A Survey on RFID Security and Privacy in Smart Medical: Threats and Protections

Xinghua Shi[1], Jinxuan Cao[1], Tianliang Lu[1] and Victor Chang[2]
[1]*College of Information Technology and Network Security, People's Public Security University of China, Beijing, China*
[2]*Xi'an Jiaotong-Liverpool University, Suzhou, China*

Keywords: Smart Medical, RFID, Threats, Protections, Standards.

Abstract: In recent years, with the rapid development of the Internet of things, smart medical has been gradually integrated into people's lives. Among them, RFID technology in the Internet of things is the most prominent application in the medical and health industry. However, these emerging technologies will bring many security and privacy problems when they are integrated into people's lives. After examining the possible security and privacy threats brought by RFID in smart medical, this paper surveys security requirements most suitable for this industry, and then compares all current RFID security and privacy protection technologies to analysis whether they are suitable for the smart medical industry. Next, the survey sets out the most far-reaching RFID standards and summarized their advantages and shortcomings in smart medical. Finally, the survey puts forward constructive suggestions on security and privacy protections for hospitals and patients involved.

1 INTRODUCTION

Smart medical refers to the establishment of a regional medical information platform for health records by using the most advanced Internet of things technology, which establish interactions between patients and medical personnel, medical institutions and medical equipment, and gradually achieve informatization (Reisenwitz et al., 2018). Radio-frequency Identification (RFID) technology has been widely used in smart medical due to its non-contact communication mode, non-line-of-sight communication process, low hardware cost and accurate positioning target. And because of RFID, the medical industry and the Internet of things industry has been a better combination. At the same time, it can also help the development and popularization of smart medical.

RFID systems (Pokala et al., 2016) use radio waves to read and capture information stored on a body tag that can be read a few feet out of the reader's direct line of sight. RFID has been widely used in smart medical, such as blood drug management, diagnostic IC card, medical equipment and real-time positioning of personnel, etc.

Similar to bar codes, each RFID tag in RFID syst ems can mark a specific device,which leads to that th e information contained in the tag can be easily obtai ned by anyone who holds a reader, which brings man y security and privacy problems (Fernándezcaramés et al., 2017). For example, criminals can identify RFI D tags in wearable monitoring devices so as to locate and track patients, or illegally collect and utilize pati ents' health data for analysis and mining. Under the d rive of huge commercial interests, once data leakage occurs, it will not only affect the public image of the hospital, but damage the patient's personal interests. (Borgohain et al., 2015). For example, Banner Healt h breach in Arizona was hacked, and the personal dat a of 3.7 million patients, employees and customers w ere stolen and misused, which means that 3.7 million people were somehow harmed (HIMSS, 2018). As o ne of the key technologies in smart medical, an in-de pth study of RFID security, privacy threats and their corresponding protection methods is crucial.

This survey first introduces the specific application of RFID in smart medical, and then analyzes the security and privacy threats which may bring to users' data when extending its application in this field. Secondly, aiming at these threats, this survey proposes some currently feasible protection methods for users' data, including physical methods and the use of password-based security protocol to provide RFID authentication security, and analyzes

Shi, X., Cao, J., Lu, T. and Chang, V.
A Survey on RFID Security and Privacy in Smart Medical: Threats and Protections.
DOI: 10.5220/0007713402780285
In *Proceedings of the 4th International Conference on Internet of Things, Big Data and Security (IoTBDS 2019)*, pages 278-285
ISBN: 978-989-758-369-8

the advantages and disadvantages of these methods and the possibility of using them in smart medical from various aspects. The rest of this survey on the analysis of the current international problems existing in the current standard concerning the RFID and put forward in the specific environment of medical wisdom RFID standard requirements. Finally, the remainder of this survey makes recommendations on the existing RFID security and privacy protection methods and standards.

2 BACKGROUND

RFID, one of the core technologies of the Internet of things, provides many benefits for the healthcare industry, including patient safety, tracking, patient-care efficiency and provider satisfaction (Barcode-us, 2018). A typical RFID system structure is shown in Figure 1.

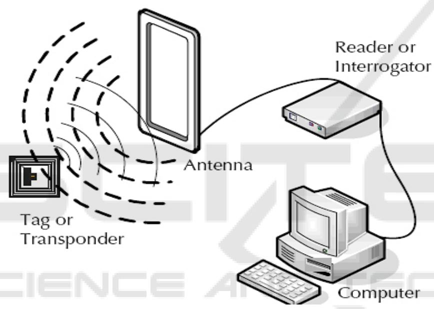

Figure 1: Construction of RFID systems.

According to the power supply mode of labels, RFID tags can be divided into three categories: passive tags, semi-passive tags and active tags (Pontius, 2018). They (especially passive tags) generally can only provide simple security functions; compared with tags, readers composed of application processing unit, RF module, control logic unit and coupling parts for radio frequency communication with tags can usually provide better security. Back-end systems typically contain a database processing system for storing and managing RFID tags' information.

RFID, one of the core technologies of the Internet of things, provides many benefits for the healthcare industry, including patient safety, tracking, patient-care efficiency and provider satisfaction. Because this is also an extension of the Internet of things in the medical industry, it is figuratively called smart medical (Lee et al., 2007). The application of RFID in smart medical can be briefly summarized into the following aspects.

(1) Surgical Instrument Tracking
Many hospitals are using the technique to track surgical instruments and other items by eliminating manual counting to save time, ensure that each item is properly sterilized to reduce the risk of infection, and better manage inventory.

(2) Improving Patient Safety:
RFID can be used to safely manage medicines in hospitals using "smart" cabinets. RFID patient wristbands can also help ensure that patients receive the right dose of each drug at the right time. RFID has even been used in some institutions to track the location of dementia patients and prevent them from getting lost.

(3) Supply Chain Management
Hospitals are under increasing pressure to cut costs. Using RFID to track supplies and medical devices inventory, a supplier can create a solution that automatically triggers a supply order based on real-time inventory information. This helps avoid unnecessary orders and ensures that employees have access to the materials they need.

(4) UDI Compliance
FDA (Food and Drug Administration) requires manufacturers of medical devices to uniquely identify medical devices to help simplify tracking and recall management. By using RFID tags for UDI (Unique Device Identification) applications, manufacturers are able to maintain compatibility while allowing the medical community to more easily track and manage their devices within the medical structure, all without barcode line-of-sight scanning requirements.

(5) Asset Management
Nurses and doctors waste time each week looking for equipment. By connecting RFID tags to wheelchairs, beds, IV pumps and other items, hospitals can locate and improve asset utilization. This saves nursing staff time and helps hospitals avoid unnecessary asset waste by more accurate asset count, which saves both time and capital.

3 RFID SECURITY AND PRIVACY RISKS

3.1 Security Threats

The security threats of the RFID system in smart medical are mainly divided into external threats and internal threats, among which external threats include attacks on tags or readers, front-end and back-end wireless communication channels (Yongming et al., 2014):

(1) Physical Attack
Due to the large scale of RFID tag application, attackers such as some medical service saboteurs can easily obtain tags and analyse or destroy them. (Danev et al., 2009).
(2) Eavesdropping or Skimming
Radio signals sent from tags and readers can be detected by radio receivers a few meters away. If data transmission is not properly protected, some illegal users can access important medical data contained in RFID tags. That is, anyone with a RFID reader can access tags that lack access control and eavesdrop on their content (Roy et al., 2016).
(3) Traffic Analysis
Even with some protection measures for RFID tag data, traffic analysis tools can be used to track and intercept the data response of RFID tags (Jannati et al., 2016).
(4) Spoofing
RFID tag fraud attacks can be carried out based on data collected from 'eavesdropping' or 'traffic interception' attacks. For example, a piece of software called 'RFDump' allows an intruder to override existing RFID tag data with fake data (Jing et al., 2010).
(5) Denial of Service Attack
RFID systems can also be attacked by denial-of-service attacks, which can cause the system to fail to work properly. The attacker's goal is to destroy the system by using a blocking reader to read label information.
(6) Reply Attack
Many RFID systems use encryption technology to ensure the authenticity and integrity of information transmission, so attacks against encryption algorithms are relatively common forms of attacks. Attackers can use brute force attacks to break the encryption algorithm level 1 to decrypt the intercepted password to obtain plain text.
(7) Virus
RFID readers could also be a target for viruses, which researchers have confirmed since 2006. Researchers have written a concept of self-replicating RFID virus, which can be injected through SQL to destroy the back-end system, enough to endanger the whole RFID system data security.

3.2 Internal Threats

Internal threats of RFID security and privacy in smart medical can be regarded as "privacy threats". Because medical data has stronger privacy, that is, stronger "utilization value". There is a data embezzlement case in the United States where the price of stolen medical records is as high as $10 each, which is 10 to 20 times the value of credit card records. Internal threats of RFID mainly include:
(1) Association Threat
One trend of RFID application in smart medical is that "one person, one card" will be rolled out in hospitals large and small all over the world, which means that all information contained by patients in the future will be stored in a small RFID tag. Although realizing the sharing and intercommunication of personal information and medical information, IC card also relates important information such as the patient's id card number and bank card number, which poses a huge threat to patients' personal privacy. Once leaked by some small hospitals or clinics, the consequences are unimaginable.
(2) Location Threat
RFID is often used for intelligent positioning. In some large hospitals, wristbands can help patients receive the appropriate dose of each drug at the right time. At the same time, RFID has even been used to track the location of dementia patients to prevent them from getting lost. But RFID itself can be accurately positioned, if the positioning information is leaked, the personal security of patients is greatly threatened.
(3) Preferences Threat
Wearable devices Based on RFD are able to record patients' medical behaviour and basic health data, such as heart rate, the condition of different organs and some additional data collection including one day's walking routes, residential address, taking medical category, etc. These seemingly irrelevant and insignificant information will expose patients' personal preference of daily life of after data processing and mining. If these preferences in data are sold by manufacturers, patients may be limited by the influence of different level, such as health supplies door-to-door, informal drugs substitute stealthily, extortion, etc. In 2016, more than 200 people living with HIV/AIDS were defrauded for leaking information, which has a big negative impact.
(4) Garbage Collection Threat
RFID is also used by many hospitals around the world to track surgical instruments and drugs for saving time by eliminating manual counts, ensuring whether each item is properly sterilized to reduce the risk of infection, and better managing inventory. However, compared with active and semi-active RFID tags, passive RFID tags used by hospitals are lighter in size and cheaper in price. As a result, many RFID tags carrying drugs or devices are discarded together with drugs, which lead to the threat of garbage collection. Because the discarded RFID tag is not "inactivated",

it may still be reused. The device and drug information contained in it is one of the important private information about the hospital, and the disclosure result will influence personal privacy and hospital secrets.

3.3 Safety Requirements

At present, smart medical is in the initial stage of the world. Whether the external and internal security and privacy threats of the RFID system above can be properly solved directly determines if smart medical treatment can be implemented and applied in life. From the perspective of RFID industrial chain, ensuring the privacy data security of users in RFID requires hospitals or medical equipment manufacturers to abide by basic laws, regulations and ethics. From the RFID itself, ensuring the security of RFID system is to ensure that the information of reader and tag interaction in RFID system real and reliable and not leak to the outside world. The followings are RFID security requirements in smart medicine:

(1) Usability

The protection scheme provided in RFID not only needs to be suitable for all the applications of smart medical, but also be able to provide all legitimate users with various types of services and organize the malicious damage of attackers.

(2) Confidentiality

In the process of medical treatment, as RFID tags often carry items or users' privacy information inside. In order to protect the legitimate rights and interests of hospitals or individuals, it is necessary to ensure the confidentiality of data inside the tag and not be disclosed.

(3) Privacy

RFID tags' privacy mainly includes tracking privacy and information privacy. In the transmission process, data of RFID tags is subject to eavesdropping, traffic interception and other attacks by lawbreakers, which will seriously affect the RFID system and users' privacy. So RFID tags need higher requirements of privacy.

(4) Integrity

Integrity includes physical integrity and data integrity. Physical integrity refers to using RFID tags is not malicious damage to its internal precision circuit structure. Data integrity refers to the RFID data when transmitting is not truncated, damaged by the attacker. When it comes to smart medical, it means to ensure both the authenticity of medical data and the integrity of medical records.

(5) Authenticity

Because the use of RFID in smart medical is bound to involve the Internet, RFID tags face the security threats of the Internet, such as malicious forgery and tampering by hackers. So it is necessary to ensure the authenticity and reliability of RFID data in the process of transmission. In the era of network opening, the effective protection of personal medical privacy in RFID is of great significance for reducing cybercrime or improving the protection of personal information.

(6) Reader Security

Since the most characteristic of RFID passive tags used in smart medical is passive, similar to 'dumb' devices, no matter who sends the request signal, they can only listen and respond, which brings the risk of modifying the tag data without authorization. At this point, Reader needs a higher security ensure. Therefore, we need to put forward higher security requirements for Reader. In addition to its own security, we also need to pay attention to the security of Reader authentication label and tag authentication Reader.

4 RFID SECURITY AND PRIVACY PROTECTION TECHNOLOGY

In view of the security and privacy threats of RFID and the protection requirements under the specific environment of smart medical treatment, corresponding security protection measures must be taken. According to the properties of security protection measures, they can be divided into physical means and cryptographic-based security protocol means:

4.1 Physical Means

In order to protect RFID tags from possible attacks and threats, physical solutions based on RFID itself are the most direct and effective protection methods (Khattab et al., 2017). Physical means can be divided into three categories, respectively, by changing the correlation between RFID tags and specific targets (such as people); Change the uniqueness of RFID tag output information; Hide RFID tag identifiers and data stored in RFID tags (Zhou et al., 2017). Specifically, it includes:

(1) Discarding

'Discarding' refers to the RFID tag from the item after the removal of abandoned. Hospitals, for example, throw away drugs with RFID tags after they use them. Although this method is simple and feasible because it does not involve technical means, as previously analysed, discarded RFID may carry a lot of private information of hospitals or patients, which can be easily collected by others. And if not handled properly, this approach can lead to environmental problems.

(2) Killing

'Killing' refers to the permanent invalidation of RFID tags. 'Killing' can be the destruction of RFID tags internal data, can also be directly destroyed RFID physical circuit (Zhou et al., 2017). For example, after receiving the instruction of "Kill" issued by the reader, the tag will automatically be degaussed becomes invalid, and no operation can be performed thereafter. Although this approach can effectively prevent the privacy disclosure of the tag, once the tag is "Kill", it will completely become invalid and cannot be used again, thus causing waste of its own cost. Because destruction requires technical means and depends on specific equipment, it is too difficult for general hospitals or patients to implement this method.

(3) Sleeping

'Sleeping' is a process in which the tag is temporarily disabled and reactivated when needed. For example, after the tag receives the "Sleep" command from the reader, it cannot respond to any request information for a short time. The tag will not work until the reader tells it to "Wake". However, if each reader can "Wake" the tag, it is not guaranteed to be secure, so different tags need to be authenticated with different passwords.

(4) Faraday Cage

'Faraday cage' (Khattab et al., 2017) is a simple method to protect RFID tags based on electromagnetic shielding principle. The main approach is to use conductive materials to make a "shell" around the label, so as to isolate external electromagnetic waves. But this method can only achieve RFID security in the "cage" inside, for health IC card such a small volume of goods is more practical, but for the detection of vital signs and injected subcutaneous label or attached to the label of medical items is helpless; Secondly, the economic cost of this method is too high.

(5) Relabelling

'Tag redirection' is to ensure the security of information by changing the unique directivity of RFID tag output information. For example, after the purchase of goods, the old serial number of the label can be completely removed, and a new serial number can be written on the label. The information number containing the information of the goods can also be retained, and the serial number containing the original host information can be updated. According to this method, users can control the uniqueness of RFID locally or globally, and hackers cannot easily break their private security. However, there is also a problem that the integrity of the old RFID cannot be damaged to obtain subsequent after-sales service.

(6) Blocker

'Blocker' is a tag that is pre-configured to resemble a known RFID tag ID (blocking ID) (Liu et al., 2017). Different from ordinary RFID tags, blocking tags prevent RFID readers from accessing tag data within a certain range by generating conflicts, thus hiding RFID tags. This method can also be implemented in software, but the implementation is difficult, and how to judge the legal reader and illegal reader is also a difficult problem.

4.2 Security Protocols based on Cryptography

4.2.1 Comparison of Different Protocols

We have analysed physical methods to ensure RFID system security in smart medicine above. According to the analysis results, although the protection mechanism based on physical means solves the system security problem to a certain extent, most methods are difficult to achieve a balance between practicality, effectiveness and cost, and physical methods usually cause label waste is not conducive to environmental protection. At present, the security authentication protocol based on cryptographic technology is the one that can be used most and take into account both system security and label cost. It can be classified according to the cryptographic technology used:

(1) Key (Array)

'Key' is a parameter input in the algorithm that converts plaintext to cipher text or cipher text to plaintext (Gandino et al., 2017). 'Key Array' is an architecture that corresponds to different authentication keys between reader and tag, that is, there is an independent authentication Key between any legitimate tag and legitimate reader in the system.

(2) Zero-knowledge Proof

'Zero-knowledge proof' (Sundaresan et al., 2015) is a protocol that originated in the early 1980s and refers to the ability of a prover to convince a verifier that an assertion is true without providing any useful information to the verifier.

(3) (Pseudo) Random Numbers

Because the number generated by the random number generator is random and independent each time, the random number cannot be reproduced and predicted (Shi et al., 2016). The random number generated on the computer is a pseudo-random number, which is often used to improve the security and confidentiality of RFID authentication protocol.

(4) Elliptic Curves

'Elliptic curve' (He et al., 2015) is defined in the limited domain Z_q on the elliptic curve expressed by E = (q, a, b, G, n, h). All of the points on the curve satisfy the Formula (1) (2):

$$y^2 = x^3 + ax + b(mod\ q) \tag{1}$$

$$\mathrm{a, b} \in \mathrm{Z_q}, 4\mathrm{a}^3 + 27\mathrm{b}^2 \neq 0(\mathrm{mod\ q}) \tag{2}$$

G is an n order point on the curve E, which is called the product point; H is the cofactor of n, namely, the quotient of the number of points on the elliptic curve E divided by order n, which means $\mathrm{h} = \#\mathrm{E}(\mathrm{Z_q})/\mathrm{n}$. Elliptic curve-based security protocol authentication USES the authorization of offline authentication technology, and when Reader changes, RFID tags do not need to be redistributed keys.

(5) Hash

'Hash' (one-way Hash function) is a commonly used encryption algorithm, because information of any length can be hashed as a fixed Hash value by it, which can make the original information difficult to be derived and prevent conflicts in specific use, thus balancing the cost and security of the system (Yu et al., 2016). This method can be further divided into hash-chain method and Hash Lock method.

4.2.2 Requirements of Protocol Design

Security protocols based on cryptography largely weigh the practicality, effectiveness and cost of physical means. Such 'active defence' based on RFID itself means the security and privacy of RFID can be guaranteed from the manufacturer, which is stronger than the 'passive defence' means adopted by end users. However, it can be seen from Table 3 that password-based security protocol protection means still cannot achieve the best effect in all aspects of smart medical treatment, so there is still a large space for development. In addition to ensuring the economic cost, implementation difficulty and encryption effectiveness, the following factors should be considered in the design process:

(1) Medium/Lightweight

As mentioned earlier, RFID passive tags are mainly applied in smart medical. That is to say, due to limited resources, they cannot provide a very perfect distribution and operation environment, so the protocol designed must be medium/lightweight to effectively support it.

(2) Offline

Reader can provide some security without maintaining real-time connection with the background server.

(3) Scalability

Scalability refers to the algorithm designed of protocol is not affected by the overall size.

(4) Integration of New Technologies

Due to the rapid development and extension of emerging technologies, the protocol designed had better be able to keep pace with The Times, such as cloud computing, fog computing, etc., to achieve the best security.

5 RFID STANDARD AND PRINCIPLE

Technical standards are standards for technical matters that need to be coordinated and unified in the field of standardization. It is based on the level of science and technology and practical experience in different periods, aiming at the universality and repetition of technical problems, the best solution. RFID standard system mainly includes RFID technology standards, RFID application standards, RFID data content standards and RFID performance standards. Here's the major RFID standards: ISO/IEC (ISO, 2014), EPCglobal (Lv et al., 2017) and UID (Ubiquitous ID Center, 2016).

In May 2009, the European commission published a recommendation on 'Privacy and Data Protection Impact Assessment Framework for RFID applications'. It aims to provide member states with legal, ethical, social and politically acceptable guidance on the design and operation of RFID applications while respecting privacy and ensuring that personal data are protected. The PIA (Privacy and Data Protection Impact Assessment) framework proposed by the European commission divides RFID applications into four levels (Vuong et al., 2010):

Level 0: applications that do not process private data and operate on RFID tags only by the user are definitely excluded from the PIA framework.

Level 1: the application does not handle private data and RFID tags are still carried by individuals.

Level 2: the application processes private data but the RFID tags themselves do not contain privacy.

Level 3: RFID tags in an application contain personal privacy data.

If the RFID application level is 1 or above, the RFID operator is required to perform a four-part analysis of the application and provide detailed explanations commensurate with the privacy and data protection impact of the determination.

Although PIA put forward different degrees of requirements for operators, but the use of RFID technology in smart medical is very different from other fields. First of all, medical health data often involves more personal privacy, that is to say, RFID operation should be more strictly managed in medical industry. Second, the four levels of PIA described above are too general to be fully applicable to the smart healthcare industry due to RFID usages are more widely and complex. For example, the collection and use of patient privacy data in RFID for human vital signs detection is certainly different from that in RFID for drug or blood management. Is PIA perfect for both of these two or more situations? Therefore, we believe that not only an appropriate framework should be established for the use of RFID in smart medical, but a more granular division should be made on the use of private data at all levels.

6 SOME SUGGESTIONS

In view of the deficiencies and requirements of existing RFID security and privacy protection technologies and standards analysed above, the following Suggestions are put forward for individuals (patients), hospitals and international standard-setting agencies:

From electronic medical records to various medical and health detection products, RFID technology in smart medical is targeted at a large number of legal citizens, but once key private data are leaked or hacked, the victims of adverse effects are also this group of people. In particular, patients of smart blood pressure and cardiopulmonary test health care products are mostly elderly people, who are more vulnerable to security and privacy threats. Therefore, individuals should pay attention to personal privacy protection. First of all, medical IC cards containing personal sensitive information, electronic medical records should be properly kept and strong passwords should be designed. Next, because RFID devices are generally connected to the Internet, so individuals also need to pay attention to the network of common hacker attacks, on time to kill viruses, healthy Internet access.

Because hospitals are not only the victims of RFID security and privacy threats, but also the initiator of many problems, the situation in hospitals is much more complicated than individuals. On the one hand, we think hospitals should not only have the responsibility to ensure the privacy and data security of patients, although the application of big data, cloud computing or Internet of things technology is very popular now. Hospitals should establish specialized RFID security and privacy protection mechanisms, which may include cloud computing data service platform with strong encryption and strict RFID tag purchase, use and disposal mechanism. At the same time, hospitals should also arrange and formulate professional and technical personnel for regular management and examination, and do their best to protect patients' sensitive information. On the other hand, the hospital is also the user of RFID technology, so RFID should be involved in the hospital departments of doctors and nurses to popularize RFID security and privacy protection knowledge, in order to prevent problems in this part of the hospital.

As for the international RFID standards setting bodies or committees, they should make more in-depth research on the RFID standards and should not neglect them, because we have noticed that the latest standards specifically targeted at RFID are now some time apart. “Sb-327 Information Privacy: Connected Devices”, recently passed in California, is not specifically related to the security and privacy of RFID, let alone RFID in smart medical. As mentioned above, it is very necessary for relevant international organizations to formulate relevant standards or laws to restrict hospitals or RFID manufacturers based on the particularity of RFID application in smart medical

7 CONCLUSIONS

In this survey, we have introduced in detail the security and privacy threats and protection methods involved in RFID in smart medical. And we put forward original and innovative constructive Suggestions for existing methods or standards respectively from individuals, hospitals and international standard-setting agencies, which can provide some reference for relevant organizations and individuals involving RFID in the work or life. Only by restricting and managing RFID industrial chain from all aspects can users' privacy and security information not be infringed. Also only like this, people can enjoy the Gospel brought to mankind by smart medical instead of information security being lost in the rapid process of science and technology.

REFERENCES

Cathy Reisenwitz et al., 2018. Smart Medical Devices That Are Changing Healthcare in 2018. In *Medical Software*.

Pokala, J. P. et al., 2016. A secure RFID protocol for Telecare Medicine Information Systems using ECC. In *International Conference on Wireless Communications*.

Fernándezcaramés T. et al., 2017. Reverse engineering and security evaluation of commercial tags for rfid-based iot applications. In *Sensors*, 17(1), 28.

Tuhin Borgohain et al., 2015. Technical Analysis of Security Infrastructure in RFID Technology. In *Eprint arXiv, 1505.00172*.

HIMSS, 2018. The biggest healthcare data breaches of 2018 (so far). Available from: *https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far*.

Barcode-us, 2018. What is RFID? Available from: *https://www.epc-rfid.info/rfid*.

Nicole Pontius, 2018. What are RFID Tags? Learn How RFID Tags Work, What They're Used for, and Some of the Disadvantages of RFID Technology. In *Industry Resources*.

Lee B. et al., 2007. Ubiquitous RFID Based Medical Application and the Security Architecture in Smart Hospitals. In *International Conference on Convergence Information Technology*.

Jin Yongming et al., 2014. RFID Lightweight Authentication Protocol Based on PRF. In *Journal of Computer Research and Development*, 51(7), 1506-1514.

Danev B. et al., 2009. Physical-layer identification of RFID devices. In *Proceeedings of the 18th USENIX Security Symposium*, 199-214.

Roy F. et al., 2016. RFID Eavesdropping Using SDR Platforms. In *International Conference on Applications in Electronics Pervading Industry*.

Jannati H. et al., 2016. Security analysis of a RFID tag search protocol. In Information Processing Letters, 116(10), 618-622.

Jing B. et al., 2010. Anti-spoofing system for RFID access control combining with face recogntion. In *International Conference on Machine Learning & Cybernetics*.

Khattab A. et al., 2017. RFID Security Threats and Basic Solutions. In *Springer International Publishing*.

ZHOU et al., 2017. Provable-secure Offline RFID Mutual Authentication Scheme in the Smart Healthcare Environment. In *Journal of Chinese Computer Systems*.

Liu X. et al., 2017. RFID Estimation with Blocker Tags. In *IEEE/ACM Transactions on Networking*, 25(1):224-237.

Gandino F. et al., 2017. A security protocol for RFID traceability. In *International Journal of Communication Systems*, 30(6).

Sundaresan S. et al., 2015. Zero knowledge grouping proof protocol for rfid epc c1g2 tags. In *IEEE Transactions on Computers*, 64(10), 2994-3008.

He D. et al., 2015. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. In *IEEE Internet of Things Journal*, 2(1), 72-83.

Shi L. et al., 2016. RFID mutual authentication protocol on pseudo-random hash function with shared secrets. In *Journal of Electronics & Information Technology*.

Yu Y. et al., 2016. Research on a provable security RFID authentication protocol based on hash function. In *Journal of China Universities of Posts & Telecommunications*, 23(2), 31-37.

ISO, 2014. Available from *https://www.iso.org/standards.html*.

Lv M. L. et al., 2017. An improved RFID anti-collision algorithm based on the standard EPCglobal class-1 generation-2[C]. In *IEEE*.

Ubiquitous ID Center, 2016. Available from *http://www.uidcenter.org/*.

Vuong C. et al., 2010. Polysaccharide intercellular adhesin (pia) protects staphylococcus epidermidis against major components of the human innate immune system. In *Cellular Microbiology*, 6(3), 269-275.