Hindawi
Security and Communication Networks
Volume 2018, Article ID 5978636, 9 pages
https://doi.org/10.1155/2018/5978636

Review Article

Security and Privacy in the Medical Internet of Things: A Review

Wencheng Sun,[1] Zhiping Cai,[1] Yangyang Li,[2] Fang Liu,[3] Shengqun Fang,[1] and Guoyan Wang[4]

[1]*College of Computer, National University of Defense Technology, Changsha 410073, China*
[2]*Innovation Center, China Academy of Electronics and Information Technology, Beijing 100041, China*
[3]*School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China*
[4]*SysCan Biotechnology Company Limited, Suzhou 215000, China*

Correspondence should be addressed to Zhiping Cai; zpcai@nudt.edu.cn

Received 2 October 2017; Revised 12 January 2018; Accepted 28 January 2018; Published 29 March 2018

Academic Editor: Huan Chen

Medical Internet of Things, also well known as MIoT, is playing a more and more important role in improving the health, safety, and care of billions of people after its showing up. Instead of going to the hospital for help, patients' health-related parameters can be monitored remotely, continuously, and in real time, then processed, and transferred to medical data center, such as cloud storage, which greatly increases the efficiency, convenience, and cost performance of healthcare. The amount of data handled by MIoT devices grows exponentially, which means higher exposure of sensitive data. The security and privacy of the data collected from MIoT devices, either during their transmission to a cloud or while stored in a cloud, are major unsolved concerns. This paper focuses on the security and privacy requirements related to data flow in MIoT. In addition, we make in-depth study on the existing solutions to security and privacy issues, together with the open challenges and research issues for future work.

1. Introduction

Medical Internet of Things is the group of devices connected to Internet, to perform the processes and services that support healthcare. MIoT has emerged as a new technology for e-healthcare that collects vital body parameters of patients and monitors their pathological details by small wearable devices or implantable sensors. MIoT has shown great potential in providing a better guarantee for people's health and supports a wide range of applications from implantable medical devices to wireless body area network (WBAN).

Generally, the MIoT structure is composed of three layers: the perception layer, the network layer, and the application layer, as shown in Figure 1. The major task of the perception layer is to collect healthcare data with a variety of devices. The network layer, which is composed of wired and wireless system and middleware, processes and transmits the input obtained by the perception layer supported by technological platforms. Well-designed transport protocols not only improve transmission efficiency and reduce energy consumption, but also ensure security and privacy. The application layer integrates the medical information resources to provide personalized medical services and satisfy the final users' needs, according to the actual situation of the target population and the service demand.

The security and privacy of patient-related data are two indispensable concepts. By data security, we mean that data is stored and transferred securely, to guarantee its integrity, validity, and authenticity, and data privacy means the data can only be accessed by the people who have authorization to view and use it [1]. More reasonable protection strategies could be developed according to different purposes and requirements. The widespread use of MIoT devices provides a better guarantee for people's health [2]; however, it also puts much pressure on information security and privacy protection.

The successful development of MIoT must take security and privacy as a core consideration. This paper proceeds as follows. In Section 2, we discuss the security and privacy requirements of medical data. In Section 3, we discuss several technical solutions and research status about security and privacy issues. In Section 4, we compare 4 kinds of

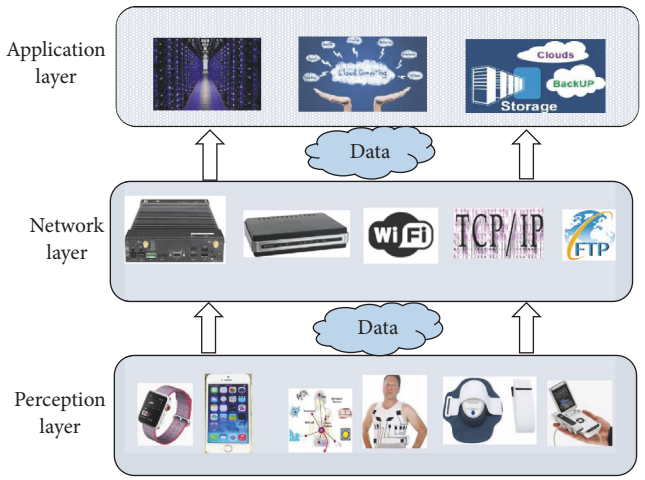

Figure 1: Structure of Medical Internet of Things.

K-anonymity, to verify whether the division of dataset has an impact on security of privacy data. Experiment results demonstrate the effectiveness of the clustering K-anonymity. In Section 5, we discuss the future research challenges and we conclude the survey in Section 6.

2. Security and Privacy Requirement

Although the majority of healthcare organizations do not spend enough resources to protect security and privacy [14], there is no doubt that security and privacy play a key role in MIoT. MIoT devices produce an increasingly large volume of increasingly diverse real-time data, which is highly sensitive. On the one hand, destroying the security of medical system or network could cause disastrous consequences. On the other hand, the patient's privacy information exists at all stages of data collection, data transmission, cloud storage, and data republication. In developing medical Internet security and privacy systems, the following four requirements should be considered.

2.1. Data Integrity. Data integrity refers to the fact that all data values satisfy semantic standards without unauthorized tampering. It includes two levels of accuracy and reliability. Data integrity can be divided into four categories, namely, entity integrity, domain integrity, referential integrity, and user-defined integrity, which can be maintained by foreign keys, constraints, rules, and triggers.

2.2. Data Usability. Data usability is to ensure that data or data systems can be used by authorized users. Big data brings not only great benefits but also crucial challenges, such as dirty data and nonstandard data. In addition, data corruption or data loss caused by unauthorized access also further destroys data usability.

2.3. Data Auditing. Audit of medical data access is an effective means to monitor the use of resources and a common measure for finding and tracking abnormal events. In addition, cloud service providers usually play untrusted roles, which require reasonable auditing methods. Audit content generally includes users, cloud service providers, access, and operation records.

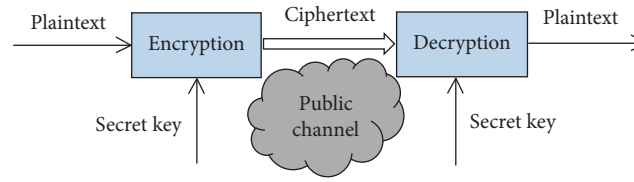

Figure 2: Common model of data encryption and decryption.

2.4. Patient Information Privacy. Patient information can be subdivided into two categories: general records and sensitive data. Sensitive data, which can also be called patient privacy, include mental status, sexual orientation, sexual functioning, infectious diseases, fertility status, drug addiction, genetic information, and identity information. We need to make sure that the sensitive data is not leaked to unauthorized users, or even if data is intercepted, the information expressed cannot be understood by unauthorized users.

3. Existing Solutions

Since MIoT devices do not have sufficient memory, computation, and communication capabilities, they require a powerful and scalable high-performance computing and massive storage infrastructure for real-time processing and data storage. Currently, most MIoT institutions store the collected medical data and deploy their application servers in the cloud. The devices can offload their healthcare tasks to the cloud accordingly. Cloud services through their elasticity and facility to access shared resources and common infrastructure in a ubiquitous and pervasive manner facilitate a promising solution for efficient management of pervasive healthcare data.

3.1. Data Encryption. Cryptography is a security technology for information exchange and communication in accordance with the agreed rules [15]. As shown in Figure 2, plaintext, also known as the original message, is encrypted into ciphertext by the encryption algorithm. Through the public channel, the message is transmitted from the sender to the receiver. The message is then decrypted into plaintext.

General data encryption can be implemented at three levels of communication: link encryption, node encryption, and end-to-end encryption. For any intermediate node in link encryption, the message received from the former link will be decrypted into plaintext and the plaintext will then be encrypted into ciphertext using the secret key of the next link. However, unlike link encryption, node encryption does not allow messages in plaintext form in the network node. Therefore, node encryption can provide high security for network data. When using end-to-end encryption, the message is not decrypted until it is transmitted to the destination. Because messages are always present as ciphertext throughout

Table 1: Security and privacy mechanisms and proposals for data encryption.

Proposals	Technologies	Application	Details
[3]	Key management scheme	Resource-constrained nodes	Solving the issue of the limited resources available through strong encryption and authentication means
[4]	Lightweight private algorithm; DES	Data transmission	Strong encryption considering the characteristic of IoT
[5]	Cloud computing	Monitoring the elder's biological data	Reducing the waste of medical resource
[6]	Authentication scheme	Mobile emergency medical systems	Guaranteeing the confidentiality of sensitive medical data

the transmission, there is no leakage of information even if a node is corrupted.

To secure e-health communications, key management protocols play a vital role in the security process. However, complex encryption algorithms or transmission protocols can greatly affect the transmission rate and even fail to perform data transmission. Furthermore, they need to occupy valuable medical resources which are not available. The tough balance between security protection and system energy consumption needs to be solved with scientific and cautious step. Table 1 shows several data encryption proposals on MIoT.

Owing to the limited resources available and privacy concerns, security issues have been major obstacles to the e-health applications that provide unobtrusive support for elderly and frail people. Abdmeziem and Tandjaoui [3] presented a lightweight end-to-end key management scheme, which is ensuring key exchange with minimal resource consumption. In their proposal, the network is heterogeneous combining nodes with different capabilities. Strong encryption methods and authentication means are used to establish session keys for highly resources-constrained nodes. The proposed protocol is based on collaboration by offloading heavy asymmetric cryptographic operations to a set of third parties. Through security analysis, the scheme can provide strong security features, as well as the scarcity of resources.

Considering the characteristics of IoT and privacy protection, Gong et al. [4] discussed the main problems in current smart healthcare system. Then they designed and completed a prototype system based on a lightweight private homomorphism algorithm and an encryption algorithm improved from DES. Finally, based on the above work, they designed and completed a prototype system based on both software and hardware. Hu et al. [5] proposed a scheme with IoT sensor based on cloud computing which is related to the digital envelope, digital certification, signature, time-stamp mechanisms, and the asymmetric encryption technology, to monitor the elder's biological data and other personal information. The proposed scheme could provide more flexible and accurate medical service as well as reducing the waste of medical resource.

Li et al. [6] proposed a secure authentication and key agreement scheme for cloud-assisted WBAN system using extended chaotic maps, as shown in Figure 3. The design of Chebyshev chaotic maps, based on the concept of Diffie–Hellman key exchange, can create secure ways or

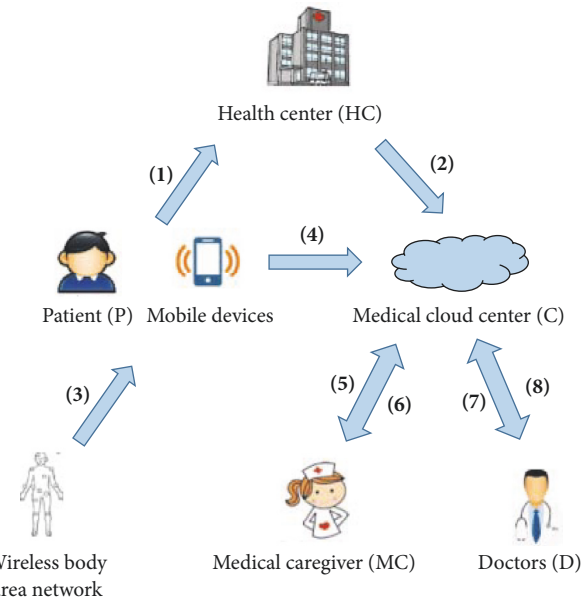

Figure 3: The architecture of cloud-assisted wireless body area network in mobile emergency medical care system.

channels for the system participants when they register. The measured health items collected from body sensors of WBAN would be encrypted before transmission. In order to support real-time analysis with continuous remote monitoring on stream-oriented health items, the monitored patient can authorize medical caregivers to access his/her health items stored in a cloud, which not only provides home care but also improves the life quality. Security and performance analyses showed that the proposed mechanism can effectively address the challenge of participant authentication in mobile emergency medical care systems.

3.2. Access Control. Access control is the means by which a data system defines the identity of a user and the predefined policies which prevent access to resources by unauthorized users [16]. There are various encryption methods applied in access control, including symmetric key encryption (SKE), asymmetric key encryption (AKE), and attribute-based encryption (ABE) [17].

According to general knowledge, cryptography relies on keys. The size and generation mechanism of secret keys

Table 2: Security and privacy mechanisms and proposals for access control.

Proposals	Technologies	Application	Details
[7]	ABE	Access control	Solving the revocation problem of emergency key
[8]	CP-ABE	Medical sensor networks	Supporting complex and dynamic security policies
[9]	ABE	Access control to PHR	Leveraging ABE to encrypt PHR files

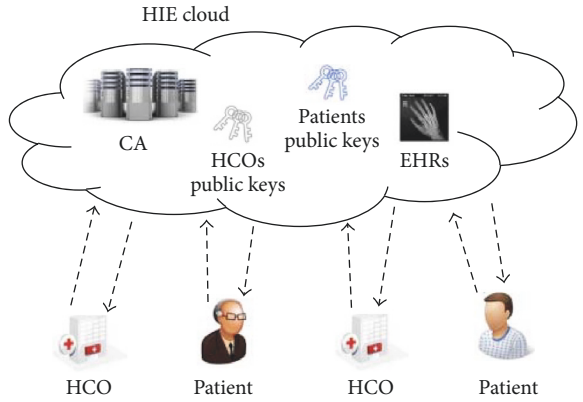

Figure 4: System components.

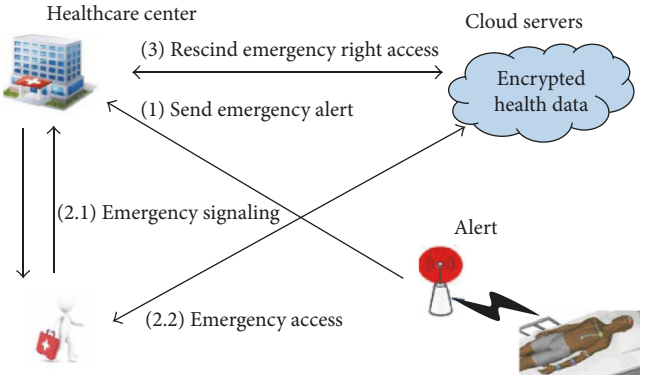

Figure 5: Example of emergency intervention.

directly affect the security of the cryptosystem. Therefore, for a cryptosystem, key management mechanism determines the security system's life cycle. Owing to the scalable key management and flexible access control polices, ABE is gradually becoming one sort of mainstream method. Table 2 shows some access control mechanisms.

In Health Information Exchange (HIE), patient health information can be shared electronically with explicit authorization of information exchange in an auditable manner. However, existing approaches for authorization in health information systems exhibit several drawbacks in meeting the needs of HIE, with noncryptographic approaches lacking a secure and reliable mechanism for access policy enforcement, while cryptographic approaches being too expensive, complex, and limited in specifying policies. Chandrasekhar et al. [18] proposed an authorization protocol for cloud-based HIEs which fills the gap between cryptographic and noncryptographic approaches. The system consists of three main components: the HIE cloud, healthcare organizations (HCOs), and the patients, as shown in Figure 4. They developed a novel proxy signature-based protocol, based on a novel discrete log-based trapdoor hashing scheme, to enable authenticated and authorized selective sharing of patient health information via a cloud-based HIE. According to their detailed security and performance analysis, the proposed protocol, using their trapdoor hash-based proxy signature scheme, achieves the best all-round performance while being provably secure.

Lounis et al. [7] presented an architecture based on attribute-based encryption (ABE), as shown in Figure 5. Since emergency access is temporary, it is crucial to revoke access rights given. However, revocation is a difficult issue in ABE schemes and may generate high overhead. The integer values and integer comparisons [19] were applied to solve the revocation problem of emergency key. In addition, they presented a numerical attribute which has a data value to express validity data of emergency key. Simulations on three scenarios showed that the proposed scheme can reduce the revocation cost and lessen the emergency response time, which means that the scheme can provide an efficient and fine-grained access control.

Lounis et al. [8] proposed a new cloud-based architecture for medical wireless sensor networks and developed an access control that supports complex and dynamic security policies, which relies on ciphertext-policy attribute-based encryption (CP-ABE). Simulation results showed that their access control is efficient, fine-grained, and scalable. Li et al. [9] proposed a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, they leveraged attribute-based encryption (ABE) techniques to encrypt each patient's PHR file and exploited multiauthority ABE to guarantee a high degree of patient privacy.

3.3. Trusted Third Party Auditing. Cloud servers are not fully trusted. The integrity and consistency of medical data stored in the cloud could be compromised if data corruption or even deletion happens without user's permission. For security reasons, the data rules are typically specified by the user, so that the server provider does not have direct contact with the source data. In addition, the Trusted Third Party (TTP) with great reputation which provides the unbiased auditing results can be introduced properly, to enable the accountability of the cloud service providers and protect the legitimate benefits of the cloud users [20]. The research issues

Table 3: Security and privacy mechanisms and proposals for data search.

Proposals	Technologies	Application	Details
[10]	Symmetric key	Supporting privacy preserving string matching	Providing strong privacy guarantees against attacks from a semihonest adversary
[11]	LKE	Searching over encrypted image	Better estimating of edges using smoothing kernels with edges information
[12]	APKS	Searching over encrypted PHR	Allowing users to obtain query capabilities from localized trusted authorities according to their attributes
[13]	CP-ABE	Searching over encrypted PHR	Supporting both fine-grained access control and multikeyword search

of TTP consist of dynamic auditing, batch auditing, and auditing on performance metric.

Over the past decades, many auditing methods have been presented. Several supervised machine learning approaches, such as logistic regression and support vector machine, have been applied to detect suspicious access [21]. However, relying too much on expected judgments and predefined tags restricts their large-scale promotion. Currently, unsupervised approaches attract more attention gradually.

Chen et al. [22] extended the relational learning methods of Malin and colleagues, to construct the global network of departmental interactions. Based on network structure, they proposed two measures to characterize departmental relationships. First, they applied certainty to characterize the strength of departments' interactions over time, which was designed to assess the extent to which changes in the network influence departments' affinity towards one another. Second, they applied reciprocity to measure the extent to which departments exhibit similar behavior with respect to one another. They studied three months of access logs from a large academic medical center and results showed that departmental interaction networks exhibit certain invariants, such as the number, strength, and reciprocity of relationships, and modeling operations at a higher level of granularity such as the departmental level are stable in the context of a relational network, which may enable more effective auditing strategies.

Govaert et al. [23] conduct a preliminary review of the relationship between audits and operating costs. According to their study, surgical auditing can function as a quality instrument and therefore as a tool to reduce costs and further studies should be performed for investigation.

3.4. Data Search. For protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance [24]. The major methods for searchable encryption include searchable symmetric encryption (SSE) and public-key encryption with keyword search (PEKS). And it should be noted that the more complex the encryption measures are, the more difficult the data is searched and the more difficult the consistency of search results is checked. If the search results cannot be applied in a timely manner, then all security and privacy measures have less meaning. Table 3 shows some data search mechanisms.

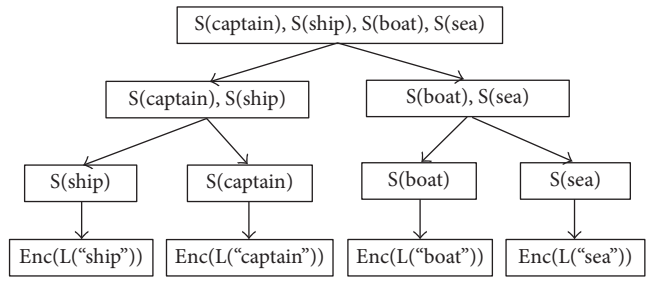

Figure 6: PASS tree example.

To achieve rich querying functionality over the encrypted data, Bezawada et al. [10] developed a symmetric key based approach to support privacy preserving string matching in cloud computing. They developed an efficient and accurate indexing structure, the Pattern Aware Secure Search (PASS) tree, a highly balanced binary tree without revealing any content similarities of the keywords. The action process of PASS tree is shown in Figure 6. Furthermore, they also described a relevance ranking algorithm to return the most relevant documents to the user based on the pattern query. Experiments over large real-life data containing up to 100000 keywords showed that the proposed algorithm can achieve pattern search in less than a few milliseconds with 100% accuracy.

To enjoy the elastic resources and lesson computational burden, personal health record (PHR) is gradually transferred to the cloud storage. Miao et al. [11] designed a secure cryptographic primitive called attribute-based multikeyword search over encrypted personal health records in multiowner setting to support both fine-grained access control and multikeyword search via ciphertext-policy attribute-based encryption (CP-ABE). Figure 7 provides an overview of m2-ABKS scheme. Empirical experiments over real-world dataset were conducted to show its feasibility and practicality in a broad range of actual scenarios.

Methods based on kernel regression can restore the image from its downsampled version with low computational cost, but with low quality around edges. Song et al. [12] proposed a Laplace guided kernel regression method (LKR), in which a novel weighted Laplace map is used to refine the smoothing kernel in KR, and the key insight of LKR is that KR based methods can better estimate edges when using smoothing kernels with edges information. Li et al. [13] formulated

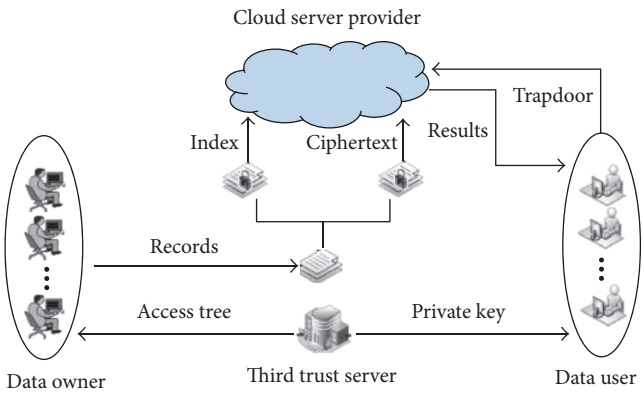

Figure 7: System model of m2-ABKS scheme.

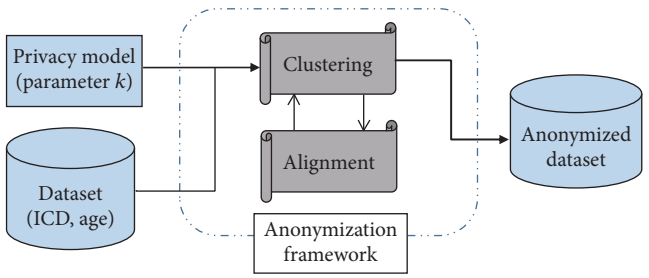

Figure 8: A general architecture of the longitudinal data anonymization process.

and addressed the problem of authorized private keyword searches (APKS) on encrypted personal health record in cloud computing environments. They allow users to obtain query capabilities from localized trusted authorities according to their attributes. In addition to document privacy and query privacy, other salient features of our schemes include efficiently support multidimensional and multiple keyword searches with simple range query and allow delegation and revocation of search capabilities.

3.5. Data Anonymization. Patient sensitive data can be divided into three categories: explicit identifiers, quasi-identifiers, and privacy attributes. Explicit identifier can uniquely indicate a patient, such as an ID number, name, and cell phone number. A combination of quasi-identifiers can also uniquely indicate a patient, such as age, birth data, and address. Privacy information refers to sensitive attributes of a patient, including illness and income. In the process of data publication, while considering the distribution characteristics of the original data, it is necessary to ensure that the individual attributes of the new dataset are properly processed, so as to protect the patient's privacy. At present, random perturbation technology and data anonymous technology are usually used to solve these issues such as k-anonymity, l-diversity, and confidence bounding. In particular, the traditional k-anonymity is widely applied. However, the drawback is that it does not do any constraints on sensitive data, and attackers can use consistency attack and background knowledge attack to identify sensitive data and personal contact, which lead to loss of privacy.

After the study of the privacy concerns of sharing patient information between the Hong Kong Red Cross Blood Transfusion Services (BTS) and the public hospitals, Miao et al. [11] found that there are three challenges, high dimensionality, data utility, and algorithm quality, which limit the application of traditional data anonymization methods. They proposed a new privacy model called LKC-privacy, using two algorithms with different adaptations, to address the problems of centralized anonymization and distributed anonymization. The first adaptation maximizes the information preserved for classification analysis, and the second one minimizes the distortion on the anonymous data for general data analysis. The two algorithms were implemented on two real-life datasets, Blood and Adult. Results showed that the proposed algorithms were flexible and scalable enough to handle large volumes of blood transfusion data with numerical attributes.

Many clustering algorithms can be applied in data anonymization for k-anonymous data. In the context of longitudinal data, the challenge is to define a distance metric for trajectories. Figure 8 provides an overview of the longitudinal data anonymization process. Fung et al. [25] selected the Maximum Distance to Average Vector (MDAV) algorithm [26], an efficient heuristic for k-anonymity, to develop their clustering algorithm. The proposed algorithm iteratively selects the most frequent trajectory in a longitudinal dataset and forms a cluster of at least k records around the latter. In addition, they define the distance between two trajectories as the cost of their anonymization. Experiments on several patient cohorts derived from the EMR system of the Vanderbilt University Medical Center showed that the proposed approach can generate anonymized data that permit effective biomedical analysis, using heuristics inspired from sequence alignment and clustering methods.

Liu and Li [27] introduced a clustering method based K-anonymity algorithm as the building block of privacy preserving for medical wearable devices. The clustering K-anonymity would assign similar records into the same equivalent set, while the similarity among these records make it harder to discriminate different identities than before. Then, they unify the quasi-identifiers in the same clusters by generalizing and suppressing operations. The output of this algorithm is a table that satisfies the principle of K-anonymity. All the records in the same equivalent set are similar to each other. In this way, it would be harder to recognize the users' identities in one equivalent set, and the privacy of these subjects would be securer.

4. Use Case

Security problems appear with the wide deployment of medical wearable devices. The most severe threat would be the privacy leakage of medical wearable devices data. After collecting data from the smart terminals, data holders of medical wearable devices are willing to share the data with application developers to enrich their services or obtain monetary benefits. The data collected contain abundant privacy information. In addition, when sharing the data recorded by

Table 4: Original data.

Height	Weight	Age	Sensitive data
172	63	27	Time serials
178	75	34	Time serials
180	72	26	Time serials
185	77	22	Time serials

Table 5: Anonymity result of original data.

Height	Weight	Age	Sensitive data
17*	**	**	Time serials
17*	**	**	Time serials
18*	7*	2*	Time serials
18*	7*	2*	Time serials

* and ** represent anonymous information.

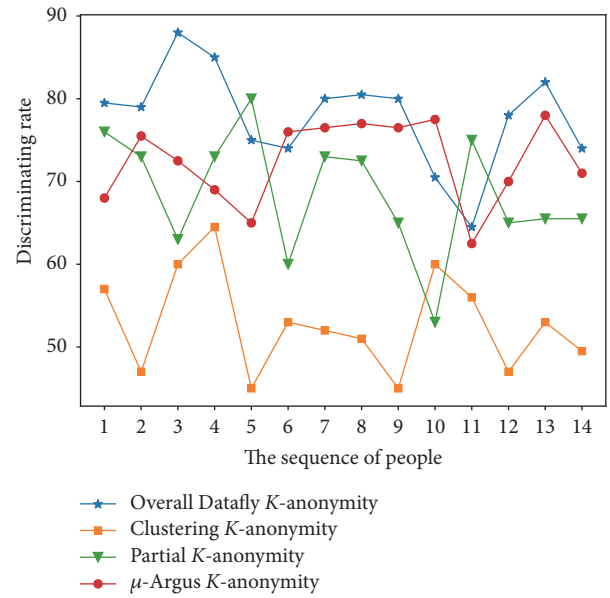

Figure 9: The discriminating rate of 2-anonymity.

human-carried wearable sensors, some personal information, such as age, height, and weight, may also be submitted under warrant. Therefore, though the original intention of data sharing is always positive, the uncontrolled personal information may raise the risk of privacy disclosure.

In this section, we compare 4 kinds of K-anonymity, including Partial Datafly K-anonymity, Overall Datafly K-anonymity [28], μ-Argus K-anonymity [29], and clustering K-anonymity, which are different in the division of datasets. We want to verify whether the division of dataset has an impact on security of privacy data. The data is collected from a real hospital database. Experiment results demonstrate the effectiveness of the clustering K-anonymity.

4.1. An Example of Privacy Disclosure. For example, as Table 4 shows, Alice is an owner of a medical wearable device, and the manufacturer of the device collects the data produced by this device and the information about her age, height, and weight. Then the data holder shared a dataset (as Table 4 shows) which contains Alice's data. The adversary Evil gets this information, and he knows that Alice is 178 cm, 75 kg, and at the age of 34. Therefore, Evil could get Alice's sensitive data readily by combining the dataset with the background knowledge.

The data holder cuts the linkage between identity and sensitive data by generalizing the quasi-identifiers before sharing according to K-anonymity. Table 5 shows the 2-anonymity result of Table 4. In Table 5, it would be hard to recognize Alice's identity with link-attack. However, the data contained in sensitive data could still disclose the identity of Alice. Specifically, if we extract proper feature of these data and put it into a suitable classifier, the identity could be recognized.

4.2. Comparative Results and Analysis

4.2.1. Comparative Results. Figure 9 shows the discriminating rate of the identities in each equivalent set. The dataset is divided according to the principle of 2-anonymity. It is clear that the discriminating rate of clustering 2-anonymity is relatively lower than other 2-anonymity. We can thus claim that the clustering 2-anonymity is the most secure method among the four considered methods.

4.2.2. Analysis. In this experiment, the sensitive data of all the records keep invariant. Because of the different combination about the equivalent set, the discriminating rate in each equivalent set would be different. Reasonable assignment of records improves security level of clustering K-anonymity.

5. Future Challenges of Security and Privacy in MIoT

Any developer in the development of the MIoT security and privacy system will take into account the impact of various factors, to get a better balance among them. In order to achieve a better security environment, several challenges require special attention.

5.1. Insecure Network. Because of the convenience and low cost, a number of devices and software services rely heavily on wireless networks, such as WiFi, which are known to be vulnerable to various intrusions including unauthorized router access, man-in-the-middle attacks, spoofing, denial of service attacks, brute-force attacks, and traffic injections [30]. In addition, most free wireless networks in public place, which have not been certified, are untrusted networks [31].

5.2. Lightweight Protocols for Devices. Low-cost devices and software applications based on sensors should follow specific policy and proxy rules to provide services. At present, if we want to provide high-grade security for the sensors, we must apply the high-cost solutions. It is a conflict in MIoT system. Developing different levels of security protocols according to application scenarios, especially lightweight

security protocols, is the main task of security protection in the future.

5.3. Data Sharing. Despite the rapid development of medical information technology, the phenomenon of information island is increasingly serious. The standards of the data gathered from devices of different manufacturers vary widely, which makes it difficult to unify management. However, the information collaboration and sharing among heterogeneous systems of MIoT constitute the inevitable trend of the future. The privatization of patient information could be very detrimental to the security of the MIoT system. Employing general data policies to combine different data could provide more comprehensible information and enhance security and privacy with hierarchical security model.

6. Conclusion

A variety of medical devices and software applications are applied to improve the quality of medical services and also generate large amounts of data. At present, the importance of data is self-evident. How to effectively protect data security and privacy at all stages of data flow will occupy an important position in future related research. Starting from the security and privacy requirements of MIoT, this paper discusses the security and privacy issues from five technical aspects and presents the challenges of future research. MIoT has been given great attention; however, the related standards and technical specifications are still improving, especially the special application requirements of healthcare, and more successful exploration is needed.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to acknowledge the financial support from the National Natural Science Foundation of China (no. 61379145) and the Joint Funds of CETC (Grant no. 20166141B08020101).

References

[1] J. Tang, A. Liu, M. Zhao, and T. Wang, "An aggregate signature based trust routing for data gathering in sensor networks," *Security and Communication Networks*, vol. 2018, Article ID 6328504, 30 pages, 2018.

[2] W. Sun, Z. Cai, F. Liu et al., "A survey of data mining technology on electronic medical records," in *Proceedings of the International Conference on E-Health Networking, Application and Services*, pp. 1–6, 2017.

[3] M. R. Abdmeziem and D. Tandjaoui, "A cooperative end to end key management scheme for e-health applications in the context of internet of things," in *Ad-hoc Networks and Wireless*, pp. 35–46, Springer, Berlin Heidelberg, 2014.

[4] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," in *Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms, and Programming, PAAP '15*, pp. 217–222, December 2015.

[5] J.-X. Hu, C.-L. Chen, C.-L. Fan, and K.-H. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," *Journal of Sensors*, vol. 2017, Article ID 3734764, 11 pages, 2017.

[6] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, pp. 1–15, 2016.

[7] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure medical architecture on the cloud using wireless sensor networks for emergency management," in *Proceedings of the 2013 IEEE 8th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2013*, pp. 248–252, October 2013.

[8] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.

[9] M. Li, S. Yu, and Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2012.

[10] B. Bezawada, A. X. Liu, B. Jayaraman, A. L. Wang, and R. Li, "Privacy Preserving String Matching for Cloud Computing," in *Proceedings of the 35th IEEE International Conference on Distributed Computing Systems, ICDCS '15*, pp. 609–618, July 2015.

[11] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, "m2-ABKS: attribute-based multi-keyword search over encrypted personal health records in multi-owner setting," *Journal of Medical Systems*, vol. 40, no. 11, article 246, 2016.

[12] C. Song, X. Lin, X. Shen et al., "Kernel regression based encrypted images compression for e-healthcare systems," in *Proceedings of the International Conference on Wireless Communications and Signal Processing*, pp. 1–6, 2013.

[13] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS '11)*, pp. 383–392, IEEE, Minneapolis, Minn, USA, July 2011.

[14] M. Huang, A. Liu, T. Wang, and C. Huang, "Green data gathering under delay differentiated services constraint for internet of things," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9715428, 2018.

[15] Y. Zhao, "Identity-concealed authenticated encryption and key exchange," in *Proceedings of the ACM Sigsac Conference on Computer and Communications Security*, pp. 1464–1479, October 2016.

[16] E. Bacis, S. D. Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, "Mix and Slice: Efficient Access Revocation in the Cloud," in *Proceedings of the 23rd ACM Conference on Computer and Communications Security, CCS 2016*, pp. 217–228, October 2016.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, November 2006.

[18] S. Chandrasekhar, A. Ibrahim, and M. Singhal, "A novel access control protocol using proxy signatures for cloud-based health

information exchange," *Computers & Security*, vol. 67, pp. 73–88, 2017.

[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, May 2007.

[20] V. Venkatesh and P. Parthasarathi, "Trusted third party auditing to improve the cloud storage security," *Wireless Communication*, 2013.

[21] A. A. Boxwala, K. Jihoon, J. M. Grillo et al., "Using statistical and machine learning to help institutions detect suspicious access to electronic health records," *Journal of the American Medical Informatics Association*, vol. 18, no. 4, pp. 498–505, 2011.

[22] Y. Chen, S. Nyemba, and B. Malin, "Auditing medical records accesses via healthcare interaction networks," in *Proceedings of the Annual Symposium proceedings. AMIA Symposium*, vol. 2012, p. 93, 2012.

[23] J. A. Govaert, A. C. M. Van Bommel, W. A. Van Dijk, N. J. Van Leersum, R. A. E. M. Tollenaar, and M. W. J. M. Wouters, "Reducing healthcare costs facilitated by surgical auditing: a systematic review," *World Journal of Surgery*, vol. 39, no. 7, pp. 1672–1680, 2015.

[24] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *Proceedings of the IEEE INFOCOM*, pp. 829–837, April 2011.

[25] B. C. M. Fung, P. C. K. Hung et al., "Centralized and distributed anonymization for high-dimensional healthcare data," *Acm Transactions on Knowledge Discovery from Data*, vol. 4, no. 4, article 18, 2010.

[26] A. Tamersoy, G. Loukides, M. E. Nergiz, Y. Saygin, and B. Malin, "Anonymization of longitudinal electronic medical records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 3, pp. 413–423, 2012.

[27] F. Liu and T. Li, "A clustering k-anonymity privacy-preserving method for wearable IoT devices," *Security and Communication Networks*, vol. 2018, pp. 1–8, 2018.

[28] J. Peng, C.-J. Tang, W.-Q. Cheng, B.-M. Shi, and S.-J. Qiao, "A hierarchy distance computing based clustering algorithm," *Chinese Journal of Computers*, vol. 30, no. 5, pp. 786–795, 2007.

[29] L. Sweeney, "Guaranteeing anonymity when sharing medical data, the datafly system," in *Proceedings of the Conference of the American Medical Informatics Association Amia Fall Symposium*, vol. 51, 1997.

[30] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "PPM-HDA: privacy-preserving and multifunctional health data aggregation with fault tolerance," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1940–1955, 2016.

[31] H. Zhang, Z. Cai, Q. Liu et al., "A survey on security-aware measurement in SDN," *Security and Communication Network*, vol. 2018, Article ID 2459154, 2018.