, g); \quad (10)$$

$$P_5 : FN \mid\equiv \sharp(r_{FN}); \quad (11)$$

$$P_6 : MS \mid\equiv \sharp(r_{MS}); \quad (12)$$

Anticipated target:

$FN \mid\equiv {S_{MS}}^a \bmod p = g^{ab} \bmod p$;
$MS \mid\equiv {S_{FN}}^b \bmod p = g^{ab} \bmod p$;

BAN logic reasoning:

By applying the BAN inference rule $R_2, R_{11}, R_4, R_5, R_{13}, R_{12}$, we can derive the following procedure.

Applying rule R_2, initial hypothesis set P_1 and formula (5), we obtain that

$$\frac{FN \mid\equiv \xrightarrow{PK_{FN}} MS, \quad FN \lhd \{r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS}\}_{PK_{FN}}}{FN \mid\equiv MS \mid\sim (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}. \quad (13)$$

Applying rule R_{11} and initial hypothesis set P_5, we obtain that

$$\frac{FN \mid\equiv \sharp(r_{FN})}{FN \mid\equiv \sharp(r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}. \quad (14)$$

Applying rule R_4, formula (13) and (14), we obtain that

$$\frac{FN \mid\equiv MS \mid\sim (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS}), \quad FN \mid\equiv \sharp(r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}{FN \mid\equiv MS \mid\equiv (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}. \quad (15)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

Applying rule R_5, initial hypothesis set P_3 and formula (15), we obtain that

$$\frac{FN \mid\equiv MS \mid\Rightarrow (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS}),\ FN \mid\equiv MS \mid\equiv (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}{FN \mid\equiv (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}. \tag{16}$$

Applying rule R_{13} and formula (16), we obtain that

$$\frac{FN \mid\equiv (r_{FN}, r_{MS}, ID_{FN}, ID_{MS}, S_{MS})}{FN \mid\equiv (S_{MS})}. \tag{17}$$

Therefore,

$$FN \mid\equiv (S_{MS}) = g^b \ mod \ p. \tag{18}$$

Because a is a random number chosen by FN, then

$$FN \mid\equiv (S_{MS}) = g^a \ mod \ p. \tag{19}$$

Applying rule R_{12}, formula (18) and (19), we obtain that

$$\frac{FN \mid\equiv (S_{MS}) = g^b \ mod \ p, FN \mid\equiv (S_{MS}) = g^a \ mod \ p}{FN \mid\equiv (S_{MS}) = g^{ab} \ mod \ p}, \tag{20}$$

Therefore,

$$FN \mid\equiv g^{ab} \ mod \ p = {S_{MS}}^a \ mod \ p. \tag{21}$$

In the same way, we obtain that

$$MS \mid\equiv g^{ab} \ mod \ p = {S_{FN}}^a \ mod \ p. \tag{22}$$

By the above security proof based on BAN logic, the formal analysis of key agreement process is demonstrated. In our key agreement scheme, the session key $\{g^{ab} \ mod \ p\}$ can be distributed to the two communication partners credibly. Our scheme is proved to be correct and can ensure the security of session process.

2) CIA properties analysis

As the three basic properties of information security, the confidentiality, integrity and availability are usually used for evaluating the security of scheme. In previous section, we have analyzed and discussed security and privacy issues of fog computing based face identification and resolution framework from these three aspects. The CIA properties of proposed scheme are analyzed in this subsection.

- *Confidentiality:* In our security scheme, data encryption algorithms are adopted to ensure the confidentiality of system in the processes of data transmission and storage. The encryption algorithms adopted at different phases are not the same. In the process of authentication and session key agreement, public key encryption mechanism based on elliptic curve is adopted to encrypt the authentication and key agreement information. After the session key is generated, we adopt symmetric key encryption algorithm based on session key, which is a symmetric cryptography, to encrypt face identifier and personal identity information of the individual. In the data storage phase, we still adopt symmetric key encryption algorithm to encrypt personal information in database. These encryption algorithms can effectively prevent the data from being stolen. Moreover, we make the best possible use of the symmetric encryption mechanism in our scheme, because it is more efficient and computing speed is faster than asymmetric cryptography mechanism, especially in the case of relatively large amount of data.
- *Integrity:* In order to prevent the data from being tampered during the transmission, we adopt hash data integrity checking algorithm based on SHA-1 to ensure the integrity of transmitted message. SHA-1 algorithm can convert the key and arbitrary length of data into a fixed length of data. Any changes occurred in the transmission process will cause the change in the output of the fixed length data. The receiver is able to discover the changes about the message by comparing hash values. Furthermore, in the data storage process, we also adopt hash data integrity checking algorithm based on SHA-1 to verify the integrity of data access process. It effectively prevent data in database from being tampered by attacker. By this way, the illegal users can not arbitrarily modify the transmitted message and the data in database.
- *Availability:* In our security scheme, we ensure the system availability by authentication mechanism. It includes the following two aspects. On the one hand, the communication parties need to verify each others ID. On the other hand, in the processes of authentication and session key agreement, we adopt the public key encryption mechanism which indirectly imply the process of identity authentication. Furthermore, the authentication mechanism can resist replay attack by sending and verifying random number generated by the two communication partners. By this way, system can ensure that legitimate users are not improperly rejected to use the information and resources. What's more, it can prevent illegal users from obtaining access authority.

VII. Conclusions

This paper focuses on the security and privacy issues of face identification and resolution framework based on fog computing, which is proposed in our previous work. The security and privacy-preservation schemes for face identification and face resolution have been proposed. Considering the characteristics of fog computing framework, we summarize the security and privacy issues in face identification and resolution. In order to solve these issues, we design the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme for the processes of face identification and face resolution. They can solve the issues of confidentiality, integrity, and availability. We implement the prototype system, which proposed scheme is applied into the fog computing based face identification and resolution system, to evaluate system performance after adding security scheme. The results show that the proposed scheme only increases a little computation and communication overhead while ensuring the security of system. Furthermore, we evaluate and analyze

the security properties of proposed scheme from the two aspects: the BAN logical formal proof and the CIA properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation, and ensure to provide secure face identification and resolution service.

ACKNOWLEDGMENT

This work was funded by the National Natural Science Foundation of China (Grant No.61471035 and Grant No.61672131), the Fundamental Research Funds for Central Universities (Grant No.06105031). The authors are grateful to the Center for Signal and Image Processing of Georgia Institute of Technology for providing Georgia Tech face database, the Caltech Computational Vision Group of California Institute of Technology for providing Caltech face database, and the BioID for providing BioID face database.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] S. Chen, H. Xu, D. Liu, and B. Hu, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 349-359, 2014.

[3] H. Ning, H. Liu, J. Ma, L. T. Yang, and R. Huang, "Cybermatics: Cyber-physical-social-thinking hyperspace based science and technology," *Future Generation Computer Systems*, vol. 56, pp. 504-522, 2016.

[4] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: Architectures, advances and challenges," *Ad Hoc Networks*, vol. 55, pp. 143-152, 2017.

[5] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, *Smart Cities: Foundations, Principles and Applications*. Hoboken, NJ, USA: Wiley, 2017.

[6] J. Ma, J. Wen, R. Huang, and B. Huang, "Cyber-Individual Meets Brain Informatics," *IEEE Intelligent Systems*, vol. 26, no. 5, pp. 30-37, 2011.

[7] J. Miranda, N. Makitalo, J. Garciaalonso, J. Berrocal, T. Mikkonen, C. Canal, et al., "From the Internet of Things to the Internet of People," *IEEE Internet Computing*, vol. 19, no. 2, pp. 40-47, 2015.

[8] H. Ning and H. Liu, "Cyber-physical-social-thinking space based science and technology framework for the Internet of Things," *Science China Information Sciences*, vol. 58, no. 3, pp. 1-19, 2015.

[9] D. L. Brock, "The electronic product code (epc)," *Auto-ID Center White Paper MIT-AUTOID-WH-002*, 2001.

[10] N. Koshizuka and K. Sakamura, "Ubiquitous ID: standards for ubiquitous computing and the Internet of Things," *IEEE Pervasive Computing*, vol. 9, no. 4, pp. 98-101, 2010.

[11] H. Ning, S. Hu, W. He, Q. Xu, H. Liu, and W. Chen, "nID-based internet of things and its application in airport aviation risk management," *Chinese Journal of Electronics*, vol. 21, no. 2, pp. 209-214, 2012.

[12] H. Ning, Y. Fu, S. Hu, and H. Liu, "Tree-Code modeling and addressing for non-ID physical objects in the Internet of Things," *Telecommunication Systems*, vol. 58, no. 3, pp. 195-204, 2015.

[13] S. Kwok, O. P. Ng, A. H. Tsang, and H. Liem, "Physimetric identification (Physi-ID)–Applying biometric concept in physical object identification," *Computers in Industry*, vol. 62, no. 1, pp. 32-41, 2011.

[14] M. Beham and S. Roomi, "A review of face recognition methods," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 27, no. 04, pp. 1356005101-1356005135, 2013.

[15] S. Shaikh and J. Rabaiotti, "Characteristic trade-offs in designing large-scale biometric-based identity management systems," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 342-351, 2010.

[16] L. Yu, L. Chen, Z. Cai, H. Shen, Y. Liang, and Y. Pan, "Stochastic Load Balancing for Virtual Resource Management in Datacenters," *IEEE Transactions on Cloud Computing*, 2016. [Online]. Available: https://doi.org/10.1109/TCC.2016.2525984

[17] P. Peer, Ž. Emeršič, J. Bule, J. Žganec-Gros, and V. Štruc, "Strategies for exploiting independent cloud implementations of biometric experts in multibiometric scenarios," *Mathematical problems in engineering*, vol. 2014, pp. 1-15, 2014.

[18] L. Yu, H. Shen, K. Sapra, and L. Ye, "CoRE: Cooperative End-to-End Traffic Redundancy Elimination for Reducing Cloud Bandwidth Cost," *IEEE Transactions on Parallel and Distributed Systems*, 2016. [Online]. Available: https://doi.org/10.1109/TPDS.2016.2578928

[19] L. Yu and Z. Cai, "Dynamic scaling of virtual clusters with bandwidth guarantee in cloud datacenters," *in IEEE INFOCOM 2016 - IEEE Conference on Computer Communications*, 2016, pp. 1-9.

[20] N. N. Khan, "Fog Computing: A Better Solution For IoT," *International Journal of Engineering and Technical Research*, vol. 3, no. 2, pp. 298-300, 2015.

[21] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," *in Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012, pp. 13-16.

[22] P. Hu, H. Ning, T. Qiu, Y. Zhang, X. Luo, "Fog Computing-Based Face Identification and Resolution Scheme in Internet of Things," *IEEE Transactions on Industrial Informatics*, 2016. [Online]. Available: https://doi.org/10.1109/TII.2016.2607178

[23] T. Qiu, A. Zhao, R. Ma, V. Chang, F. Liu, and Z. Fu, "A task-efficient sink node based on embedded multi-core soC for Internet of Things," *Future Generation Computer Systems*, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.future.2016.12.024

[24] Y. Zheng, Z. Peng, and A. V. Vasilakos, "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, no. 3, pp. 120-134, 2014.

[25] H. Song, G. A. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications*. Chichester, UK: Wiley-IEEE Press, 2017.

[26] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2706-2716, 2016.

[27] Q. Du, L. Sun, H. Song, and P. Ren, "Security Enhancement for Wireless Multimedia Communications by Fountain Code," *IEEE COMSOC MMTC Communications C Frontiers*, vol. 11, no. 2, pp. 47-51, 2016.

[28] C. Dsouza, G. J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," *in IEEE International Conference on Information Reuse and Integration*, 2014, pp. 16-23.

[29] L. Wang and A. M. Wyglinski, "Detection of man-in-the-middle attacks using physical layer wireless security techniques," *Wireless Communications & Mobile Computing*, vol. 16, no. 4, pp. 408-426, 2016.

[30] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, pp. 2991-3005, 2015.

[31] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI - A System for Secure Face Identification," *in Proceedings of the 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 239-254.

[32] Y. Huang, L. Malka, D. Evans, and J. Katz, "Efficient Privacy-preserving Biometric Identification," *presented at the Network and Distributed System Security Symposium (NDSS)*, 2011.

[33] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7905-7916, 2015.

[34] A. Bommagani, M. Valenti, and A. Ross, "A Framework for Secure Cloud-Empowered Mobile Biometrics," *in 2014 IEEE Military Communications Conference (MILCOM)*, 2014, pp. 255-261.

[35] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," *in 2013 Proceedings IEEE INFOCOM*, 2013, pp. 2652-2660.

[36] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2594-2608, 2016.

[37] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," *in 2015 6th International Conference on the Network of the Future (NOF)*, 2015, pp. 1-3.

[38] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," *in 10th International Conference on Wireless Algorithms*, Systems, and Applications (WASA), 2015, pp. 685-695.

[39] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," *in 2014 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2014, pp. 1-8.

[40] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037-2041, 2006.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2659783, IEEE Internet of Things Journal

[41] F. Pujol and J. Garcia, "Computing the Principal Local Binary Patterns for face recognition using data mining tools," *Expert Systems with Applications*, vol. 39, no. 8, pp. 7165-7172, 2012.
[42] T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, 2002.
[43] R. Lienhart and J. Maydt, "An extended set of haar-like features for rapid object detection," *in Proceedings of the 2002 International Conference on Image Processing*, 2002, pp. 900-903.
[44] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.
[45] W. Zhang, K. Hansen, and T. Kunz, "Enhancing intelligence and dependability of a product line enabled pervasive middleware," *Pervasive & Mobile Computing*, vol. 6, no. 2, pp. 198-217, 2010.
[46] N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography," *Designs Codes & Cryptography*, vol. 19, no. 2-3, pp. 173-193, 2000.
[47] J. Buchholz, "Advanced Encryption Standard," *in International Workshop on FAST Software Encryption*, 2001, pp. 83-87.

Pengfei Hu (S'16) received the B.E. degree from the School of Computer Science, Zhengzhou University of Aeronautics, China, in 2012. He is currently working toward the Ph.D. degree from the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. He focuses on the objects modelling in cyber-physical space convergence and Internet of Things. His research interests include Internet of Things, identification and resolution of physical objects, and cyber-physical modelling. He is a student member of IEEE.

Huansheng Ning (M'10, SM'13) received a B.S. degree from Anhui University in 1996 and Ph.D. degree in Beihang University in 2001. Now, he is a professor and vice dean of School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research focuses on Internet of Things, cyber-physical modeling. He is the founder of Cyberspace and Cybermatics and Cyberspace International Science and Technology Cooperation Base. He serves as an associate editor of IEEE System Journal and IEEE Internet of Things Journal. He is the Co-Chair of IEEE Systems, Man, and Cybernetics Society Technical Committee on Cybermatics. He has hosted the 2013 World Cybermatics Congress (WCC2013/iThings2013/CPSCom2013/Greencom2013), and the 2015 Smart World Congress (SmartWorld2015/UIC2015/ATC2015/ScalCom2015/CBDCom2015/IoP2015) as the joint executive chair. He gained the IEEE Computer Society Meritorious Service Award in 2013, IEEE Computer Society Golden Core Award in 2014.

Tie Qiu (M'11, SM'16) received Ph.D and M.Sc. from Dalian University of Technology (DUT), in 2012 and 2005, respectively. He is currently Associate Professor at School of Software, Dalian University of Technology, China. He was a visiting professor at electrical and computer engineering at Iowa State University in US (2014- 2015). He serves as an Associate Editor of IEEE Access and Computers & Electrical Engineering (Elsevier journal),an Editorial Board Member of JACST, a Guest Editor of Elsevier Ad Hoc Networks, a Program Chair of iThings2016, a Workshop Chair of CISIS13 and ICCMSE15, a TPC member of Industrial IoT15, ICSN16, AIA13, EEC14, EEC15 and EEC16. He has authored/co-authored 7 books, over 50 scientific papers in international journals and conference proceedings.He has contributed to the development of 3 copyrighted software systems and invented 10 patents. He is a senior member of China Computer Federation (CCF) and a Senior Member of IEEE and ACM.

Houbing Song (M'12, SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012. In August 2012, he joined the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV, where he is currently an Assistant Professor and the Founding Director of both the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us), and West Virginia Center of Excellence for Cyber-Physical Systems sponsored by West Virginia Higher Education Policy Commission. He has published more than 100 academic papers in peer-reviewed international journals and conferences. His research interests include cyber physical systems, internet of things, cloud computing, and big data analytics. Dr. Song is a senior member of IEEE and a member of ACM. He was the first recipient of the Golden Bear Scholar Award, the highest faculty research award at WVU.

Yanna Wang received the B.E. degree from the University of Science and Technology of Hebei, China, in 2015. She is currently working toward the M.S. degree from the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. Her research interests include Internet of Things,computer network security.

Xuanxia Yao received her B.S. degree from Jiangsu University, M.S. and Ph.D. degree from University of Science and Technology Beijing (USTB), China. She is an associate professor in School of Computer and Communication Engineering, USTB. She is the author of one book, more than 30 articles. Her research interests include network and information security, Internet of Things and cloud computing. She is a member of CCF (China Computer Federation).