7-1-2017

A Privacy Preserving Framework for RFID Based Healthcare Systems

Farzana Rahman
Marquette University, farzana.rahman@marquette.edu

Anwarul A. Bhuiyan
Marquette University

Sheikh Iqbal Ahamed
Marquette University, sheikh.ahamed@marquette.edu

Accepted version. *Future Generation Computer Systems*, Vol. 72 (July 2017): 339-352. DOI.

A Privacy Preserving Framework for RFID Based Healthcare Systems

Farzana Rahman
Department of Computer Science, James Madison University, VA
Md Zakirul Alam Bhuiyan
Department of Computer & Information Sciences, Temple University, PA
Sheikh Iqbal Ahamed
Department of Mathematics, Statistics & Computer Science, Marquette University, WI

Keywords

RFID, Privacy, Healthcare, Electronic Medical Record, Security

Abstract

RFID (Radio Frequency IDentification) is anticipated to be a core technology that will be used in many practical applications of our life in near future. It has received considerable attention within the healthcare for almost a decade now. The technology's promise to efficiently track hospital supplies, medical equipment, medications and patients is an attractive proposition to the healthcare industry. However, the prospect of wide spread use of RFID tags in the healthcare area has also triggered discussions regarding privacy, particularly because RFID data in transit may easily be intercepted and can be send to track its user (owner). In a nutshell, this technology has not really seen its true potential in healthcare industry since privacy concerns raised by the tag bearers are not properly addressed by existing identification techniques. There are two major types of privacy preservation techniques that are required in an RFID based healthcare system—(1) a privacy preserving authentication protocol is required while sensing RFID tags for different identification and monitoring purposes, and (2) a privacy preserving access control mechanism is required to restrict unauthorized access of private information while providing healthcare services using the tag ID. In this paper, we propose a framework (PriSens-HSAC) that makes an effort to address the above mentioned two privacy issues. To the best of our knowledge, it is the first framework to provide increased privacy in RFID based healthcare systems, using RFID authentication along with access control technique.

1. Introduction

The Radio Frequency Identification technology (RFID) is growing so fast that few application sectors can beat that scorching rate of growth. RFID is a technology for automated identification with radio waves. It has three main parts: RFID tags, an RFID reader and a central server. RFID tags have an antenna and a tiny data chip for information storage and are commonly installed on objects or products that need to be identified. The content of the chip can be read/written with an RFID reader which is connected to the server [1], [2].

Near field communication (NFC) [3] is a similar technology like RFID with much less capability. NFC is a subset of RFID that limits the range of communication within 10 cm or 4 inches. However, one advantage of NFC is that some mobile phones are being equipped with NFC now a day. However, this advantage of NFC is overshadowed by its limitations, like NFC has a very limited range and it cannot be programmed like active RFID tags. Therefore, it cannot be used in applications where the reading range has to be in meters. It cannot be used in many sophisticated applications where the active tag has to be programmed for special purpose. Specially, in most of the healthcare applications (like: pharmaceutical drug tracking, patient specific meal dispatch and such sophisticated application) longer range and tag programming capability is required. Since RFID tags can be read in longer range and it can be programmed for special purpose, it has become popular over the last decade in many real life application areas including healthcare.

RFID technology can provide a number of benefits to the healthcare industry, improving overall safety and operational efficiency because it operates without line-of-sight while providing immense capabilities. In fact, RFID can contribute to create the hospital of the future by improving patient care

and safety, optimizing the workflows, reducing the operating costs, and reducing costly thefts. There are a number of ongoing trials and studies at hospitals and healthcare centers around the world utilizing and integrating RFID into their hospital information systems. One study estimates that the market for RFID tags in healthcare will rise rapidly from $90 million in 2006 to $2.1 billion in 2016. Primarily, this will be because of item level tagging of drugs and Real Time Locating Systems for staff, patients and assets to improve efficiency, safety and availability and to reduce losses [4].

By attaching RFID tags to different entities in healthcare industry (people and objects), RFID technology can provide tremendous automation in identification, tracking, monitoring and security control measures. Some of the most promising RFID based systems that are already being successfully tested (or deployed) are patient identification and monitoring, patient's drug usage monitoring, surgical instrument tracking and locating, newborn identification, hospital personnel identification and tracking, blood bag tracking, detecting pharmaceutical counterfeit, avoiding theft of medical equipment, tagging of meal plateaux to ensure patients get the appropriate diet, ensuring proper identification of laboratory specimens, restrict access to high threat areas of the hospital to authorized staff, etc. In a patient identification system of an RFID based hospital every patient is identified using an RFID tag installed wristband [5]. A reader is used to identify the ID of the tag which allows the system to identify the patient uniquely. It also allows doctors, nurses and other hospital personnel to access the medical information of the legitimate patient from the server, using the tag ID. The ID can also be used to access various healthcare services, for example, identifying and dispatching prescribed medicine for a particular patient.

In spite of several ongoing researches on RFID based healthcare systems [6], [7], there are still some significant research challenges that need to be addresses. RFID tags generate vast quantities of information while used in healthcare services, but information systems and enterprises need to find ways to ingest, analyze, and archive that huge volume of data [8]. These capabilities directly affect the major issues currently experienced by healthcare organizations while helping to drive down costs [9]. There are many ways that big data methods could improve health outcomes. The more data that is aggregated about a given condition using RFID tags and sensors, the better researchers and clinicians might be able to trace what interventions have worked well and which have not been effective. Moreover, personalization algorithms could create ever more customized approaches for patient management. However, the big data collected over a period of time also allows scope for third party to perform security infringements and privacy violations. The inherent capability of precise and reliable identification attracts RFID systems in the area of tracking applications. This potentiality, however, can put individual privacy at a risk. A threat to consumer privacy is one of the major obstacles in the widespread deployment of RFID systems. A field trial of RFID embedded loyalty cards in Europe was canceled due to consumer protest over privacy concerns [10]. Another legal law violation have been reported against RFID application tracking kids on school buses, even though the RFID chips were installed on the buses for better route navigation and communication purposes [11]. The use of RFID chips in retail industry has been negatively reposted and protested recently all over North America [12]. Additionally, plenty of healthcare applications using RFID chips are always facing controversy from consumer and government due to potential privacy leakage of its users [13], [14]. Many tracking application used in E-Passports, consumer shopping, smart keys and such everyday applications have gone through strong opposition from users and policy makers since there are potential chances of

privacy violation [14]. Hence, security and privacy are the two most important issues that must be addressed before the enormous deployment of RFID tags in omnipresent environment. Our proposal in this paper offers a unique methodology to ensure more privacy for the big data collected from an RFID system.

The security and privacy problems of RFID based applications become even more critical when it is used in healthcare environment which typically deals with sensitive human (patient) information. We have identified the following four major security and privacy related research challenges in RFID based healthcare systems. First, RFID tags can be read at a small distance, through materials, even without the knowledge of its owner. Second, if the communication between tags and readers is performed in wireless environment, any unauthorized reader may try to track the tag to access user's private information. Third, data collected from RFID tags can potentially be used by multiple users (doctors, nurses, pharmacists etc.) and multiple organizations to provide various healthcare services. Fourth, the ID of the RFID tags along with its Electronic Medical Record (EMR), collected over a period of time, may expose significant private information of user such as: trace of personal health information, clinical history and financial information. In a nutshell, RFID technology has not really seen its true potential in healthcare since above mentioned four privacy concerns are not properly addressed by existing techniques.

1.1. Our major contributions

In this paper, we make an effort to address the above-mentioned four challenges with following contributions:

- We point out two major privacy concerns in RFID based healthcare systems: *privacy concerns in RFID sensing* and *privacy concerns in RFID based healthcare service access*.
- In this paper, we propose a framework (PriSens-HSAC), consisting of two major components that can address the above-mentioned two privacy issues respectively.
- The PriSens component proposes a group based anonymous authentication protocol to solve the tradeoff between the scalability and privacy problem of RFID sensing in healthcare. This component provides more privacy and discloses less information than existing RFID authentication schemes. The novelty behind our idea is to preserve privacy in RFID sensing by introducing the notion that adversary cannot break unlinkability with probability better than random guessing. This component addresses the first two challenges mentioned before. PriSens component ensures that no sensitive information is disclosed to the adversary even if a tag's information is read by an adversary, without the knowledge of its owner.
- The HSAC component proposes a privacy preserving healthcare service access mechanism to maintain user's privacy while accessing various healthcare services. This component uses P-RBAC (see Section 7) based access control mechanism to allow access to sensitive information only to authorized users. This component addresses the last two challenges mentioned before. HSAC component ensures that the EMR associated with a specific RFID tags identifier is only

accessible by authorized users, hence ensuring privacy of the RFID based information system used in the healthcare environment.

- We also present the evaluation of the framework by measuring the level of the achieved privacy. Our evaluation clearly illustrates that our proposal provides better privacy in RFID based systems applied in a healthcare setting.

The rest of the paper is organized as follows. Section 2 presents the motivation of our work. In Section 3, we present relevant related work. In Section 4, we discuss the privacy issues of RFID tag sensing in healthcare setting. In this section, we also discuss the privacy issues in RFID based healthcare service access. In Section 5, we present the architecture of our proposed framework. Then we present the group based anonymous authentication protocol (PriSens) in Section 6. In Section 7, we explain the working methodology of HSAC component in detail. The security and privacy analysis of PriSens protocol is presented in Section 8. In Section 9, we evaluate our framework by measuring the privacy level provided by PriSens protocol. In Section 10, we briefly discuss the benefits of using RFID in healthcare systems and our proposed framework. Finally, we conclude the paper in Section 11.

2. Motivation

2.1. RFID in healthcare

There are certain fundamental properties of all RFID information systems that are particularly relevant to privacy, regardless of the specific application type or deployment scenario. RFID tags contain unique identifiers, indicating not only the presence of an object, like a product bar code, but also an individualized serial number. The ability to uniquely identify individual items has privacy implications when those items can be associated with people. RFID tag data can be read/written at a distance, without line-of-sight and through many camouflaging materials, potentially without the knowledge or consent of the individual who may be carrying the tag. RFID information systems can also capture time and location data, upon which item histories and profiles can be created, making accountability for data use critical. When such systems are applied to people, it may be viewed as surveillance.

With the deployment and use of RFID technology in the healthcare domain, there are increasing privacy concerns regarding the technical designs of RFID systems. If RFID tags contain personal information, which could include health information, or data linked to personally identifiable individuals, without the proper security or integrity mechanisms in place, privacy interests become prominent. Personal health information is among the most sensitive types of information. As such, it requires stronger justifications for its collection, use and disclosure, rigorous protections against theft, loss and unauthorized use.

While RFID technology can improve the overall quality of healthcare delivery, the benefits must be balanced with the privacy and security concerns. The use of RFID introduces a new set of risks: security risks are associated with the possible failure of the RFID system under various security attacks, i.e. tracking, eavesdropping, and denial of service, while the threat to privacy resides in the capabilities to permanently save and link information about individuals through temporal and spatial extension of data collection activities. Although concerns about information privacy are not unique to the

healthcare domain, health related information can be perceived as more personal and more sensitive. Due to the highly personal and sensitive nature of healthcare data, both healthcare providers and patients can be expected to resist further digitalization though the usage of RFID technology until security and privacy protections is in place. Usually, RFID based sensing activities related to healthcare can be divided in two types:

Direct sensing activity: These activities refer to various identification and monitoring systems. Some of the most promising RFID based direct sensing activity that are already being successfully tested (or deployed) in a number of hospitals are: hospital personnel [5], patient and newborn identification and monitoring [5], patient's drug usage monitoring [15], surgical instrument tracking and locating [16], and blood bag tracking [15].

Indirect inferred activity: These activities use direct sensing activity data to infer important information. For example, detecting pharmaceutical counterfeit, avoiding theft of medical equipment, the tagging of meal plateaux to ensure that patients get proper diet according to their treatment, allergies and tastes etc.

Fig. 1 illustrates a simple architecture of an RFID system in healthcare. It has two individual modules: (1) *RFID Sensing Module*—consisting of all the RFID identification and monitoring systems. (2) *Service Provider Module*—consisting of all the systems that use legitimate RFID identification data to provide various healthcare services (ex. physician's diagnosis, prescription, medicine usage chart, specialist's opinion, insurance verification, appropriate medicine dispatch, etc.). Some simple example scenario of RFID tag usage in healthcare area can be as follows:

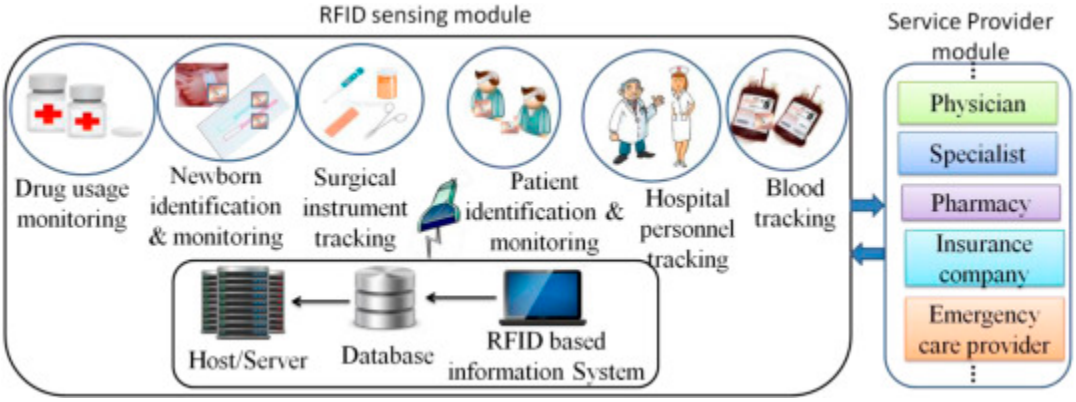

Fig. 1. An RFID based ubiquitous healthcare system.

Medicines' authenticity tracking: Ensuring the origin of medicines is essential to guarantee their quality. RFID tag based identification and authentication methods can guarantee the origin of medicines, especially in pharmaceutical supply chains. Electronic Product Codes (EPC) (e.g. a serial number) in RFID tags are used to track each individual medicine along the supply chain. Each EPC/RFID tag is attached to a drug unit. Thus, it is possible to track every individual drug unit and to verify its authenticity. An attacker can exploit this tracking mechanism to lead to potential privacy violation of the drug user.

Patients' drug dispatch: Usually, in case RFID based hospitals, a patient is identified using RFID installed wristband [5]. The medical information of the legitimate patient is then pulled up from the central database and passed onto the physician's PDA which is a part of the service provider module. The physician's system may suggest medicine based on diagnosis and the pharmacy system may use the prescription to dispatch proper medicine for the patient. An attacker can exploit the information system of the pharmacy to lead to potential privacy violation of its user.

Financial transactions: Depending on the health care system, patients must pay for the service that they receive. In addition, health care providers must be able to verify that a given patient is covered under a particular plan, what specific procedures, lab tests, and whether dependents are covered. In this case, RFID can be used to identify patients using wristbands [5] which can pull up all those information in seconds for hospital bill calculation. Any attacker can use their own reader to impersonate as a legitimate reader and can read patient's wristbands to gain further access to patent's personal information.

Patients' disease monitoring: Wide varieties of methods have been used to identify patients when they are in hospitals. One of the most popular methods is based on using a wristband in which a bar code is printed. However, recently the barcode based bracelets have been replaced by RFID tag based bracelets [5]. In some chronic diseases, continuous monitoring of patients is very important. RFID technology could be used to send information from patients to a control system. The control system could activate an alarm based on the received data.

2.2. Two fold privacy preservation

RFID has received considerable attention within the healthcare since early 2000. The technology's promise to efficiently track hospital supplies, medical equipment, medications and patients is an attractive proposition to the healthcare industry. However, the prospect of wide spread use of RFID in the healthcare area has also triggered discussions regarding privacy. Some major research challenges related to the development and deployment of RFID based healthcare are as follows:

- RFID tags can be read at a small distance. If the communication between tags and readers is performed in wireless channel, adversary may try to infer personal information to track people remotely.
- Deployed ubiquitous healthcare systems may have both access permission and privacy invasion problems for the patient's individual medical data that may be overheard by unauthorized persons trying to access the system stealthily.
- The information sensed using RFID tags may need to be shared with various authorities to access healthcare services. The ID of the tag along with its EMR, collected over a period of time, may expose user's private information.

It is evident that in RFID based healthcare systems, the privacy concerns are twofold and we need to have twofold privacy management mechanism in place: (1) *A privacy preserving authentication protocol is required while sensing RFID tags. This protocol will preserve privacy when different*

identification and monitoring process are executed in "RFID sensing module" of Fig. 1, (2) *A privacy preserving access control technique is required while receiving services from "service provider module" of* Fig. 1 *to ensure user preferred privacy level is achieved*.

With this privacy mechanism in place, the true potential of an RFID based healthcare system can finally be exploited. The widespread adoption of such privacy preserving RFID based healthcare system will open doors for various assisted care, remote health monitoring, and elderly care systems. Eventually, it will help to ensure quality healthcare facilities, longer life expectancy, reduced death rate, and preserve patient's privacy.

3. Related work

The HSAC component of the PriSens-HSAC framework uses P-RBAC [17] as part of the HSAC component. There are plenty of role based access control techniques in the literature. In [18], the authors propose an enhanced role based access control mechanism for hospital information systems. However, the authors did not consider privacy issues. Purpose based access control (PBAC) models also have been proposed to protect sensitive data [19], [20], but the purpose is difficult to define. Jin et al. propose a framework for e-Health systems [21], which supports patient-centric selective sharing of virtual composite e-Health data using different levels of granularity. However, it focuses on the framework only and does not discuss a detailed approach for policy definition and management. Attribute based access control (ABAC) adopts XACML [22] to define policies, and transform them into access control lists (ACLs). However, commercial DBMS kernel cannot support XACML and thus existing ABAC module in databases is implemented in and on the fly basis. This brings high performance degradation for the database.

The major component of PriSesn-HSAC framework is PriSens which is an RFID authentication protocol. Several authentication protocols have been proposed to secure RFID systems against major attacks. RFID security based research area can be divided into two categories. The first category is protocol based. This category mainly focuses on implementing protocols using secure, lightweight primitives on small RFID tags in order to ensure security and privacy. The second category is hardware based and this category focuses on improving RFID tag hardware so that it can provide additional security primitives. Our focus is on the first category. So we will not discuss about the hardware based category. However, interested readers can refer to [1], [23] for more details.

Within the area of the protocol based on category numbers of techniques have been proposed for ensuring RFID security and the assortment of authentication protocols is quite extensive. Back-end database played an essential role in most early works on RFID security. Researchers came up with highly secure protocols but authentication was done mostly by the back-end server rather than the reader itself.

Weis et al. [24] proposed authentication protocol which used back-end database to perform the authentication. Under this scheme, an RFID tag replies with a different value each time it is queried by a reader as each reply of the tag involves a random number. This protocol is more suitable when an

RFID system wants to provide strong security. However, this protocol is not very convincing for providing strong privacy of RFID tag bearers.

Another lightweight protocol is OSK [25]. Ohkubo, Suzuki and Kinoshita proposed that two hash function H and G are sufficient to provide indistinguishability and forward secrecy. Here, H is a one way hash function and G has random oracle. According to this protocol, a tag is initialized with a shared secret and the back-end server maintains a list of tags (id, s_i). The tag updates its secret key after each query according to the following formula $s_{i+1} = H(s_i)$. And in response to the query from a reader, the tag replies $a_i = G(s_i)$. The server on the other hand uses a_i to identify the tag by performing a brute force search through the list of tags. OSK does not ensure scalability.

In [26], Avoine and Oechslin modified OSK which removed the scalability problem. They introduced a time–memory trade off which reduced the computational complexity for inverting the hash function. But this feature was achieved at the cost of increased memory.

Another problem of OSK is that a malicious reader may easily desynchronize a tag which eventually results in DOS attack. Another hash function based authentication protocol was proposed by Seo et al. [27] which ensures scalability. This protocol is also untraceable. The most significant contribution of this paper is scalability and forward secrecy. One of the main drawbacks of this protocol is that ownership transfer requires external intervention.

Seo et al. proposed another authentication protocol [28] that ensures high scalability and ownership transfer. It is a lightweight authentication protocol that employs a proxy in addition to the back-end server. The protocol is based on Universal Re-encryption which allows the back-end server to get the tag identifier only after a simple decryption. This decryption requires a constant time which makes it one of the highest scalable authentication protocol. But its application area is restricted because of the use of proxy. This protocol is best suited for personal use. But it suffers from the problem of traceability and some other security issues such as DOS attack and swapping.

YA-TRAP [29] is a famous authentication protocol that places little burden on the back-end server. The principle advantage of this protocol is that the central database avoids any real time processing. Authors proposed that YA-TRAP is really advantageous in situations where tag information is processed in batches rather than in real time. The fundamental idea of this protocol is based on monotonically increasing timestamp which makes this protocol secured against tracking. But the use of the timestamp makes this protocol unsecured against DOS attack. In this protocol, an RFID tag update its timestamp based on a value provided by the reader. At the same time each tag stores $T_{\max}$, where $T_{\max}$ is the maximum value that can be reached by the timestamp. When the timestamp reaches $T_{\max}$ a tag does not answer to the reader's queries. Hence an adversary can send the tag a large enough timestamp so that it goes beyond $T_{\max}$. Thus it becomes quite easy for a malicious reader to create DOS attack. Although the solution to DOS was proposed in $\mathrm{Y\ A\text{-}TRAP} +$ [30], this protocol still lacks forward secrecy.

In [31], Hoque et al. proposed a serverless authentication protocol for RFID system. But their system is also more focused on defending various attacks without the help of central database. Moreover, in their system, the reader has to do a lot of computation to find out

of the required tag. In [32], the authors proposed an RFID authentication protocol that supports not only security and privacy, but also recovery in RFID systems. The protocol can get back the desynchronized tags and readers to their normal state, and thus provides robustness. The focus of this system was to defend against various attacks, rather than provide better privacy for the RFID tag owners.

In [33], Hoque et al. proposed a privacy preserving RFID authentication protocol. However, this protocol is not entirely suitable for RFID based healthcare systems, since it does not address the unique privacy requirements of RFID based healthcare systems, where the tag owner's privacy needs to be enhanced.

Private authentication techniques proposed to protect user privacy in RFID systems can be classified into two categories, non-tree-based approaches and tree-based approaches. Non-tree-based protocols usually perform linear search, $O(N)$, to find out a tag. But, the linear search is not efficient for systems with huge number of tags. Another non-tree-based approach, Hash-lock [24] method uses the hash value of a key to identify a tag. Molnar and Wagner proposed a tree based approach in [34] that reduces the complexity of authentication from $O(N)$ to $O(logN)$.

Numbers of research have been conducted to find out a trade-off between the complexity and the level of privacy provided by the key-tree based scheme. This trade-off is identified and analyzed by Avoine et al. in [35], by Buttyan, Holczer, and Vajda in [36], and more recently by Nohl and Evans in [37]. These papers quantify the level of privacy provided by the key-tree based scheme when some tags are compromised. Avoine et al. proposed a group based private authentication scheme in [38] that improves the tradeoff between scalability and privacy. But the privacy level decreases as more and more tags are compromised. Another authentication technique proposed by Zhou in [39] focuses on utilizing fewer resources on the tags for authentication. However, even though they we able to achieve more security and efficiency, their proposed approach did not focus on providing privacy for the users. HB-family protocols based on LPN assumption are also booming as one of the attractive candidates for secure low cost protocols based on EPC tags [40] due to its security against quantum adversaries, efficient computational time and memory requirement etc. However, their focus was to design a secure authentication protocol to meet the demand of low-cost tags. A summary of most of the major protocols are shown in Table 1.

Table 1. Comparison of existing techniques.

	Complexity	Cloning resistance	Tracking resistance	Privacy protection
OSK [25]	$O(N)$	Yes	Yes	Yes
Weis [24]	$O(1)$	No	No	No
Tree based [34]	$O(\log N)$	Yes	No	Yes
Group based [38]	${}^{1}O(\gamma)$	Yes	Yes	Yes
Avoine 05 [35]	$O\left(N^{2/3}\right)$	Yes	No	Yes
Dimitriou [41]	$O(\log N)$	Yes	No	Yes
Henrici and Müller [42]	$O(1)$	No	No	Yes
Seo [27]	$O(\log N)$	No	No	Yes
Serverless [31]	$O(N)$	Yes	Yes	Yes

Our proposed PriSens-HSAC framework provides higher level of privacy and security, both in terms of RFID sensing and EMR accessing. The framework provides more privacy in RFID based healthcare system by proposing a better privacy preserving authentication protocol and by using P-RBAC while accessing healthcare services. To the best of our knowledge, PriSens-HSAC is the first framework to provide increased privacy in RFID based healthcare systems through the usage of RFID authentication along with access control technique. Though our major motivation in these paper is to enhance the privacy of users in an RFID based healthcare system, our proposed PriSens-HSAC framework addresses all of the security requirements too. PriSens-HSAC framework has scope not only in healthcare industry, but also in other applications where privacy of tag bearers is an important issue.

4. Privacy concerns in RFID systems

4.1. Privacy issues in RFID sensing

Ensuring strong privacy in RFID sensing imposes a higher complexity on the reader. Conversely, improving efficiency may hamper some privacy. Here, our main focus is on the tradeoff between privacy and scalability of RFID systems.

Molnar and Wagner [34] first proposed a *tree based hash protocol* for RFID systems to reduce the search complexity of the reader from $O(N)$ to $O(log_{\alpha}N)$, where α is the branching factor at each level of the tree. But this approach achieves better scalability at the cost of some privacy loss of the tags [37]. Fig. 2(a) shows a balanced key tree with $N = 8$ and $\alpha = 2$. Suppose the tag T_3 in Fig. 2(a) becomes compromised. All the tags of the system are partitioned into three disjoint sets. The adversary can now uniquely distinguish the tag T_4 and identify the tags T_1 and T_2 as a unique partition. All the remaining

tags (T_5, T_6, T_7, T_8) form a single partition because the tag shares no key with them. Therefore each tag of this partition (T_5, T_6, T_7, T_8) is anonymous among these four tags. The privacy provided by this scheme diminishes as more and more tags are compromised.

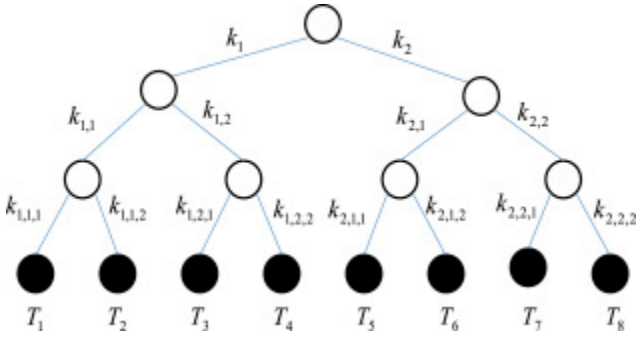

Fig. 2(a). (a) Tree based hash protocol with $N = 8$ and $\alpha = 2$.

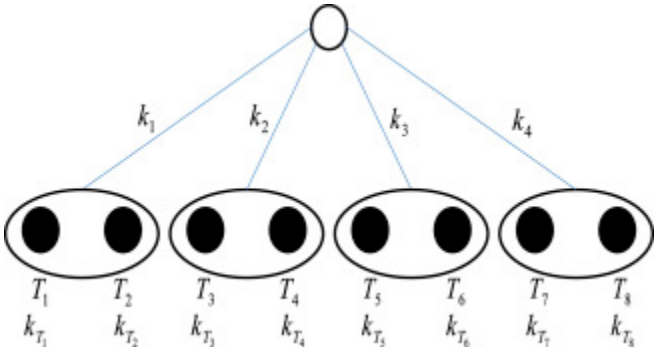

Fig. 2(b). (b) Group based protocol, with $N = 8$ and $\gamma = 4$.

Fig. 2. Two privacy preserving RFID authentication protocols.

Avoine et al. [38] proposed a *group based authentication protocol* to address the privacy problem of the tree based hash protocol. According to this protocol, tags are divided into γ disjoint groups of equal size. Fig. 2(b) shows the group organization of the tags where $N = 8$ and $\gamma = 4$. This protocol reduces the complexity of both the reader and the tag. The tag always has to perform two encryptions. In the worst case, the reader has to perform $\gamma + 1$ encryptions. In addition, each tag needs to store only two keys for the authentication. The group organization of this protocol improves the level of privacy. For instance, if the tag T_3 is compromised, the adversary can uniquely identify only the tag T_4 (see Fig. 2(b)). The adversary cannot uniquely distinguish the other tags $T_1, T_2, T_5, T_6, T_7, T_8$. Each of these tags remains anonymous among these six tags. Like other protocols, this protocol also has some limitations. There is a tradeoff between the number of groups and the group size. To address this problem, we propose an efficient anonymous private authentication (PriSens) scheme that allows the tags to have more privacy (i.e. less information disclosure) by keeping the reader's complexity within a practical range. However, PriSens is much better than the other schemes, in terms of providing more privacy, where the worst case reader's complexity is $O(N)$ (where N is the number of total tags in the system). To provide improvement in privacy preservation, PriSens incurs small increase in the

complexity of the reader. Since readers are more powerful than the tags, they can handle this increase in search complexity. Therefore, this protocol is specifically suitable for healthcare since its main goal is to achieve scalable automation as well as preserve privacy.

4.2. Privacy issues in RFID based healthcare service access

The ID of the RFID tag identified by PriSens, may need to be shared with physicians, pharmacy, insurance company and emergency care providers to access various healthcare services. This information, collected over a period, may expose significant private information such as trace of personal location, health information etc. To address this, we propose a privacy preserving access control technique to restrict unauthorized access of patient's private information.

5. Architecture of PriSens-HSAC framework

To solve the two major privacy issues in RFID based healthcare systems, we propose PriSens-HSAC, a framework consisting of two major components. One component is PriSens that proposes a group based anonymous authentication protocol to solve the tradeoff between the scalability and privacy of RFID sensing in healthcare. PriSens provides more privacy with efficiency than existing RFID authentication protocols. We discuss the details of PriSens in Section 6. The second component is HSAC that proposes a privacy preserving healthcare service access mechanism to maintain user's privacy while accessing various healthcare services. HSAC follows the concept of role based access control mechanism to restrict unauthorized access to private data. We discuss the details of HSAC component in Section 7. The architecture of the framework is shown in Fig. 3.

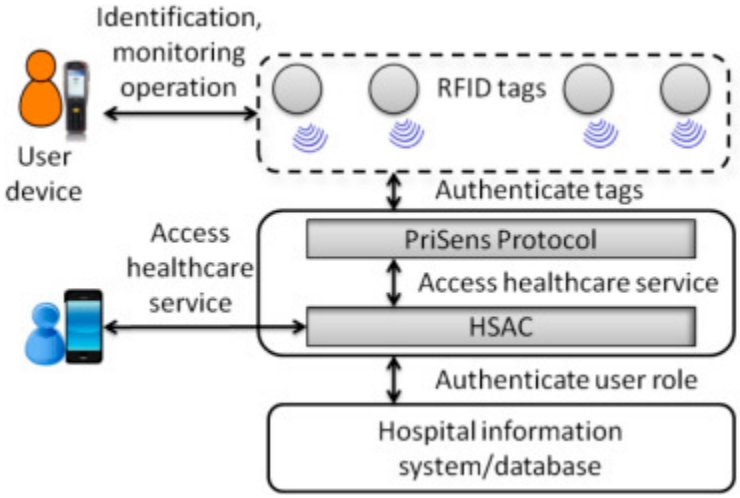

Fig. 3. Architecture of PriSens-HSAC framework.

When any RFID based identification or monitoring operation takes place in a healthcare system, the reader as well as tags in concern executes PriSens protocol to preserve user privacy. It is important to notice that PriSens can preserve privacy and defend against attacks launched by the outsider adversary. For example, if any unauthorized reader tries to launch any attack in the RFID information

system of the hospital or tries to violate user privacy (by tracking the user), PriSens can defend against the launched attacks and provide better privacy compared to the other existing protocols [34], [38]. If any unauthorized user wants to access any healthcare service (ex. access patient's medical history using the ID of the tag), HSAC will not allow the user to access that service using a privacy aware role based access control mechanism [17]. Therefore, it is evident that PriSens component will run in tags and reader. Nevertheless, HSAC component can be executed in user's mobile devices, central server or any other machines that uses ID if the RFID tag to access healthcare related services.

6. Overview of PriSens protocol

In this sub-section, we will describe the details of PriSens (Group based Anonymous Authentication Protocol for RFID Sensing) Protocol.

6.1. Privacy characterization in PriSens

In literature, several different notions of privacy have been proposed so far. Some authors mention *information privacy* as the privacy of RFID systems. This privacy notion is the act of preventing a tag from disclosing its product information [25], [24]. But protecting information privacy keeps tags traceable. Therefore, it is a weak notion of RFID privacy. Some define *unlinkability* as the strong notion of RFID privacy [37], [43]. Unlinkability means the inability to distinguish between the responses from the same tag and the responses from different tags of the system. Providing unlinkability ensures strong privacy when the adversary cannot distinguish between two tags with a probability better than random guessing [2]. In our protocol, we protect privacy of the tags by providing unlinkability between two tags of the system.

The level of privacy obtained by any protocol can be measured using the *anonymity set*. *Anonymity* has been proposed in the context of mix-nets in [44]. Mix-nets are used to make the sender (and the recipient) of a message anonymous. The anonymity set is defined as the set of all potential senders (recipients) of the message. Anonymity is defined as being not identifiable among a group of entities, i.e., the members of the anonymity set. A higher degree of anonymity is achieved with an anonymity set of larger size. Perfect anonymity is achieved if anonymity set contains all the members capable of sending (receiving) messages in system.

6.1.1. System model of PriSens

In our protocol, tags are divided into groups of equal size. Suppose, N is the total number of tags in the system and τ is the number of groups. So, the group size is $n = \frac{N}{\tau}$. Next, we define the components and parameters of our system.

Issuer. The issuer initializes each tag during the deployment by writing the tag's information into its memory. The issuer also authorizes the reader access to the tags. Even each group receives its unique group key and a pool of identifiers from the issuer.

Group. Each group has a n number of tags. The issuer assigns a unique group key k_{G_i} to the ith group G_i of the system. This key is shared between the members (tags) of this group. Each group also receives the following pool of identifiers from the issuer $\xi_i = \{\mathrm{ID}_{i,1}, \mathrm{ID}_{i,2}, \dots, \mathrm{ID}_{i,M}\}$ where, $1 \leq i \leq \tau$ and M is a system parameter. The pools of any two groups do not share any identifier, i.e., $\xi_i \cap \xi_j = \emptyset, \forall i \neq j$. Each tag of the group G_i is assigned a couple of identifiers from ξ_i by the issuer.

Tag. All the tags of the system are divided into τ groups. Each tag receives the shared group key of the group that the tag belongs to, a unique secret key that is known only to the reader and the tag itself, and a set of identifiers from the pool of identifiers of the group. Suppose, the tag T_j belongs to the group G_i. This tag possesses the group key k_{G_i}, the unique secret key k_{G_i}, and a set of identifiers Ω_{ij}. Each key is of θ bits, where θ is the security parameter of symmetric key encryption. We define the Ω_{ij} as follows

$\Omega_{ij} = \{\mathrm{ID}_{i,j_1}, \mathrm{ID}_{i,j_2}, \dots, \mathrm{ID}_{i,j_m}\}$,where ,

- each ID_{i,j_x} is chosen randomly following uniform distribution from the pool ξ_i and $j_x \in \{1,2, \dots, M\}$, where $1 \leq x \leq m$
- $\mathrm{ID}_{i,j_x} \neq \mathrm{ID}_{i,j_y}$, for all $x \neq y$
- m is also a system parameter and $M > m$.

The identifiers are assigned to the tags in such a way that at least one identifier of a tag is shared with at least two other members of the same group. So, we can say for the tag T_j,

$\exists p, q\left[\mathrm{ID}_{i,j_x} \in \left(\Omega_{ip} \cap \Omega_{iq}\right)\right]$,

Where p, q are any two members of G_i and $p \neq q$.

Reader. The reader is connected to the backend server. We assume the communication channel between the reader and the backend server is secured. From now on, we denote the backend server as the reader. In our system, the tag is the prover and the reader is the verifier. The reader receives all the secret information by the issuer during the deployment. The issuer issues the reader a set of secret information for each group in the system $\psi = \{\ \langle k_{Gi}, \sigma_i \rangle \mid 1 \leq i \leq \tau\}$, where k_{G_i} is the secret group key and σ_i is the mapping of the identifiers of the pool with the secret keys of tags. Formally,

$\sigma_i = \{\ \langle \mathrm{ID}_{i,x}, \pi_x \rangle \mid 1 \leq x \leq M \text{and} \mathrm{ID}_{i,x} \in \xi_i\}$,

where is the set of secret keys of tags associated with the $\mathrm{ID}_{i,x}$ can be defined as an empty set if no tag is associated with the $\mathrm{ID}_{i,x}$ or it can be a set of size at least one. Formally,

$$\pi_x = \begin{cases} \{k_{\omega_1}, k_{\omega_2}, \dots\}, & \text{where} \omega_* \in \{T_1, T_2, \dots, T_N\} \\ \emptyset, & \text{otherwise .} \end{cases}$$

System parameters. Since each tag receives m identifiers randomly chosen from the pool of M identifiers, according to the ID distribution strategy, we can say that each tag has at least one identifier

common with at least two group members. The probability that each tag shares at least one identifier with at least two group members is

$$P_{\text{share}} = 1 - \left(\frac{\binom{M-m}{m}}{\binom{M}{m}} \times \frac{\binom{M-2m}{m}}{\binom{M}{m}}\right) = 1 - \frac{((M-m)!)^3}{(M!)^2(M-3m)!}$$

where $M \geq nm$. For example, we consider an RFID system of 1000 tags divided in 10 groups. 100 tags are in each group. For simplicity, we assume $M = 100$ and $m = 10$. Then the probability that each tag shares at least one identifier with at least two group members is $P_{\text{share}} = 96.87\%$.

Note, in our system, M is a system parameter which basically refers to the number of identifiers assigned to a particular group. And m refers to the number of identifiers assigned to each tag. The more identifiers are assigned, that is the more the value of M, the harder it is for the adversary to break privacy. However, we cannot make M such a very large number so that the system becomes slow. There has to be a tradeoff between the two and system designer needs to make a decision of choosing M based on the requirement of system's performance and privacy need.

6.1.2. Brief overview of PriSens

In this subsection, we describe our protocol. In PriSens, in order to authenticate a tag, the reader sends a single challenge to the tag. The answer of the tag has two parts. In the first part, the tag answers to the reader by encrypting with the group key the reader's challenge concatenated with a nonce picked by the tag, and the tag's identifier (chosen from the pool of IDs). In the second part, the tag encrypts the challenge concatenated with the nonce using its own secret key. Encrypting the identifier is needed since the key used for encryption does not identify uniquely the tag. Upon reception of the answer, the reader identifies the tag by trying all the group keys until the decryption succeeds. Once the reader finds out the tag ID, then it checks the second part. The reader tries all secret keys associated with the identifier to decrypt the second part of the message. Without the second part, every tag could impersonate every other tag in the same group. Fig. 4 shows how PriSens works.

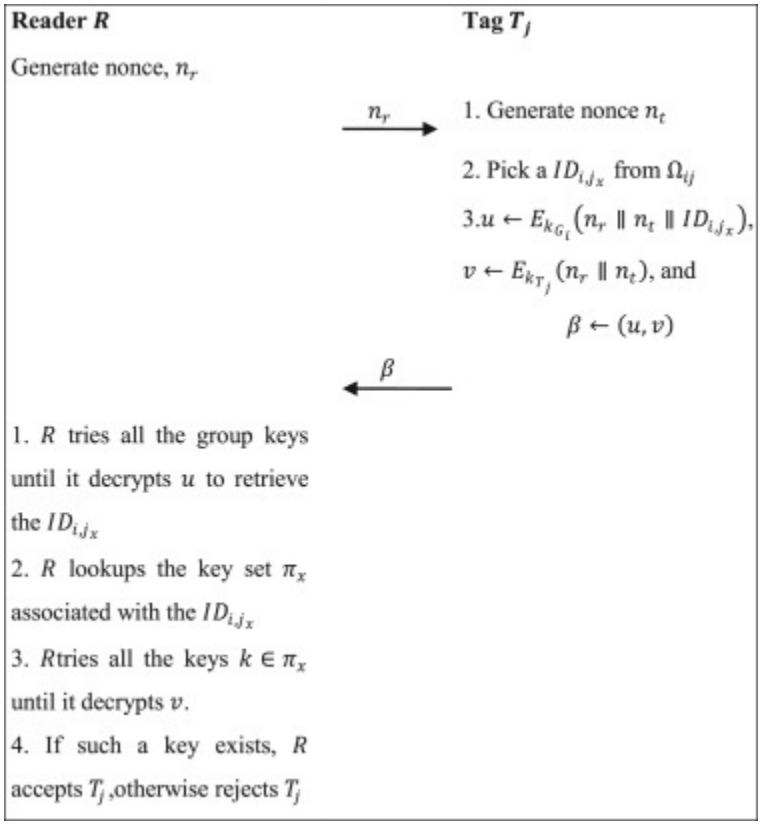

Fig. 4. The PriSens protocol.

The reader starts to query the tag with a nonce n_r. Upon the reception of the query, the tag generates another nonce n_t. Suppose the reader interrogates the tag T_j. In the second step, the tag picks an identifier, say ID_{i,j_x}, from Ω_{ij}. Then the tag computes as shown in Fig. 4. Here, $E_k(.)$ denotes symmetric key encryption with key k. The tag replies with the β. Now the reader searches all the group keys until it finds the correct one that properly decrypts the first part (u) of the response. If the reader retrieves the identifier ID_{i,j_x} that the tag used in its response, then the reader tries to decrypt the second part (v) of β with the potential set of secret keys (π_x) associated with ID_{i,j_x}. After finding the right secret key, the reader can uniquely identify the tag T_j. Sharing some identifiers of a tag with other members of the group provides unlinkability even if any tag is compromised by the adversary.

Search complexity of PriSens

According to PriSens, the reader's complexity is slightly increased than the group based scheme [34]. After receiving the response $\beta = (uv)$ from a tag T_j, the reader searches for the correct group key to decrypt u. In the worst case, the reader has to perform this operation τ times. If such a group key exists, the reader can retrieve the identifier ID_{i,j_x} from u. Now, the reader has to search for the tag's secret key to identify T_j by decrypting v properly. The reader searches a key space of size $|\pi_x|$. Therefore, in the worst case, the reader's total complexity is $\tau + |\pi_x|$. In the best case, the size of π_x is 3 and in the worst case, it can be n, size of the group. But in the group based scheme, the reader's

complexity in worst case is N. Nevertheless, PriSens is much better than the other schemes where the worst case reader's complexity is $\tau + 1$, the number of total tags in the system. To provide improvement in privacy protection, we have to sacrifice this small increase in the complexity of the reader. Since readers are more powerful than tags, they can handle this increase in search complexity.

Memory complexity of PriSens

According to PriSens, tags need to store m number of identifiers along with the group key and the unique secret key. Though tags have limited resources, however, the increase in memory requirement is acceptable than the increase in computation and communication complexity. A smart RFID tags have memory capacity of 32 kB or more. Even RFID tags with extended memory capacity are available at the market. All these tags can store the information required for PriSens.

7. Overview of HSAC framework

In this section, we describe the details of HSAC (Privacy Preserving Healthcare Service Access Mechanism) framework. Unauthorized disclosure of health related information can have serious consequences like: refusal of employment, seclusion from family or community groups and personal embarrassment. Once information has been disclosed, the damage cannot be undone so to earn user trust it is important that unauthorized disclosure is prevented. Also to prevent any kind of insider attack in the RFID based hospital information system, unauthorized access of sensitive data should be prevented. A major concern in RFID based healthcare system is how to protect user privacy when the RFID identification data, i.e. patient's private information are increasingly passed around and accessed by a large number of people such as doctors, nurses, technicians, and researchers. This information, collected over a period, may expose significant private information such as: trace of personal location, medical history, treatment history, and even financial information. One measure is to use access control technique, which requires that only authorized entities or users with a legitimate request satisfying related policies or laws can access sensitive information.

7.1. Access policy requirements for healthcare privacy

In modern day healthcare systems, most of the organizations are internetworking their systems, increasing the potential for unauthorized access. Since there are countless individual scenarios, circumstances and relationships, the access control framework must be flexible and highly expressive. The framework needs to ensure that a user's access policy can be recorded and enforced in a manner that reflects their understanding of who they want to have access and who they do not want to have access. This will typically involve *allowing* or *disallowing* consent to groups or roles. In order to restrict access of certain information to only certain people, allowing or disallowing access to certain roles needs to be included too. To employ allowance and disallowance of consent or access rights explicit denial of access to particular role is necessary.

The electronic medical record (EMR) in modern day healthcare information systems allows healthcare sectors to provide anytime–anywhere access to patient's info and overall medical history, thereby

increasing efficiency and improving patient care. Yet this ubiquitous transaction presents significant privacy risks. Hence, someone need to implement access control as part of these services to ensure that the right people get the right information at the right time. However, doing such a critical job manually for every single patient is simple impossible and hence information management systems used in healthcare system use some kind of technique to automate the process using access control mechanism. The need for RBAC stems from the HIPAA Privacy Rule's minimum necessary provisions. Most health care services (HCOs) need to implement fine-grained authorization protocols, since their users must be granted specific access privileges that define actions they may perform. In meeting the HIPAA Security standard for access control, many healthcare sectors are combining rule and policy-based access control with role-based access control, which provides efficiency and helps meet the HIPAA Privacy requirements.

7.2. Brief overview of HSAC

Role based access control (RBAC) [45] is a popular security model. Due to its flexibility, RBAC model has been widely applied to healthcare information systems [46], [47]. The RBAC model that NIST has proposed for standardization does not support explicit denial except in a limited way by using constraints [38]. In this paper, we propose HSAC, a privacy preserving healthcare service access mechanism. The architecture of HSAC is shown in Fig. 5. HSAC proposes to preserve user preferred privacy while accessing healthcare services using Privacy-aware Role Based Access Control (P-RBAC) [17]. The adoption of a model like P-RBAC in a RFID based healthcare seems justifiable since healthcare is a complex environment that deals with various user roles in multiple organizations. Classical RBAC, does not support role roaming among different organizations. Furthermore, in order to protect privacy in healthcare sector, not only the content of EMR but also some meta information about EMRs, e.g., the creators, owners are required for privacy protection. However, the main feature of P-RBAC lies in the complex structure of privacy permissions that reflects a structured ways of expressing privacy rules. Aside from the data and the action to be performed on the data, in P-RBAC, privacy permission explicitly states the intended purpose of the action along with the conditions under which the permission can be granted and the obligations that are to be finally performed. It helps in verifying that the access control policies of the healthcare organization are compliant with privacy regulations. Moreover, in HSAC, we allow users to have preferred privacy configuration by including user defined privacy policies along with the organizational privacy policies.

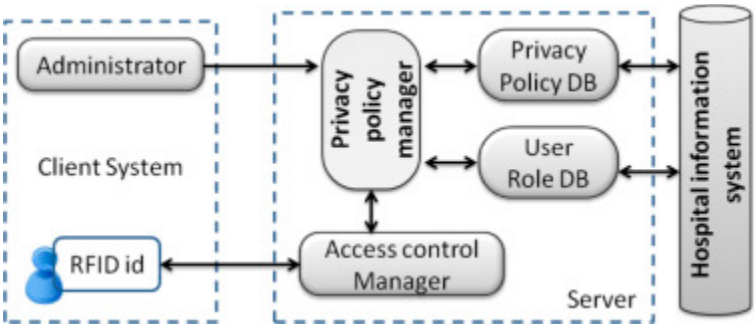

Fig. 5. The architecture of HSAC.

In HSAC, the administrator can define and manage traditional privacy policies related to the access of various data as well as user preferred privacy policies. For example, some doctor may not want anyone else to view her patient's medical diagnosis without her permission. The Privacy Policy Manager (PPM) breaks down all these policies into unit privacy policy and unit user role. The unit policy and unit role are stored in Privacy Policy DB (Database) and User Role DB (Database). The User Role DB module also contains a role hierarchy. For example, any information that can be viewed by the nurse must be accessible by the doctor too. Only a part of information visible to nurse may be accessible by the pharmacist, who only needs to know which drug to dispatch for which patient. Moreover, the pathologist only needs to know the *lab test name*, and the accounts section of the hospital needs to know the breakdown of costs for various services provided to the patient. It is hard to develop a generalized role hierarchy since it may differ for different institutions. However, such a role hierarchy can be defined by the administrator based on the preference and organization requirements. Whenever, a user requests for some healthcare service using the ID of the tag, the Access Control Manager (ACM) locates policies defined by the PPM. The PPM then brings up the requested information by querying stored unit policies and merging them for the particular user role. If ACM detects any violation of any unit privacy rule for a particular role, the service request is denied.

8. Security and privacy analysis

In this section, we formally prove that our protocol preserves data privacy and provides unlinkability. In addition, we analyze the preservation of privacy in some attack scenarios where some of the tags of the system are compromised by the adversary $\hat{A}$.

8.1. Information privacy

Theorem 1

PriSens *preserves information privacy with respect to the adversary* $\hat{\mathrm{A}}$.

Proof

Let us assume $\mathcal{O}_{\mathrm{pick}}$ provides the adversary $\hat{A}$ with a tag T. $\hat{A}$ transmits this tag to the oracle $\hat{A}$ with a nonce n_1. Then $\mathcal{O}_{\mathrm{encrypt}}$ provides $\hat{A}$ with the response β.

Now, $\hat{A}$ selects a ID. To break data privacy $\hat{A}$, should tell if β is produced using the ID. This implies that $\hat{A}$ has to identify the input of the encryption by just learning the cipher text. $\hat{A}$ can succeed in two cases. First, if she can retrieve the inputs from the output of the random oracle. But this contradicts with our assumption that the inputs of a random oracle are computationally intractable from the output of the oracle. Second, if $\hat{A}$ knows the secret keys of the tag T. Without tampering the tag T, if $\hat{A}$ can determine the keys by learning the cipher texts, this again breaks the semantic security of the

symmetric key cryptography. Therefore $\hat{A}$ can break data privacy with probability no better than random guessing. Thus it proves data privacy property of Definition 1. ■

8.2. Unlinkability

Theorem 2

PriSens *provides unlinkability with respect to the adversary* $\hat{A}$.

Proof

Let us assume $\mathcal{O}_{\text{pick}}$ provides the adversary $\hat{A}$ with two tags T_0, T_1 from the same group. These two tags go into the learning phase. $\hat{A}$ transmits T_0, T_1 to $\mathcal{O}_{\text{flip}}$ which outputs the response β_b.

Now, to break unlinkability, the adversary $\hat{A}$ has to tell the value of b. We assume that the adversary's guess is right. In other words, the adversary can determine whether the response β_b is produced by T_0 or T_1, given the learned responses from both the tags. The responses of a tag cannot be a signature of the tag because according to our protocol, a nonce on the tag side makes each response different from all the previous responses originated from the same tag. Therefore, we can say that the guess is right because the adversary knows the keys (the group key and the secret key) stored on these two tags. Without tampering the tags T_0, T_1, the adversary has to determine the keys stored on these tags by just observing the cipher texts. But this contradicts with the semantic security of symmetric key cryptography. Therefore the adversary can break unlinkability with no better approach than random guessing. Thus it proves the unlinkability property of Definition 2. ■

8.3. Physical attack

Under this attack, we consider that the adversary $\hat{A}$ can compromise any tag with a probability of $\frac{1}{N}$. Whenever a tag becomes compromised, the adversary learns all private information stored on the tag T_j. Therefore, the adversary can now decrypt u of each response β originated from the other members of the group G_i. Thus, $\hat{A}$ can learn the identifier that a tag is using to produce its response by decrypting the u. We discuss the after effect of this attack with an example and demonstrate how PriSens provides unlinkability even if the adversary realizes the identifiers used in the responses.

We consider a group G_i of four tags T_1, T_2, T_3, and T_4. Suppose the adversary compromised the tag T_3 as shown in Fig. 4. Now the adversary learns the group key k_{G_i}, the tag secret key k_{T_3} and a set of identifiers $\Omega_3 = \{1,2,3,4\}$. From now on, the adversary can decrypt part of all the responses originated from T_1, T_2, and T_4 with the group key k_{G_i}. However, the adversary still cannot decrypt v part of these responses since she does not possess the secret keys of these tags. With this learned information (k_{G_i}

and Ω_3), the adversary tries to track the other tags of this group. Since the adversary can decrypt u of each responses, she can learn the identifier underlying the cipher text u. In other words, she can discover which identifier has been used to produce a response. The arrow in Fig. 6 represents that the responses of the authentication sessions (after T_3 is compromised) are transmitted from the tags (T_1, T_2, T_4) to the reader. The identifiers used in these responses are shown above the arrow. Each identifier is shown in plain text since the adversary can retrieve the identifier by decrypting u of β using k_{G_i}.

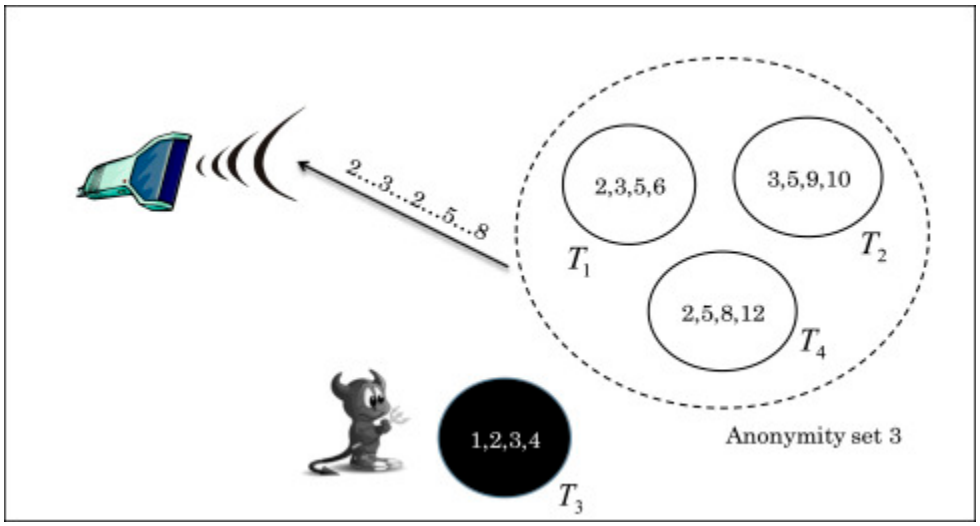

Fig. 6. After effect of a physical attack on PriSens, where T_3 is compromised by the adversary.

According to our protocol, even if the adversary comes to know about the identifier used in a response, she cannot conclude which of the potential tags is the sender of this response. In our example, the adversary discovers the identifier 2 is used two times, but she cannot be certain which of these tags (T_1, T_2, T_4) is the originator(s) of these responses. Though T_3 shares the identifier 2 with only T_1 and T_4, however, the adversary has no knowledge about the parties with whom T_3 is sharing which of its identifiers. Even the adversary does not know how many of the identifiers of Ω_3 are being shared. So, under this scenario, the anonymity set of the potential senders of a given response seems to be 3 to the adversary. Therefore, when the adversary compromises one tag from the group of uncorrupted tags, PriSens forms an anonymity set of size 1 and another anonymity set of size $(n-1)$ from the group instead of anonymity sets of size 1 like the group based authentication [34]. This noticeable partition improves the level of privacy provided by PriSens. Because, the remaining $(N-n)$ tags of the system forms the other anonymity set which is same under both the protocols. Thus PriSens prevents adversary benefit from tracking by compromising a tag.

We now consider the case of compromising multiple tags of the same group. In the above scenario, even if $\hat{A}$ compromises either T_1 or T_4 after compromising T_3, the adversary cannot be certain whether T_2 has identifier 2 in Ω_2 or not. Therefore, the size of anonymity set is still 2, i.e., $n-c$, where is the number of compromised tags of the group. If $\hat{A}$ compromises T_2 instead of T_1 or T_4, the size of anonymity set is still 2 (i.e., $n-c$). Therefore, we conclude that the anonymity set, formed from a

group that is under physical attack, is of size $(n - c)$, where n is the group size and c is the number of compromised tags of the given group.

8.4. Tracking attack

In tracking attack, an adversary tries to track a tag (T_j) over time. It succeeds if it is able to distinguish T_j from other RFID tags over time. Under this attack, adversary repeatedly queries T_j with a value which yields a consistent reply. This consistent reply becomes a signature of T_j. Adversary can reuse the same random nonce n_r learned from any previous challenge-response. By incorporating n_t in the tag side, our protocol becomes secured against tracking as adversary cannot predict n_t. Consequently T_j will reply a new output each time it is queried using a different random nonce and different identifier selected from the identifier pool assigned to tag T_j. Thus adversary fails to get any consistent reply from T_j. As a result it cannot follow T_j afterwards and the tracking attack is not successful. Hence our protocol proves to be secure against tracking attack.

9. Evaluation

Though our framework consists of two major components, the main privacy preservation is done by the PriSens component while identifying a tag via radio frequency channel. HSAC is able to preserve privacy by restricting unauthorized access given that HSAC follows a proper implementation of P-RBAC technique and privacy policies are properly defined. Therefore, it is more significant to evaluate the privacy achieved by the PriSens component.

In this section, we measure the level of privacy achieved by PriSens as a function of the total number of compromised tags. We compare the performance of PriSens against the group based authentication protocol proposed in [34] by Avoine et al. We consider two privacy metrics for the measurement of privacy. First, our privacy measurement technique is based on anonymity set like the privacy metric used by Avoine et al. [38] and we name this metric “privacy level”. Second, we identify the amount of information disclosed by a scheme as another metric presented in [37]. This metric is based on Shannon’s information theorem [48] and we name this metric “information leakage”.

9.1. Measurement of privacy based on anonymity set

The level of privacy of an RFID system, achieved by a scheme, at a given time, is a function of the total number of compromised tags at that time. When some tags are compromised, the set of all tags are partitioned such that the adversary cannot distinguish the tags belong to the same partition, but she can distinguish the tags that belong to different partitions. So, these partitions become the anonymity sets of their members. The level of privacy based on anonymity set, $\wp$, can be measured as the average anonymity set size [34].

$$\wp = \frac{1}{N}\sum_i |P_i|\frac{|P_i|}{N} = \frac{1}{N^2}\sum_i |P_i|^2$$

Where $|P_i|$ denotes the size of partition P_i and $\frac{|P_i|}{|N|}$ is the probability that a randomly chosen tag belongs to partition P_i.

According to PriSens, a similar kind of partitions is formed when tags become compromised. If c_i is the number of compromised tags within group G_i, then the set of the tags within this group is partitioned into c_i anonymity sets of size 1 and another anonymity set of size $(n - c_i)$. If $\mathbb{C} = \{c_i | c_i \text{is the total compromised tags within} G_i\}$ is the set of compromised groups, $|\mathbb{C}|$ is the total number of compromised groups, and $C = \sum_{\text{each} c_i \in \mathbb{C}} c_i$ is the total number of compromised tags, the level of privacy achieved by PriSens can be expressed as

$$\wp = \frac{1}{N^2}((n(\tau - |\mathbb{C}|))^2 + \sum_{\text{each} c_i \in \mathbb{C}} (c_i + (n - c_i)^2))$$

where $N =$ total number of tags in the system

• $n =$ total number of tags within a group

$\tau =$ total number of groups in the system.

9.2. Measurement of privacy based on information leakage

We measure the information leakage in bits based on Shannon's information theorem [48]. If we have a group of tags of size S and the adversary divides this group into two disjoint subgroups of size $S/2$, then 1 bit of information is disclosed out of $log_2 S$ bits. Extending this concept from two subgroups of equal size to two subgroups of different sizes, where $\frac{S}{a}$ tags are in one subgroup and the remaining tags are in another subgroup, we can measure the average amount of information disclosed in bits as follows

$$I = \frac{1}{a} log_2(a) + \frac{a-1}{a} log_2(\frac{a}{a-1}).$$

In general, if the adversary splits N tags of the system into k disjoint partitions, then

$$I = \sum_{i=1}^{k} \frac{|P_i|}{N} \cdot log_2(\frac{N}{|P_i|})$$

Where $|P_i|$ denotes the size of partition P_i. According to our protocol, if $\mathbb{C} = \{c_i | c_i \text{is the total compromised tags within} G_i\}$ is the set of compromised groups, $|\mathbb{C}|$ is the total number of compromised groups, and $C = \sum_{\text{each} c_i \in \mathbb{C}} c_i$ is the total number of compromised tags, the amount of information leakage in bits can be expressed as

$$I = \left(\frac{n(\tau - |\mathbb{C}|)}{N} log_2\left(\frac{N}{n(\tau - |\mathbb{C}|)}\right)\right) + \sum_{\text{each} c_i \in \mathbb{C}} \left(c_i\left(\frac{1}{N} log_2 N\right) + \frac{(n - c_i)}{N} log_2\left(\frac{N}{(n - c_i)}\right)\right)$$

where, N, n, and τ bear the same meaning mentioned before.

9.3. Experimental results

We have compared both the protocols, PriSens and the group based authentication, using a Matlab simulation. The experiment results establish that the level of privacy provided by PriSens is higher than that of the group based authentication. Our comparison is based on the two metrics presented above, the level of privacy (based on anonymity set) and information leakage. We have come up with a conclusion same as [37] that the information leakage describes the privacy threats better than the anonymity set.

In our simulation, we have considered two systems with $N = 2^{16}, \tau = 64$ and $N = 2^{20}, \tau = 64$. Tags are selected to be compromised with a uniform random distribution. The number of compromised tags ranges from 0 to 160. We have run the simulation for 100 times and computed the average achieved by PriSens and the group based authentication as a function of the total number of compromised tags C (Fig. 7(a)–(b)).

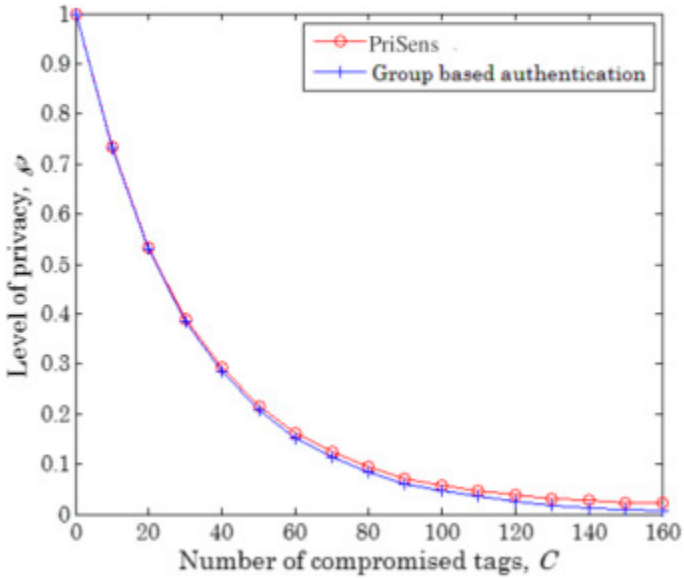

Fig. 7(a). (a) Level of privacy based on anonymity set, with $N = 2^{16}$ and $\tau = 64$.

.

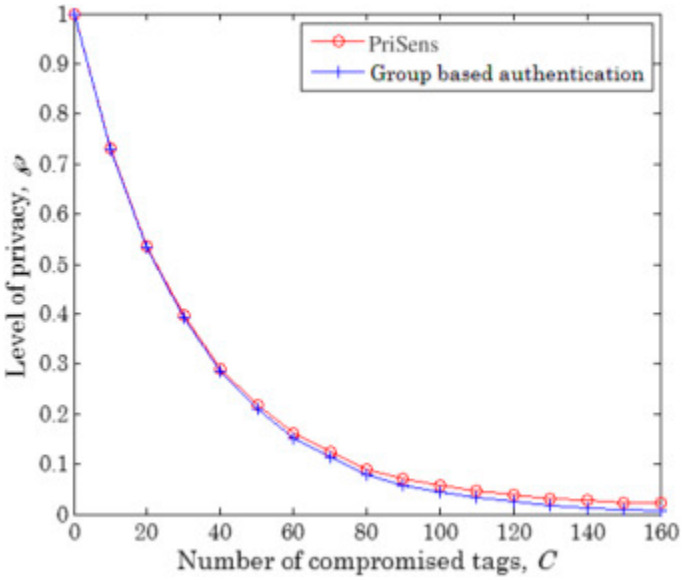

Fig. 7(b). (b) Level of privacy based on anonymity set, with $N = 2^{20}$ and $\tau = 64$.

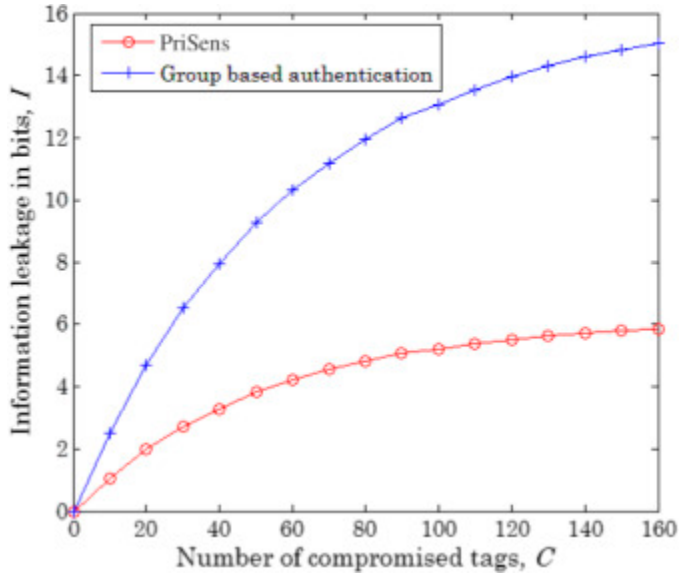

Fig. 7(c). (c) The amount of information leakage, with $N = 2^{16}$ and $\tau = 64$.

.

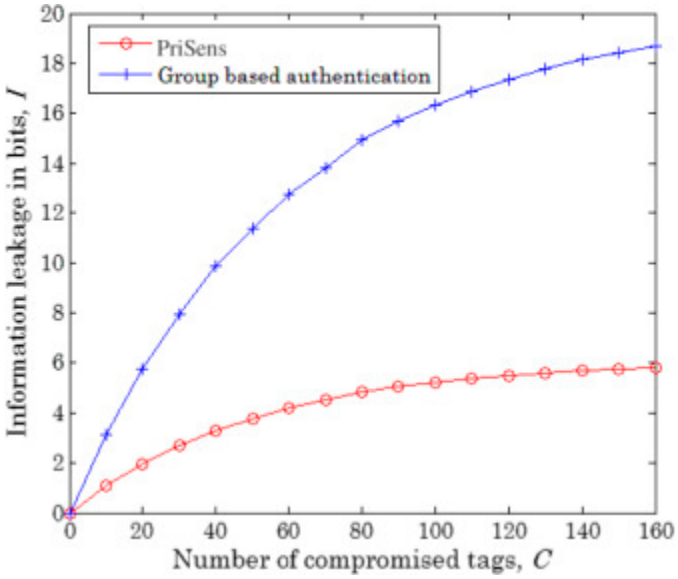

Fig. 7(d). (d) The amount of information leakage, with $N = 2^{20}$ and $\tau = 64$.

Fig. 7. Experimental results of PriSens against the group based authentication.

The small increase in the level of privacy achieved by PriSens is visible when the total number of compromised tags becomes more than 30. During the simulation, we have also computed the average amount of information leakage I, for both the protocols, as a function of the total number of compromised tags (Fig. 7(c)–(d)). The plots depict that a significant amount of improvement in privacy protection is achieved by PriSens. With the increase in the total number of compromised tags C, the average amount of information disclosed by the group based authentication is quite higher than the information disclosed by PriSens.

In Fig. 7(c) ($N = 2^{16}$), when C becomes 160, the group based authentication discloses about 15 bits out of 16 bits of information, while PriSens discloses about 6 bits of information. The group based authentication discloses 56.25% more information than PriSens in a similar setup.

Fig. 7(d) ($N = 2^{20}$) shows that the group based authentication reveals almost 19 bits out of 20 bits of information and PriSens reveals around 6 bits of information. This time the group based authentication discloses 65% more information than PriSens. Based on the simulation results, we can conclude that the information disclosed by the group based authentication increases with the size of the system; however, PriSens shows consistency in the information leakage in both the cases. Information leakage is a better metric to demonstrate the privacy threats in RFID systems than anonymity set. Though the improvement in $\wp$ provided by PriSens against the group based authentication is not significant, however, we can say that PriSens provides better privacy protection than the group based authentication, based on the results of the amount of information disclosed by these two protocols.

10. Discussion

While RFID technology can improve the overall quality of healthcare system, the potential benefits of RFID technology have been accompanied by threats of privacy violations [49]. The use of RFID introduces a new set of risks: security risks are associated with the possible failure of the RFID system under various security attacks, i.e. tracking, eavesdropping, and denial of service, while the threat to privacy resides in the capabilities to permanently save and track information about individuals through temporal and spatial extension of data collection. Even though concerns about information privacy are not unique to the healthcare domain, health related information can be perceived as more personal and more sensitive. A recent report by the California HealthCare Foundation found that 67% of the national respondents worry about the privacy of their personal medical information [50]. Due to the highly personal and sensitive nature of healthcare data, both healthcare providers and patients can be expected to resist further digitalization and data source sharing of personal health data until security and privacy protections are in place. The motivating example of RFID applications presented in this paper are examples of RFID based healthcare or such systems where user's privacy is the most important issue. The goal of our proposed framework is to preserve privacy efficiently as well as provide basic security like confidentiality, unlinkability, and authentication. PriSens protocol is able to achieve all these goals since it discloses much less information than the existing protocols. HSAC component of our framework also helps in ensuring more privacy in RFID based healthcare systems by regulating user access to sensitive personal information using smart access control techniques.

11. Conclusion

In this paper, we propose a framework, PriSens-HSAC that provides increased privacy for RFID based healthcare systems. The PriSens component provides better privacy compared to the existing RFID authentication protocols while identifying an RFID tag in healthcare setting. The HSAC component restricts unauthorized access of patient's private information by using P-RBAC mechanism. Though our major motivation behind this proposal is to enhance the privacy of users in an RFID based healthcare system, our proposed PriSens-HSAC framework also addresses all the security requirements. There are numbers of benefits of using our proposed framework. First, the use of our proposal will clearly provide more privacy and disclose less information if the RFID application is ever attacked by an adversary, which eventually will ensure more privacy for its users. Second, the PriSens component of the framework will work even if the tags are very cheap meaning even if they have less computational capability, which is ideal for mass deployment of RFID systems. Third, HSAC component of the framework will allow authorized users to access EMR linked with RFID data which in turn ensure more privacy for the users. Our evaluation also clearly illustrates that the adoption of this framework will allow RFID based healthcare systems to preserve user privacy. The widespread adoption of such privacy preserving framework for RFID systems will open doors for various assisted care, remote health monitoring, and elderly care applications.

In PriSens-HSAC framework, one research investigation could be to investigate the performance and accuracy of the entire framework by utilizing it in various real scenarios for different user roles like: Physician, Emergency care provider, and Pharmacist. To better investigate the privacy preservation

issue, one could also test the accuracy of the framework by simulating the system scenario under various attacks. One other research direction in case of PriSens-HSAC framework can be to investigate the privacy levels achieved for different types of service requests and different attacks. Another future research direction in the context of privacy preservation in RFID systems could be to study the privacy threats in RFID data publishing phase and show that traditional anonymization techniques are not applicable for RFID data due to its challenging properties: high-dimensional, sparse, and sequential. Future research can also be focused to adopt a newer privacy model like LKC-privacy that can overcome these challenges in the data publishing phase. Another future work can be in the direction of changing the domain of identifiers to be used by the tags after a certain time period. In order to increase privacy and to randomize tag's output even more, new set of identifiers could be assigned after a certain period which will require changes in our proposed framework to address different challenges.

References

[1] A. Juels, RFID security and privacy: A research survey. RSA Laboratories. 2005.

[2] A. Juels, S. Weis, Defining strong privacy for RFID. in: Proc. of the Cryptology ePrint Archive, Report 2006/137, IACR. 2006.

[3] Limitations of NFC http://www.smartcard.co.uk/articles/R2R%20Technology%201_0.pdf [Last accessed: 21.09.2012].

[4] P. Harrop, T.C. Harvey, RFID for Healthcare and Pharmaceuticals, in: IDTechEx, 2008. Last accessed at http://www.idtechex.com/research/reports/rfid_for_healthcare_and_pharmaceuticals_2008_2018_000146.asp.

[5] R. Wessel, RFID bands at the Jacobi Medical Center. 2005. Last accessed—March 2012 at [http://www.rfidgazette.org/2005/12/rfid_bands_at_t.html].

[6] M. Chen, S. Gonzalez, Q. Zhang, M. Li, V. Leung**A 2g-rfid based e-healthcare system**, Proc. Wirel. CommunMag., 17 (1) (2010), pp. 37-43.

[7] C.E. Turcu, C. Turcu, V. Popa, An RFID-based system for emergency health care services, in: Proc.of WAINA '09. USA, pp. 624–629.

[8] RFID needs big data tools [URL: http://www.informationweek.com/big-data/big-data-analytics/rfid-needs-big-data-tools/d/d-id/1106246?].

[9] BlueBean. The Benefits of RFID in the Healthcare Organization, RFID Solutions for the Healthcare Industry. 2007. Last accessed—March 2012 at http://www.rfidhealthcare.com/.

[10] CASPIAN Press Release. Metro's decision to drop the loyalty card, 2004. Last accessed June 2010—http://www.spychips.com/metro/press-release-feb-27.html.

[11] Press Release: Invasion of Privacy? RFID Tracking Kids On School Buses, URL: http://www.ibtimes.com/invasion-privacy-rfid-tracking-kids-school-buses-privacy-advocates-concerned-attendance-management [Last accessed: 3/28/2016].

[12] Press Release: RFID Tags—Smart Idea or Invasion of Privacy?, URL: http://www.streetdirectory.com/travel_guide/115640/technology/rfid_tags___smart_idea_or_invasion_of_privacy.html [Last accessed: 3/28/2016].

[13] F. Rahman, S.I. Ahamed, J.J. Yang, Q. Wang, I am not a goldfish in a bowl: A privacy preserving framework for RFID based healthcare systems, in: Proc. of IEEE International Conf. e-Health Networking, Applications and Services, Healthcom. 2012, pp. 335–340.

[14] L. Hildner**Defusing the threat of RFID: protecting consumer privacy through technology-specific legislation at the state level**, Harvard Civ. Rights-Civ. Liberties Law Rev., 41 (2006), pp. 133-176.

[15] W. Yao, C. Chu, Z. Li, The use of RFID in healthcare: Benefits and barriers, in: Proceedings of the IEEE International Conference on RFID-Technology and Applications, 2010.

[16] N. Rivera1, R. Mountain, L. Assumpcao, A.A. Williams, A.B. Cooper, D.L. Lewis, R.C. Benson, J.A. Miragliotta, M. Marohn, R.H. Taylor, ASSIST—Automated System for Surgical Instrument and Sponge Tracking, in: Proceedings of the IEEE International Conference on RFID. Las Vegas, Nevada, USA 2008.

[17] A.F. Dafa-Alla, E.H. Kim, K.H. Ryu, Y.J. Heo, PRBAC: an extended role based access control for privacy preserving data mining, in: Proc. ofACIS International Conference onComputer and Information Science, 2005, pp. 68–73.

[18] C.G. He, C.Z. Cao, S.D. Bao, An enhanced role-based access control mechanism for hospital information systems, in: Proc. ofConf.on Computational Intelligence and Security, 2011, pp. 1001–1005.

[19] N.L.J.W. Byun, E. Bertino, Purpose based access control of complex data for privacy protection, in: Proc. of SACMAT., 2005, pp. 102–110.

[20] N.Z.N. Yang, H. Barringer, A purpose-based access control model, in: Proc. of IAS., 2007, pp. 143–148.

[21] H.H.J. Jin, G.J. Ahn, Patient-centric authorization framework for sharing electronic health records, in: Proc. SACMAT., 2009, pp. 125–134.

[22] T.M.S. Godik**Extensible access control markup language (xacml). Technical Report v1.1** (2003).

[23] M. Rieback, B. Crispo, A. Tanenbaum**The evolution of RFID security**, IEEE Pervasive Comput. (2006)

[24] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Lecture Notes in Computer Science (2004).

[25] M. Ohkubo, K. Suzuki, S. Kinoshita, Cryptographic approach to privacy friendly tags, in: Proc. of RFID Privacy Workshop, 2003.

[26] G. Avoine, P. Oechslin, A scalable and provably secure hash based RFID protocol, in: Proc. of PerSec., 2005, pp. 110–114.

[27] Y. Seo, K. Kim**Scalable and untraceable authentication protocol for RFID**, International Workshop on Security in Ubiquitous Computing Systems, Springer-Verlag, Seoul, Korea (2006).

[28] Y. Seo, H. Lee, K. Kim, A Lightweight Authentication Protocol Based on Universal Re-encryption of RFID Tags. 2006.

[29] G. Tsudik**YA-TRAP: Yet another trivial RFID authentication protocol**, International Conference on Pervasive Computing and Communications, (PerCom '06), IEEE, IEEE Computer Society Press, Pisa, Italy (2006).

[30] M. Burmester, T.V. Le, B.D. Medeiros**Provably secure ubiquitous systems: Universally composable RFID authentication protocols**, Conference on Security and Privacy for Emerging Areas in Communication Networks—SecureComm, IEEE, Baltimore, Maryland, USA (2006), August-September.

[31] M.E. Hoque, F. Rahman, S.I. Ahamed, J.H. Park, **Enhancing privacy and security of RFID system with serverless authentication and search protocols in pervasive environments**, Springer J. Wirel. Pers. Commun., 55 (1) (2009), pp. 65-79.

[32] M.E. Hoque, F. Rahman, S. Ahamed, Supporting recovery, privacy and security in RFID systems using a Robust authentication protocol. in: Proc.of SAC., 2009, pp. 1062–1066.

[33] M.E. Hoque, F. Rahman, S.I. Ahamed, AnonPri: An efficient anonymous private authentication protocol, in: Proc. of PerCom., 2011, pp. 102–110.

[34] D. Molnar, D. Wagner, Privacy and security in library RFID: Issues, practices, and architectures, in: Proc. of CCS. 2004. pp. 210–219.

[35] G. Avoine, E. Dysli, P. Oechslin**Reducing time complexity in RFID systems**, B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography, LNCS, vol. 3897, Springer (2005), pp. 291-306.

[36] L. Buttyan, T. Holczer, I. Vajda**Optimal key-trees for tree-based private authentication,** Proc. of Privacy Enhancing Technologies Workshop, (PET 2006), Springer (2006), pp. 332-350.

[37] K. Nohl, D. Evans, Quantifying information leakage in tree-based hash protocols, in: Proc. of ICICS. 2006, pp. 228–237.

[38] G. Avoine, L. Buttyan, T. Holczer, I. Vajda, Group-based private authentication, in: Proc. of WoWMoM, 2007, pp. 1–6.

[39] Jingxian Zhou**A Quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification**, J. Commun., 10 (2) (2015), pp. 117-123.

[40] M.S.I. Mamun, A. Miyaji**A privacy-preserving efficient RFID authentication protocol from SLPN assumption**, Int. J. Comput. Sci. Eng. (IJCSE), 9 (2014), Inderscience Publishers.

[41] T. Dimitriou, A lightweight RFID protocol to protect against traceability and cloning attacks, in: Proceedings of SecureComm, 2005, 2005, pp. 59–66.

[42] D. Henrici, P. Müller, Providing security and privacy in RFID systems using triggered hash chains, in: Proceedings of IEEE PerCom, 2008. pp. 50–59.

[43] C. Chatmon, T.V. Le, M. Burmester**Secure anonymous RFID authentication protocols. Technical Report**, Florida State University, Department of Computer Science, USA (2006)

[44] C. Diaz, S. Seys, J. Claessens, B. Preneel, Towards measuring anonymity, in: Proc. of PET, 2002. USA, pp. 54–68.

[45] D. Ferraiolo, D.R. Kuhn**Role based access control**, Proc. of Conference on National Computer Security, National Institute of Standards and Technology, MD (1992), pp. 554-563.

[46] P.S.M.Y. Becker, Cassandra: flexible trust management, applied to electronic health records, in: Proc. of Computer Security Foundations Workshop, 2004, pp. 139–154.

[47] A.G.R. Bhatti, K. Moidu, Policy-based security management for federated healthcare databases (or rhios), in: Proc. of the Workshop on Healthcare Information and Knowledge Management, 2006, pp. 41–48.

[48] C. Shannon**A mathematical theory of communication**, Bell Syst. Tech. J., 27 (1948), pp. 379-423 and 623–656.

[49] R.L. Juban, D.C. Wyld**Would you like chips with that?: Consumer perspectives of RFID**, Manag. Res. News, 27 (11–12) (2004), pp. 29-44.

[50] L.S. Bishop, B.J. Holmes, C.M. Kelley, National consumer health privacy survey 2005. California HealthCare Foundation. Available online at: http://www.chcf.org/publications/2005/11/national-consumer-health-privacysurvey-2005.