Type: xxx

Cryptoanalysis on a Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System

Jinyong Chang[1, 2, *], Qiaochuan Ren[1] and Anling Zhang[3]

[1] School of Information and Control Engineering, Xi'An University of Architecture and Technology, Xi'An, 710055, shaanxi, P.R. China

[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, P.R. China

3 Department of Mathematics, Changzhi University, Changzhi, 046011, Shanxi, P.R. China

[*]Corresponding Author: Jinyong Chang. Email: changjinyong@xauat.edu.cn

Received: XX Month 202X; Accepted: XX Month 202X

Abstract: The interconnecting of the biomedical sensors (in healthcare system) with cloud for the internet-of-medical-things (IoMT) technology has great potential to ameliorate people's living conditions. The privacy-preserving of personal health information (PHI) and the mutual authentication between the sensors and other entities are two main factors that affect the further applications of cloud-centric IoMT technology. In the recent work [*IEEE IoT Journal, vol. 7(10), 10650-10659, 2020*], Kumar and Chand applied identity-based aggregate signcryption scheme to the smart healthcare system (KC-system, for short), which provides privacy-preserving of PHI and the mutual authentication function, simultaneously. However, in this paper, we carefully analyze the security of KC-system and find out that the critical authentication keys of entities can be easily recovered from their communication contents. In other words, the mutual authentication function of KC-system can be easily broken. Moreover, the recovering of the keys will lead to the tedious processes, including obtaining partial private key (from network manager) and requesting for key-protection (from key-protection servers), become completely useless. Finally, we remark that it seems to be hard to remedy the current KC-system so that it is immune to our attack.

Keywords: Security Analysis, Internet of Medical Things (IoMT), Cloud Computing, Smart Healthcare System.

1 Introduction

Wireless body area network (WBAN) is an emerging paradigm in ubiquitous healthcare, whereby sensors, that are implanted or worn on human body, collect and send real-time patient's personal health information (PHI) data such as breathing rate, heart rate and blood pressure and so on [1]. Typically, WBAN is a kind of network consisting of various tiny sensors, which have limited power, storage as well as computing ability. After collecting patient's PHI, they transmit it to medical professional (or data consumer) via this public network [2].

From security perspective, any attack on the sensors or unauthorized access to the network may result in life-threatening risk to the patients since the transmitted data is just their sensitive PHI [3]. Obviously, the security and privacy problems are the first challenge for the further applications of WBAN [4]. The second challenge lies in that day-to-day increasing transmission of PHI data overburdens the resource-constraint cellular network [5], [6]. Many literatures find that the recent cloud-enabled internet of things (IoT) can be potentially served the data storage and computing power [7]-[9]. Another

advantage of combing cloud with e-health monitoring system is that the remote diagnosing from an authorized medical entity becomes more convenient. However, some new security risks, such as a semi-trusty cloud may be curious to inappropriately access patient's PHI [10], also appear. In addition, how to validate the integrity of the stored PHI on cloud is another critical problem for the cloud-based smart healthcare system [11].

In order to solve the above security and privacy-preserving problems, kinds of cryptographic techniques, like encryption and signature, are considered for the cloud-centric IoMT system to simultaneously ensure privacy and authenticity. In general, encryption and signature can be composed in several ways: Sign-and-encrypt, sign-then-encrypt, and encrypt-then-sign. Each implementation mode is a simple composition of encryption and signature schemes, and thus is inefficient for the IoMT healthcare system.

It is also well-known that signcryption is an important public-key cryptographic primitive, which can achieve authentication and privacy simultaneously with a much smaller cost. Like other public-key cryptographic primitives [12], [13], signcryption scheme has also to face the problem that how to fix the relation between the public-key and its true entity. Identity-based signcryption (IBSC) scheme (see [14]-[17]) can easily bypass this issue since entity's public-key is just its public information, such as email address, identity-card number, and so on. But the key-escrow problem (i.e. any entity's private key is known to the key-generation center) still exists in IBSC schemes. Therefore, researchers suggested the notion of certificateless signcryption scheme and tried to use it to the cloud-centric IoMT healthcare system.

In the recent work [18], Kumar and Chand pointed out that, compared with IBSC, certificateless signcryption cannot achieve the identity-based nature. Therefore, they proposed an escrow-free identity-based aggregated signcryption (EF-IBASC) scheme and constructed a device-to-device aggregated-data communication protocol (see [19]) for cloud-centric smart healthcare system (KC-system, for short), whose security is based on the underlying EF-IBASC scheme. As Kumar et al. claimed, their healthcare system has many merits including PHI's privacy-preserving, mutual authenticity of the entities, because the underlying signcryption scheme can simultaneously provide encryption and signature functions.

Unfortunately, in this paper, we will prove that the critical authentication function of the KC-system cannot be guaranteed because the authentication key(s) can be easily recovered from the communication contents transmitted in the network. In other words, one of the two guarantees (i.e. authentication and privacy) for Kumar et al.'s signcryption scheme is completely broken.

Next, we briefly introduce the underlying idea of our attack and then discuss its consequences.

Recall that, in KC-system, each entity E needs to register and obtain its authentication key d_E from the network manager (NM). In order to avoid the key-escrow problem, the NM only returns a partial private key for E. Moreover, for key's security, E also requests for key protection from many key-protection servers (KPSs), who return the corresponding shares. The key d_E is computed by combining the partial private key (from NM) with the shares (from KPSs).

In the process of data transmission, the jth biomedical sensor (BMS) computes the encryption of the PHI data and signature (under the authentication key d_{BMS}^j). Then send the aggregated message CT_j to personal-assisted device (PAD). Note that, CT_j contains the two items:

$$C_{aggr,j} \in \mathbb{Z}_q^*, \text{ and } E_j = C_{aggr,j} d_{BMS}^j \in \mathbb{G}_1,$$

where $\mathbb{G}_1$ is an additional group with large prime-order q. According to the basic number theory [20], we know that the authentication key d_{BMS}^j can be easily recovered from E_j if $C_{aggr,j}$ is public. Hence, the authentication key d_{BMS}^j (of this BMS) is no longer secure. Similarly, other entities' authentication keys can also be recovered.

The consequences of this attack contain the following two aspects:

1) The exposure of the authentication key leads to the tedious generation of d_E be completely

useless.

2) The mutual authentication function of the KC-system does not work. As a result, malicious adversary may pretend to be legal entity to join in the system and try to break the smart healthcare system.

Finally, we remark that this attack on the KC-system seems to be hard to resist. Until now, we don't know how to remedy it unless one can propose a completely new scheme for the cloud-centric IoMT-enabled smart healthcare system.

Organizations. The following parts are organized as follows. In Section 2, we introduce the system model of IoMT-enabled smart healthcare system. Then recall the construction of the KC-system in Section 3. Next, in Section 4, we present our attack on the KC-system and discuss the consequences of this attack. Finally, conclusions are given in Section 5.

2 System Model of IoMT-Enabled Smart Healthcare System

In this section, we introduce the system model of IoMT-enabled smart healthcare system. As depicted in Fig. 1, it consists of the following six entities.

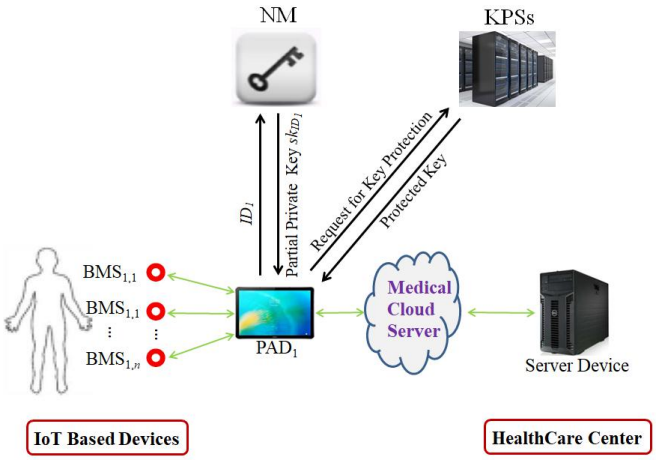

Fig. 1 System Model of IoMT-Enabled Smart Healthcare System

- **Network Manager (NM).** This entity initializes the whole system, and generates the system parameters as well as its own master secret key. In order to avoid the key-escrow problem of the previous identity-based authentication scheme, the NM is viewed as a semi-trusted entity. Therefore, given the identity ID_1, it only returns a *partial* private key.
- **Key-Protection Servers (KPSs).** These entities provide the key-protection services for user's private key. More precisely, they generate their public-secret key pairs, and then compute independent shares to user's protected private key.
- **Biomedical Sensor (BMS).** The whole system includes many BMSs. Each BMS is a tiny sensor and has very limited storage space, battery life as well as computing power. All the BMSs are installed on/outside the patient's body (i.e. some wearable sensors), or deployed in the patient's tissues (i.e. some implanted sensors).
- **Personal-Assisted Device (PAD).** This entity is a data sink, which has sufficient computing power and storage space. In the system, the PAD collects real-time PHI data transmitted from several BMSs and transfers patient's PHI to cloud server for storing (after signing it based on its private key). In fact, it is viewed as not trustworthy entity in Kumar et al.'s model because they think that, for an adversary, it is effortless to physically steal or statistically attack it.

- **Medical Cloud Server (MCS).** This entity provides storing services for the PHI transferred from PAD. In addition, it also provides the accessiability of the stored PHI to SD. It is viewed as a semi-trusted entity.
- **Service Device (SD).** This device is on the medical institution's side, which is allowed to access the PHI stored on MCS, and diagnoses the patient's diseases (based on PHI). Finally, send the prescription to the corresponding BMS in the reverse direction.

TABLE 1. Symbols and Abbreviations.

Symbols	Descriptions
WBAN	Wireless Body Area Network
IoT	Internet of Things
IoMT	Internet-of-Medical-Things
PHI	Personal Health Information
IBSC	Identity-Based Signcryption
EF-IBASC	Escrow-Free Identity-Based Aggregated Signcryption
NM	Network Manager
KPS	Key-Protection Servers
BMS	Biomedical Sensor
PAD	Personal-Assisted Device
MCS	Medical Cloud Server
SD	Service Device

3 Review of the KC-System

Recall that the KC-system consists of the following algorithms:

- **System Setup.** For the security parameter λ, the NM generates a bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive and multiplicative groups, respectively, with the same prime-order q. Let P be $\mathbb{G}_1$'s generator and denote by m, l and t the sizes of message, identity and timestamp (in bits). Then five hash functions are chosen as follows. $H_1: \{0,1\}^l \to \mathbb{G}_1$, $H_2: \{0,1\}^* \to \{0,1\}^{m+l+t} \times \mathbb{G}_1$, $H_3: \mathbb{G}_2 \times \{0,1\}^n \to \mathbb{Z}_q^*$, $H_4: \mathbb{G}_1^m \to \mathbb{Z}_q^*$, and $H_5: \mathbb{G}_1^n \to \mathbb{Z}_q^*$. Next, the NM randomly chooses s_0 from $\mathbb{Z}_q^*$ and defines the public key as $P_0 = s_0 P$. Broadcast P_0 to each KPS^i, who also randomly chooses $s_i \in \mathbb{Z}_q^*$, defines $P_i = s_i P_0$, and returns P_i to the NM. Finally, the NM generates the system public key as

$$Y = \sum_{i=1}^{n} P_i = s_0(s_1 + s_2 + \cdots + s_n)P.$$

- **Entity's Authentication and Registration.** Let $E \in$ {BMS, PAD, SD} and ID_{E} be its identity. First, E randomly chooses $x_E \in \mathbb{Z}_q^*$, computes $X_E = x_E P$, $D_E = x_E H_1(ID_{\mathrm{E}})$, and sends $(ID_{\mathrm{E}}, X_E, D_E)$ to NM, who computes and returns the partial private key

$$(X_{E0}, D_{E0}) = (s_0 X_E, s_0 D_E).$$

  Then E requests to KPS^i for key protection, who computes and returns $D_{Ei} = s_i D_{E0}$ (to E). Finally, E recovers the (full) private key

$$d_E = x_E^{-1} \sum_{i=1}^{n} D_{Ei} = s_0(s_1 + s_2 + \cdots + s_n) H_1(ID_{\mathrm{E}}).$$

- **PHI Aggregate Signcryption.** The jth BMS first randomly chooses $a_j \in \mathbb{Z}_q^*$ and computes

$$A_j = a_j H_1\left(ID_{BMS}^j\right), B_j = a_j P.$$

  Then set $K_j = e\left(a_j d_{BMS}^j, H_1(ID_{SD})\right)$, and compute $S_j^k = H_2\left(ID_{SD}, A_j, K_j, S_j^{k-1}\right)$, where S_j^{k-1} is

the previous key. For the timestamp $T_{i,j} \in \{0,1\}^t$ and PHI $M_{i,j} \in \{0,1\}^m$, the jth BMS computes $h_{i,j} = H_3(M_{i,j}, A_j, T_{i,j})$ and

$$C_{i,j} = \left(a_j + h_{i,j}\right)d_{BMS}^j,\ D_{i,j} = \left(M_{i,j} \| C_{i,j} \| ID_{BMS}^j \| T_{i,j}\right) \oplus S_j^k,$$

where $1 \le i \le m, 1 \le j \le n$. Aggregate the PHI as

$$C_{aggr,j} = H_4\left(C_{1,j}, C_{2,j}, \cdots, C_{m,j}\right) \text{ and } E_j = C_{aggr,j}d_{BMS}^j.$$

Finally, transmit $CT_j = \left\{A_j, B_j, C_{aggr,j}, \Sigma_i D_{i,j}, E_j\right\}$ to PAD.

- **PHI Re-Aggregation.** After receiving the signcrypted data $CT_1, CT_2, \cdots, CT_n$, the PAD re-aggregates them as

  $$C_{PAD} = H_5\left(C_{aggr,1}, C_{aggr,2}, \ldots, C_{aggr,n}\right),\ F = C_{PAD}d_{PAD}.$$

  Then store $CT_{PAD} = \left\{A_j, B_j, C_{PAD}, C_{aggr,j}, \Sigma_i D_{i,j}, E_j, F\right\}$ on the MCS.

- **Public Verifiability.** On stored encrypted data $CT_{PAD} = \{A_j, B_j, C_{PAD}, C_{aggr,j}, \Sigma_i D_{i,j}, E_j, F\}$ on the MCS, anyone in the network can verify the integrity of data as follows.

  Checks the equality

  $$e(F, P) = e(Q_{PAD}, Y)^{C_{PAD}} \text{ and } e(E_j, B_j) = e(A_j, Y)^{C_{aggr,j}}.$$

  If true, the data is complete and correct; otherwise, it is incorrect or missing.

- **Unsigncryption.** After downloading the data CT_{PAD}, SD first computes $K_j^{'} = e(d_{SD}, A_j)$ and $S_j^k = H_2(ID_{SD}, A_j, K_j^{'}, S_j^{k-1})$. Then decrypt the PHI as $M_{i,j}||C_{i,j}||ID_{BMS}^j||T_{i,j} = D_{i,j} \oplus S_j^k$. Finally, accept $M_{i,j}$ if it holds that

$$e\left(\sum_{i=1}^{m}\sum_{j=1}^{n} C_{i,j}, P\right) = e\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_j + h_{i,j}H_1\left(ID_{BMS}^j\right)\right), Y\right) \tag{9}$$

The correctness of the KC-system is discussed and proved by Kumar and Chand in [18].

4 Security Analysis on the KC-System

In this section, we analyze the security of the above KC-system. In particular, we will first prove that the authentication keys for BMS and PAD can be easily recovered, and then analyze its consequences.

4.1 Insecurity of Entities' Authentication Keys

Note that, in the final phase of algorithm "Entity's Authentication and Registration", each entity $E \in$ {BMS, PAD, SD} obtains the authentication key

$$d_E = s_0(s_1 + s_2 + \cdots + s_n)H_1(ID_{\mathrm{E}}) \in \mathbb{G}_1,^{1}$$

which should be secret to anyone else. However, we will analyze that these authentication keys can be recovered by anyone who eavesdrops the transmitted contents among the entities.

Concretely, recall that, in the algorithm "PHI Aggregate Signcryption", the jth BMS signs and encrypts the original PHI messages $M_{1,j}, M_{2,j}, \cdots, M_{m,j}$ into

$$\left(C_{1,j}, D_{1,j}\right), \left(C_{2,j}, D_{2,j}\right), \cdots, \left(C_{m,j}, D_{m,j}\right),$$

[1] If E is the jth BMS, then its authentication key d_{E} is denoted by d_{BMS}^j.

and then aggregates them into

$$C_{aggr,j} = H_4\left(C_{1,j}, C_{2,j}, \cdots, C_{m,j}\right) \in \mathbb{Z}_q^*, E_j = C_{aggr,j} d_{BMS}^j.$$

Finally, send $CT_j = \{A_j, B_j, C_{aggr,j}, \Sigma_i D_{i,j}, E_j\}$ to PAD.

Here, we know that any eavesdropper can see the transmitted CT_j, which includes $C_{aggr,j}$ and E_j. From the two items, the eavesdropper can recover the authentication key d_{BMS}^j of this BMS as follows.

From $C_{aggr} \in \mathbb{Z}_q^*$ and q is a prime, so C_{aggr} and q are relatively prime, we can easily know that there exist integer μ such that

$$\mu C_{aggr} \equiv 1 \ mod\ q,$$

which can be obtained by Extended-Euclidean algorithm.

Hence, it holds that

$$\mu E_j = \mu C_{aggr,j} d_{BMS}^j = \left(\mu C_{aggr,j}\right) d_{BMS}^j = 1\ d_{BMS}^j = d_{BMS}^j.$$

As a result, anyone seeing the content CT_j can easily compute and recover the authentication key d_{BMS}^j of the jth BMS.

In addition, from the description of the algorithm "PHI Re-Aggregation", we know that the PAD will send

$$CT_{PAD} = \left\{A_j, B_j, C_{PAD}, C_{aggr,j}, \Sigma_i D_{i,j}, E_j, F\right\},$$

in which $CT_{PAD} \in \mathbb{Z}_q^*$ and $F = C_{PAD} d_{PAD}$, to the MCS. Similarly, any eavesdropper can easily compute and recover the authentication key d_{PAD} of the PAD from F.

As Kumar and Chand suggested, after obtaining the patient PHI, SD diagnoses it and returns the signcrypted prescription P by using a similar algorithm as "PHI Aggregate Signcryption". In this case, anyone can also recover SD's authentication key by performing a similar analysis as recovering d_{BMS}^j.

In all, the authentication keys can be recovered by any eavesdropper who only needs to observe the communication contents among the entities.

4.2 The Consequence I.

Now, we discuss the first consequence (denoted by Consequence I) of the above attack.

Recall that, in the system-setup step of the KC-system, the NM initializes the system, authenticates the entity with identity ID, and issues partial private key, which is further protected by multiple KPSs, to it. Meanwhile, the KPSs forward the protected private key shares to the entity, who finally combines the shares and extracts its authentication key d_E. We remark that the ultimate goal of these processes is to guarantee that the entity can correctly extract the key d_E.

Since, in our attack, any eavesdropper can easily recover the authentication key d_E, the tedious processes, such as requesting partial private key (from NM) and asking for key-protection (from multiple KPSs), are of no use. Therefore, the first consequence under our attack is that many steps in the algorithms "System Setup" and "Entity's Authentication and Registration" (especially for the latter one) become useless and thus can be "cut" from the KC-system.

4.3 The Consequence II.

Here, we discuss the second consequence (denoted by Consequence II) of our attack. In particular,

the exposure of d_E (for $E \in \{\text{BMS, PAD, SD}\}$) will result in loss of the authentication function of the whole KC-system. In other words, malicious adversary may pretend to be legal entity to join in the system and thus break the smart healthcare system.

Next, we take "malicious BMS" (denoted by BMS^*) for example to show it. According to the description of our attack, BMS^* can easily recover the authentication key d_{BMS}^j of the jth BMS, who is a legal entity in the system. Then it can pretend to BMS_j and interact with other entities as follows.

Randomly choose $a^* \in \mathbb{Z}_q^*$ and compute

$$A^* = a^* H_1\left(ID_{BMS}^j\right), B^* = a^* P.$$

Then set $K^* = e\left(a^* d_{BMS}^j, H_1(ID_{SD})\right)$ and compute

$$S_*^k = H_2\left(ID_{SD}, A^*, K^*, S_*^{k-1}\right),$$

where S_*^k is the previous key. For the timestamp T_i^* and PHI M_i^*, BMS^* computes $h_i^* = H_3(M^*, A^*, T_i^*)$ and

$$C_i^* = (a^* + h_i^*) d_{BMS}^j, D^* = \left(M_i^* \| C_i \| ID_{BMS}^j \| T_i^*\right) \oplus S_*^k.$$

Aggregate the PHI as

$$C_{aggr}^* = H_4(C_m^*, C_m^*, \cdots, C_m^*), \text{ and } E^* = C_{aggr}^* d_{BMS}^j.$$

Finally, send $CT^* = \left\{A^*, B^*, C_{aggr}^*, \Sigma_i D_i^*, E^*\right\}$ to PAD.

Note that this CT^* can pass the public verifiability since it holds that

$$\begin{aligned} e(E^*, B^*) &= e\left(C_{aggr}^* d_{BMS}^j, a^* P\right) \\ &= e\left(C_{aggr}^* s_0 (s_1 + s_2 + \cdots + s_n) H_1\left(ID_{BMS}^j\right), a^* P\right) \\ &= e\left(a^* H_1\left(ID_{BMS}^j\right), s_0 (s_1 + s_2 + \cdots + s_n) P\right)^{C_{aggr}^*} \\ &= e(A^*, Y)^{C_{aggr}^*}. \end{aligned}$$

Obviously, the legal entity BMS_j is successfully replaced by a malicious adversary BMS^*, but the KC-system cannot detect and avoid it. Therefore, the mutual authentication function as Kumar et al. claimed is broken.

4.4 Invalid Public Verifiability Algorithm.

An adversarial cloud server can pass the algorithms "Public Verifiability" auditing, even if it does not well maintain the outsourced data. In other words, the "Public Verifiability" algorithm cannot achieve the expected function.

Specifically, $\Sigma_i D_{i,j}$ in the data packet $CT_{PAD} = \left\{A_j, B_j, C_{PAD}, C_{aggr,j}, \Sigma_i D_{i,j}, E_j, F\right\}$ sent to the cloud by user U can be arbitrarily deleted or modified by the cloud, while $\Sigma_i D_{i,j}$ is the most important in the entire data package, because the user's personal health information $M_{i,j}$ and $T_{i,j}$ are XORed with S_j^k and then stored in $D_{i,j}$.

For example, we assume that the encrypted data $CT_{PAD} = \{A_j, B_j, C_{PAD}, C_{aggr,j}, \Sigma_i D_{i,j}, E_j, F\}$ on the

MCS has been modified to $CT^{*}_{PAD} = \{A_j, B_j, C_{PAD}, C_{aggr,j}, E_j, F\}$, and the verifier runs the algorithm "Public Verifiability". At this time, $CT^{'}_{PAD}$ can still be passed by two equations of "Public Verifiability":

$$e(F, P) = e(Q_{PAD}, Y)^{C_{PAD}} \text{ and } e(E_j, B_j) = e(A_j, Y)^{C_{aggr,j}}.$$

Therefore, the MCS passes the verifier's auditing, even if CT_{PAD} is modified to CT^{*}_{PAD}. The expected public verifiability function is invalid.

5 Conclusions

In this paper, we analyze the security of the KC-system, which is proposed for smart healthcare system. Although Kumar et al. claimed that their system can achieve both the privacy-preserving of patient's health information and identity, and the mutual authentication of the entities included in the system, we proved that their authentication key can be easily recovered from their communication contents. Hence, the complicated processes of the KC-system become completely useless. Moreover, potential attacks may also occur in their smart healthcare system. In addition, we also proved that the KC-system did not achieve the expected public verifiability function.

Funding Statement: This work was supported in part by National Natural Science Foundation of China (No. 61672416; No. 61872284), and in part by Project of Natural Science Research in Shaanxi (No. 2018JM6105, 2019JM118).

Conflicts of Interest: Authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Zhou, "An Improved Lightweight Certificateless Generalized Signcryption Scheme for Moile-Health System," in *International Journal of Distributed Sensor Networks,* vol. 15(1), 1-16, 2019.

[2] M. Kumar, S. Chand, "A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network," in *IEEE Systems Journal,* DOI: 10.1109/JSYST.2020.2990749, 2020.

[3] Y. Zhang, D. Zheng, R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," in *IEEE Internet Things Journal,* vol. 5(3), pp. 2130-2145, 2018.

[4] W. Sun, Z. Cai, Y. Li, et al., "Security and Privacy in the Medical Internet of Things: A Review," in *Security Comm. Net.*, vol. 2018, ID: 5978636, 2018.

[5] J. Chang, B. Shao, Y. Ji, et al., "Secure Network Coding from Secure Proof of Retrievability," in *SCIENCE CHINA Information Sciences,* early access, doi: 10.1007/s11432-020-2997-0.

[6] V. Sureshkumar, R. Amin, V. Vijaykumar, et al., "Robust Secure Communication Protocol for Smart Healthcare System with FPGA Implementation," in *Future Generation Computation Systems,* vol. 100, pp. 938-951, 2019.

[7] Y. Li, Y. Yu, R. Chen, et al., "IntegrityChain: Provable Data Possession for Decentralized Storage," in *IEEE Journal of Selected Areas in Communications,* vol. 38(6), pp. 1205-1217, 2020.

[8] H. Shacham, B. Waters, "Compact Proofs of Retrievability," in *Journal of Cryptology,* vol. 26, pp. 442-483, 2013.

[9] B. Wang, B. Li, Hui Li, et al., "Certificateless Public Auditing for Data Integrity in the Cloud," in *IEEE CNS'2013,* doi: 10.1109/CNS.2013.6682701, 2013.

[10] H. Yan, J. Li, Y. Zhang, "Remote Data Checking with a Designated Verifier in Cloud Storage," in *IEEE Systems Journal,* vol. 14(2), pp. 1788-1797, 2020.

[11] A. Omala, N. Robert, F. Li, "A Provably-Secure Transmission Scheme for Wireless Body Area Network," in *Journal of Medical Systems,* vol. 40(11), pp. 247, 2016.

[12] J. Chang, Y. Ji, B. Shao, et al., "Certificateless Homomorphic Signature Scheme for Network Coding," in *IEEE/ACM Trans. on Networking,* vol. 28(6), pp. 2615-2628, 2020.

[13] H. Xiong, Z. Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks," in *IEEE Transactions on Inf. Forensics Security,* vol. 10(7), pp. 1442-1455, 2015.

[14] M. Kumar, S. Chand, "ESKI-IBE: Efficient and Secure Key Issuing Identity-Based Encryption with Cloud Privacy Centers," in *Multimedia Tool Applications,* vol. 78, pp. 19753-19786, 2019.

[15] J. Chang, H. Wang, F. Wang, et al., "RKA Security for Identity-Based Signature Scheme," in *IEEE Access,* vol. 8, pp. 17833-17841, 2020.

[16] J. Li, H. Yan, Y. Zhang, "Identity-Based Privacy Preserving Remote Data Integrity Checking for Cloud Storage," in *IEEE Systems Journal,* DOI: 10.1109/JSYST.2020.2978146, early access, 2020.

[17] J. Chang, B. Shao, Y. Ji, et al., "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage, Revisited," in *IEEE Communications Letters,* vol. 24(12), pp. 2723-2727, 2020.

[18] M. Kumar, S. Chand, "A Secure and Efficient Cloud-Centric Internet-of Medical-Things-Encabled Smart Healthcare System with Public Verifiability," in *IEEE Internet of Things Journal*, vol. 7(10), pp. 10650-10659, 2020.

[19] A. Zhang, J. Chen, Q. Hu, et al., "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks", in *IEEE Transactions on Veh. Technology,* vol. 65(4), pp. 2659-2672, 2016.

[20] D. Burton, "Elementary Number Theory, 7th Edition," publisher: TMG, ISBN-10: 1259025764, 2012.