A Privacy-Preserving Attribute-Based Authentication Scheme for Cloud Computing

Chanying Huang*†, Songjie Wei *, Kedong Yan *, Gongxuan Zhang *and Anmin Fu *
* Nanjing University of Science and Technology, Nanjing, China
† E-mail: hcy@njust.edu.cn Tel/Fax: +86-25-84315660

***Abstract*—Cloud computing is a revolutionary information technology paradigm, which provides users with unlimited, scalable, low-cost and convenient resource services. Challenging security issues such as user privacy, access control, etc. still urgently need to be addressed. Authentication, as the first line of defence to guarantee cloud security, still faces great security and privacy challenges. Users' privacy is generally neglected during authentication. Some authentication solutions provide privacy preservation yet do not consider fine-grained access control. To solve this problem, existing authentication schemes applied bilinear pairing for authorized and fine-grained access to cloud data. However, efficiency is still an unsolved challenge for the bilinear pairing cryptography. To address the challenge, this paper proposes an efficient attribute-based authentication scheme. The proposed authentication scheme can achieve efficient fine-grained access control and privacy preservation as well. We conduct theoretical security analysis, and carry out experiments to prove that the proposed scheme has good performance in terms of computational, communication and storage overheads.**

I. Introduction

Cloud computing is an emerging information technology paradigm, which provides us with unlimited, scalale, low-cost and convenient resource services. With the development of cloud computing, more and more enterprises and individuals store their data in the distributed cloud, and share these data via cloud server. Cloud data storage and sharing have become one of the most important cloud services, and also become the trend of social development [1], [2]. On the one hand, cloud services provide users with massive, convenient data storage and data sharing. But on the other hand, security and privacy concerns are still the major obstacles that hinder the widespread use of cloud computing [3]–[6]. In cloud computing, to avoid data from unauthorized access/use, authentication is the first line of defence to guarantee system and data security.

Generally, the authentication schemes for the cloud employ different techniques such as password (something users know), smartcard (something users have), biometrics (something users are) or their combination [7]–[10]. However, since traditional password-based authentication schemes are subject to password guessing attacks, smartcard-based protocols are vulnerable to stolen or lost threats, and biometric-based authentication schemes require critical privacy protection of the biometric information, cloud data still faces unauthorized access issue and other hidden dangers. Specifically, when handling the authorized accessing of sensitive information such as healthcare information, privacy preservation is of the utmost importance. Nevertheless, user's privacy is commonly neglected, especially when a user challenges the cloud server to request for other users' data for data sharing purpose.

In addition to users' privacy protection, fine-grained authorized access is another challenging issues for cloud computing. With traditional ID-based techniques, fine-grained acess control cannot be achieved. Attribute-based cryptography is suitable for addressing fine-grained access problem for cloud computing. In attribute-based system, the private key of a user is directly related with his/her attribute set distributed by the system attribute authority. With this characteristic, attribute-based technique has many important applications, and especially is ofen applied to e-health cloud [11], [12], where users with different attribute sets can access to different parts of the healthcare data for privacy reason. Recently, lots of authentication protocols combined bilinear pairing and attribute-based techniques for fine-grained access control [13]–[16]. Therefore, to prevent sensitive information from unauthorized accessing or abuse, so that only legitimate users are allowed to access the private information from the cloud server, and further reach fine-grained access control, it is of great importance to further study privacy-preserving attribute-based authentication and authorization solutions for cloud computing.

A. Literature review

To deal with authorized access control, there exist a series of authentication schemes, which employ different techniques. As discussed above, traditional authentication schemes employed password, smartcard, biometrics or their combination [7]–[10]. To address impersonation attack in previous scheme [17], Jiang et al. presented an e-health cloud-based authentication protocol using light-weight elliptic curve cryptography [10]. However, Jiang et al.'s scheme is still vulnerable to denial-of-service (DoS) attacks. Irshad et al. improved Jiang et al's scheme by using session variables and adding an additional one-half round-trip during mutual authentication. Their proposed solution was secure in well resisting to replay attack and denial-of-service attack [18].

This work is supported by China NSF (61802183, 61472189,61806095), Jiangsu Planned Projects for Postdoctoral Research Funds (1701146B), CERNET Next Generation IT Inovation Project (NGII20160105), State Key Laboratory of Air Traffic Management System and Technology (SKLATM201703), and the National Science Foundation of China (61572255).

In recent research works on authentication for cloud environment, many studies focus on addressing the problem of users' privacy disclosure [19]–[27]. Chen et al. proposed a privacy authentication scheme based on cloud for medical environment [19]. However, their scheme failed to achieve patient anonymity in the patient uploading phase. Additionally, the scheme also failed to provide message authentication in healthcare center uploading phase or patient uploading phase. Chiou et al. improved Chen et al.'s scheme and proposed a new authentication scheme that provided anonymity, unlinkability, and message authentication for medical cloud environment [20]. Yet their proposed scheme failed to support fine-grained access control. Chaudhry et al. proposed an enhanced privacy preserving remote user authentication scheme to overcome user anonymity violation problem and smart card stolen problem, and proved the security of proposed scheme using random oracle model [21]. Jiang et al. proposed a privacy aware authentication scheme for distributed mobile cloud computing services [22]. The latter two schemes have the same problem as Chiou et al.'s scheme. Qiu et al proposed a scheme that used a bilinear pairing to achieve fine-grained access control and protect cloud data in [23]. To protect users' privacy during authenticaiton, Gupta et al. used a bilinear pairing to achieve anonymous authentication in [26]. Rui et al. introduced a decentralized approach and provided authentication scheme without revealing the identity of the user for secure data storage in clouds [27]. By using attribute-based signature, their authentication approach could address anonymity and user revocation problems. However, computation efficiency is the major limitation of their scheme.

To address the above mentioned problems, this paper introduce an efficient privacy-preserving authentication scheme for cloud computing. By employing attribute-based cryptography, the proposed authentication scheme can provide fine-grained access control. In addition, we analyse and prove the security of the proposed scheme. We also discuss and demonstrate the proposed scheme is efficient in computational and communication overheads.

B. Our contribution

In this paper, we consider achieving authorized access and attribute privacy preserving with high efficiency simultaneously. The main contributions of this paper are in three-fold, as follows:

1) We propose a secure attribute-based authentication scheme with fine-grained access control for cloud computing. The proposed scheme provides authorized access to PHR system with privacy-preserving.
2) We provide an extensive security analysis and show that sufficient security protection and privacy preservation are guaranteed in the proposed authentication scheme. Primary security requirements such as authorization and sensitive attributes protection are satisfied. In addition, the proposed scheme can effectively resist general attacks such as replay attack, forgery attacks and collusion attacks.
3) We also carry out comprehensive performance evaluation and further perform simulation experiments on both Intel and smart phone platforms. Accordingly, experimental results demonstrate that the proposed attribute-based authentication scheme is practical, with reasonable storage requirement, efficient computational and low communication overheads.

The notations used in this paper are listed in Table I.

II. Preliminaries

A. Attributes

The attributes of a user/subject consist of type-identifier (e.g. patient, doctor, pharmacy), and characteristics that define the identity of the subject such as affiliation, profession, speciality, level, etc.

Fig. 1 shows an example of different users (health provider and patient) owning different sets of attributes, which are distributed by the trusted authority (TA).

B. Bilinear Pairing

Let G_1 and G_2 be an additive and a multiplicative group respectively, with large prime order q. Assumed that g is a random generator of G_1, and $e : G_1 \times G_1 \rightarrow G_2$ denotes the bilinear map, for which the following properties hold:

- Bilinear: $e(g^a, h^b) = e(g, h)^{ab}$, $\forall g, h \in G_1$ and $\forall a, b \in Z_q^*$.
- Non-degenerate: $\exists g \in G_1$ such that $e(g, g) \neq 1$.
- Computable: e is efficiently computable.

III. System Model

In our scheme, all users (or patients) need to register with the trusted attribute authority (TA), and TA takes charge of initializing the whole system, issuing public parameters, system master key and the universal attribute set. TA also issues a unique attribute set and the corresponding private key for a registered user. Users or patients will store their data (including sensitive personal data) into the cloud for data sharing purpose. Other user who wishes to access to patients' data should first conduct authentication with the cloud. There are three major parties involved in our scheme.

1) Cloud Server: The data storage site, patients can upload their personal data to it and visitors can also access the stored data after authentication.

TABLE I
Notations

Notations	Descriptions
A_U	The universal attribute set
A_i	User i's attribute set $A_i \subset A_U$
SK_i	User i's secret key set based on its attribute set A_i
$< x_j^A, D_j^A >$	Attribute authentication key set that $D_j^A = g^{x_j^A}$
$H(\cdot)$	One-way hash function
λ	Attribute ccess proof used to access the cloud server

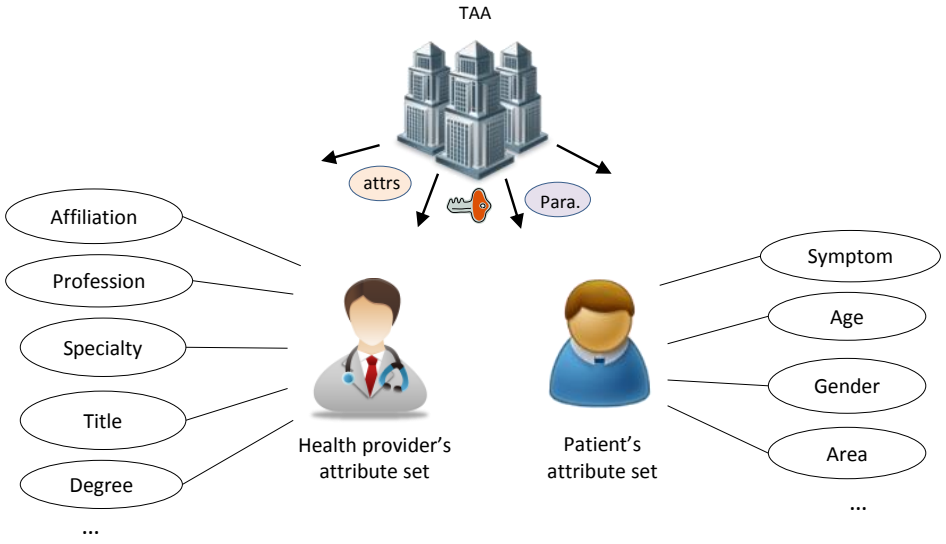

Fig. 1. Attributes of Users.

2) Trusted Attribute Authority (TA): The trusted attribute and key distribution center. TA is in charge of system initialization, including initializing system public parameters, system public key, system master key and universal attribute set, and user registration, including issuing a unique attribute set and the corresponding private key for the registered user.
3) User/Patient: The user that uploads his/her personal data to the cloud server for storage and sharing.
4) User/Visitor: The user that wishes to access to the cloud data.

IV. ABAS: Attribute-Based Authentication Scheme

In this section, we present the proposed attribute-based authentication scheme, which consists of three phases: system initialization, proof generation and proof verification. We also show the proof of the correctness of verification at the end of this section.

A. System initialization

In the initial step, the trusted attribute authority (TA) initializes the whole system using Algorithm $Syst\_Initi()$.

Algorithm $Syst\_Initi(Para, MK_{sys}, PK_{sys})$

- The input of the algorithm is secret $para$, a series of system values, as follows.
  - ▷ TA first formalizes the universal attribute set as $A_U = \{a_1, a_2, ..., a_n\}$
  - ▷ And system master key MK_{sys} and public parameter PK_{sys}
- Its outputs are system master key $MK_{sys} = (\beta, g^{\alpha})$ and public PK_{sys} including bilinear group G_1, bilinear map $e(g, g)^{\alpha}$ and an H that hashes maps to bit-string.

B. Proof Generation:

For a user or visitor VT_i to access a patient's health record, it has to provide a correct attribute-based access proof to the cloud server to achieve authorized access.

Algorithm $Attr\_Proof\_Gen(\lambda)$

- This algorithm achieves generating the authentication attribute proof. To access a cloud server, visitor VT_i
  - ▷ **Step 1.** Generates the description of the required PHR Inf, which is attached with timestamp TS,
  - ▷ **Step 2.** Creates an access proof AP with its secret key set X_{VT_i}, where

$$X_{VT_i} = \{x_j^A\}, \tag{1}$$

based on its attribute set A_{VT_i}. There are several steps to complete this procedure as follows.

1) Chooses attribute subset $\widehat{A}_{VT_i}$, where $\widehat{A}_{VT_i} \subseteq (A_{VT_i} - \overline{A}_{VT_i})$, and $\overline{A}_{VT_i}$ denotes the set of some sensitive attributes.
2) Generates a corresponding index

$$I = \{0, 1\}^n, \tag{2}$$

with n-bit length, i.e. $|I| = n$ as well to indicate which attributes are included in. $I_j = 1$ if $a_j \in \widehat{A}_{VT_i}$; otherwise $I_j = 0$. For instance, if $\widehat{A}_{VT_i} = \{a_1, a_2\}$, we get the corresponding index as $I = 110, ..., 0$.
3) Computes attribute proof as

$$AP = g^{\frac{1}{h(Inf|TS)+\sum_{j\in\widehat{A}_{VT_i}} x_j^A}} \tag{3}$$

- The proof $\lambda = (Inf|TS, i, I, AP)$ is then sent to the cloud server.

C. Proof Verification:

The cloud server then conducts verification before agreeing to the request of care provider, as Algorithm $Attr\_Proof\_Ver(\lambda, RT)$. In particular, the cloud server can empower providers with specific attributes to have the access right, by setting up a certain value to the index IV, where $IV_j = 0$ means "do not care" about the corresponding attribute.

Algorithm $Attr\_Proof\_Ver(\lambda, RT)$

- To verify the λ, The cloud server carries out two-step verification:
  - ▷ **Step 1.** First checks the validity of the received timestamp TS.
  - ▷ **Step 2.** For a valid TS, the cloud server then checks the index, first
  $$I \neq 0, \tag{4}$$
  then compares the received I with IV:
  $$\forall j, I_j - IV_j \geq 0. \tag{5}$$
  Cloud server would continue to next step only if (5) holds; otherwise it would terminate the verification process by return $RT = 0$.
  - ▷ **Step 3.** For a valid I, the cloud server then computes
  $$\iota = \prod_{a_j \in A_U} (I_j \cdot D_j^A)^{(s_i)^{|I^1|-1}} \tag{6}$$
  where $|I^1|$ denote the number of 1 in index I, and further conducts the following verification as
  $$e(g^{h(Inf|TS)} \cdot \iota, AP) \stackrel{?}{=} e(g, g) \tag{7}$$
- The verification succeeds if (7) holds, and the algorithm returns 1.

D. Correctness of Verification:

Suppose there are w 1's in I, we prove the correctness of the verification as follows. Let $Left$ as the left part of (7)-that is $e(g^{h(Inf|TS)} \cdot \iota, AP)$, we get:

$$\begin{aligned} Left &= e(g^{h(Inf|TS)} \cdot (\textstyle\prod_{a_j \in A_U} I_j \cdot D_j^A)^{s_i^w}, AP) \\ &= e(g^{h(Inf|TS)} \cdot (\textstyle\prod_{a_j \in A_U} I_j \cdot g^{v_j \cdot s_i^w}, AP) \\ &= e(g^{h(Inf|TS)} \cdot g^{\sum_{a_j \in \hat{A}_{VT_i}} v_j \cdot s_i^w}, AP) \\ &= e(g^{h(Inf|TS)+\sum_{a_j \in \hat{A}_{VT_i}} x_j^A}, AP) \\ &= e(g, g)^{(h(Inf|TS)+\sum_{a_j \in \hat{A}_{VT_i}} x_j^A) \cdot (\frac{1}{h(Inf|TS)+\sum_{a_j \in \hat{A}_{VT_i}} x_j^A})} \\ &= e(g, g) \end{aligned}$$

If VT_i holds the claimed attributes, verification will succeed. The cloud server then sends the encrypted PHR to the HS upon the required PHR description Inf.

V. Security Analysis

We analyse the security issues of the proposed attributed-based authentication scheme. In what follows, we specifically discuss how the proposed scheme provides sufficient security from the resistance to various pre-defined attacks, including replay attack, forgery and collusion attacks.

A. Resistance to Replay Attack

In authentication proof generation process, time-stamp TS is included as well in the attribute proof λ. Therefore, it can guarantee the proposed scheme to be resistant to replay attack.

B. Resistance to Forgery Attack

An attacker with attribute set A^* and authentication key $X^* =< x_j^{*A} >$ attempts to impersonate user u_i with authentication key $X_{u_i} =< x_j^A >$, and forge the attribute proof λ^* as

$$\lambda^* = (Inf|TS, I, AP^*). \tag{8}$$

If the fake AP^* makes the equations hold:

$$e(g^{h(Inf|TS)} \cdot \iota, AP^*) = e(g, g), \tag{9}$$

the attacker succeeds. We then prove the attacker does not win in forgery attack.

Again, suppose there are m 1's in I; and attacker forges an AP^* with its authentication key as

$$AP^* = g^{\frac{1}{h(Inf|TS)+\sum_{a_j \in A^*} x_j^{*A}}}, \tag{10}$$

while the cloud server computes ι as

$$\iota = \prod_{a_j \in A_U} (I_j \cdot D_j^A)^{(s_i)^{|I^1|-1}} = \prod_{a_j \in A_U} I_j \cdot g^{v_j \cdot s_i^m}. \tag{11}$$

Obviously,

$$e(g^{h(Inf|TS)} \cdot \iota, AP^*) \neq e(g, g), \tag{12}$$

since $h(Inf|TS) + \sum_{a_j \in A}(v_j \cdot s_i^m)$ in ι could not counteract the term $\frac{1}{h(Inf|TS)+\sum_{a_j \in A^*}(v_j^* \cdot s^{*m})}$ in AP^*. Therefore, forgery attack is resisted in the proposed scheme.

C. Resistance to Collusion Attack

This attack is launched by multiple users colluding to create a valid access proof. Attackers will fail in our attribute-based authentication scheme. For instance, user m with A_m and user n with A_n collude, with the attempt to generate a proof with a valid attributes set A'. We assume that $A' \subseteq (A_m \cup A_n)$, which means that the attribute combination of m and n satisfy the attributes requirement and we let w_m's attributes of user u_m and w_n's attributes of user u_n are included here. Even though the colluded attributes A_c satisfies A', the colluded attribute proof AP_c will not be accepted by the cloud server with the reason that AP_c would include term: $\sum_j (v_j \cdot s_m^{w_m} \cdot s_n^{w_n})$, which results in $e(g^{h(Inf|TS)} \cdot \iota', AP_c) \neq e(g, g)$. Since

$$\iota' = \sum_{a_j \in A'} (v_j \cdot s'^{(w_m + w_n)}), \tag{13}$$

and s' was randomly generated by TA and $s' \neq s_m s_n$.

As a result, it is infeasible for colluding attackers to create a valid access proof and our system can resist against collusion attack.

VI. Performance Discussion

A. Communication cost:

We consider total packets that need to be transmitted to finish the authentication process.

A user or visitor (possible some authorized user) transfers the access proof, the size of which is contributed by the required PHR description inf, attribute set $\widehat{A}_{HS}$, AP' and AP_{inf}. Let $N_{\widehat{A}} = |\widehat{A}_{HS}|$ represents the cardinal number of set $\widehat{A}_{HS}$, and l_D is the length of secret key D, where $D = g^x \in G_1$. We then summarize the communication overheads of achieving the establishment of anonymous authentication in attribute-based scheme in Table II.

B. Computational Overhead

We then evaluate computational cost from both theoretical analysis and simulation experiments.We further simulate and measure the execution time of these major contributed operations in PC (Intel) or smartphone platform, the results of which are listed in the next section.

a) Theoretical results: Table. III summarized the computational complexity for the proposed authentication scheme.

b) Environmental setting: Our experiments were performed on a 3.30 GHz Intel Core i5-2500 processor, as well as iOS platform with 512-MB of RAM.

We conduct the experiments with the above setting environment to study the time cost of the major operations in the proposed solution. As is well known by all, both XOR and hash C_H generate extremely low computation costs, which is negligible compared to other operations of the scheme.Let the computational costs of bilinear pairing on mobile and PC platforms are denoted respectively as C_P and C'_P; similarly, the cost of multiplication operations are denoted as C_M and C'_M.

Our simulation results were as follows: on iOS, the time required to compute a C_P is 74.1 ms, and a C_M is 10.4ms; on the PC with the i5-2500 processor, C'_P and C'_M are 2.9 ms 1.0 ms, respectively.

TABLE II
Communication Cost of The Proposed Scheme

User	Communication Cost
Cloud Server	L_{ACK}[a]
User/Visitor	L_{INF}[b] $+2 \cdot L_{RN}$[c] $+ L_I$[d] $+ L_{AP}$[e]

[a] The length of ACK
[b] The length of description information Inf
[c] The length of random number
[d] The length of I: n bits
[e] The length of authentication proof AP

TABLE III
Computational Cost of Two Proposed Schemes in *mSIPS*

User	Computational Cost
Cloud Server	$N_{\hat{A}_{HP}}{}^{*} \cdot C_M{}^{\dagger} + C_M + C_P{}^{\ddagger}$
User/Visitor	$2N_{\hat{A}_{HP}} \cdot C_M + C_H{}^{**}$

[*] The number of attributes in HS selected attribute set $\hat{A}_{HP}$
[†] Computational cost of multiplication operation
[‡] Computational cost of bilinear pairing
[**] Computational cost of a hash

VII. Conclusion

In this paper, we provided an efficient privacy preserving attribute-based authentication scheme for secure cloud computing. The proposed scheme achieved two objectives, i.e. privacy preservation and fine-grained access to patients' personal health records. Through detailed security analysis, the proposed solution was shown to be secure and resisted various attacks including forgery attack, replay attack, and collusion attack, etc. The experimental simulation was further conducted to prove that our scheme was efficient in computational and communication overheads.

References

[1] Ryan M D, " Cloud computing security: The scientific challenge, and a survey of solutions, *Journal of Systems & Software*, 2013, 86(9):22632268.

[2] Wu, Yulin, et al. " Dynamic Data Operations with Deduplication in Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE International Conference on Computational Science and Engineering IEEE*, 2017:562-567.

[3] Xia Z, Wang X, Sun X, et al., "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, *IEEE Transactions on Parallel and Distributed Systems*, 2016, 27(2): 340-352.

[4] Zissis, Dimitrios, and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, 28.3(2012):583-592.

[5] Lu, R., Lin, X. and Shen, X., "SPOC: A secure and privacy- preserving opportunistic computing framework for mobile-healthcare emregency," *Parallel and Distributed Systems, IEEE Transactions on*, Vol. 24, pp. 614-624, 2013.

[6] Pise P D, Uke N J, "Efficient security framework for sensitive data sharing and privacy preserving on big-data and cloud platforms, *International Conference on Internet of Things and Cloud Computing*. ACM, 2016:38.

[7] Farash MS, Attari MA, "An efficient client-client password-based authentication scheme with provable security," *Journal of Supercomputing*, 2014, 70(2):10021022.

[8] Chen TY, Lee CC, HwangMS, Jan JK, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, 2013, 66(2):10081032.

[9] Wang D, Wang N, Wang P, et al., "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity", *Information Sciences*, 2015, 321:162-178.

[10] Jiang Q, Khan M K, Lu X, et al., "A privacy preserving three-factor authentication protocol for e-Health clouds," *Journal of Supercomputing*, 2016, 72(10):3826-3849.

[11] Guo L, Zhang C, Sun J, et al., "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks," *IEEE Transactions on Mobile Computing*, 2014, 13(9):1927-1941.

[12] Zhou J, Lin X, Dong X, et al., "PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributedm-Healthcare Cloud Computing System," *Parallel and Distributed Systems IEEE Transactions on*, 2015, 26(6):1693-1703.

[13] Li J, Chen X, Huang X., "New attributebased authentication and its application in anonymous cloud access service," *International Journal of Web and Grid Services*, 2015, 11(1): 125-141.

[14] Liu H, Ning H, Xiong Q, et al., "Shared authority based privacy-preserving authentication protocol in cloud computing," *IEEE Transactions on parallel and distributed systems*, 2015, 26(1): 241-251.

[15] Liu H, Ning H, Yue Y, et al., "Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices," *Future Generation Computer Systems*, 2018, 78: 976-986.

[16] Liu J K, Au M H, Huang X, et al., "Fine-grained two-factor access control for web-based cloud computing services", *IEEE Transactions on Information Forensics and Security*, 2016, 11(3): 484-497.
[17] Wu F, Xu L, Kumari S, et al., "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks", *Computers & Electrical Engineering*, 2015, 45(C):274-285.
[18] Irshad A, Chaudhry S A, "Comments on A privacy preserving three-factor authentication protocol for e-health clouds, *Journal of Supercomputing*, 2016:1-5.
[19] Chen C L, Yang T T, Chiang M L, et al., "A privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, 2014, 38(11):1-16.
[20] Chiou S Y, Ying Z, Liu J., "Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment," *Journal of Medical Systems*, 2016, 40(4):101.
[21] Chaudhry S A, Farash M S, Naqvi H, et al., "An enhanced privacy preserving remote user authentication scheme with provable security," *Security and Communication Networks*, 2016, 8(18):3782-3795.
[22] Jiang Q, Ma J, Wei F., "On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," *IEEE Systems Journal*, 2016, (99):1-4.
[23] Qiu M, Gai K, Thuraisingham B, et al., "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry", *Future Generation Computer Systems*, 2018, 80: 421-429.
[24] Chaudhry S A, Farash M S, Naqvi H, et al., "A Robust and Efficient Privacy Aware Handover Authentication Scheme for Wireless Networks,"*Wireless Personal Communications*, 2017, 93(2):311-335.
[25] Jeong, Yoon Su, and S. S. Shin, "An Efficient Authentication Scheme to Protect User Privacy in Seamless Big Data Services," *Wireless Personal Communications*, 2016, 86.1:7-19.
[26] Gupta N, Tayal S, Gupta P, et al., "Review on Privacy-Preserving Authentication application in Cloud Computing Sharing," *International Journal of Computational Intelligence Research*, 2017, 13(4): 647-651.
[27] Ruj S, Stojmenovic M, Nayak A. "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE transactions on parallel and distributed systems*, 2014, 25(2): 384-394.