**DAYANANDA SAGAR COLLEGE OF ENGINEERING**

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with ‘A’ grade, Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078.



**SEMINAR REPORT**

**on**

**“Lightweight RFID Protocol for Medical Privacy Protection in IoT”**

Submitted By

**Osman C. Dsilva**

**1DS16CS074**

**Eighth Semester B.E (CSE)**

**2019-2020**

Under the guidance of

**Prof. Dr. Amutha S.**

**Dept. of CSE**

**DSCE, Bangalore**

**Department of Computer Science and Engineering**

**Dayananda Sagar College of Engineering**

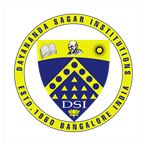
**Bangalore-78**

**VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM**

**DAYANANDA SAGAR COLLEGE OF ENGINEERING**

**Shavige Malleshwara Hills, Kumaraswamy Layout, Bangalore-560078**

**Department of Computer Science & Engineering**

****

**CERTIFICATE**

This is to certify that the seminar work entitled “Lightweight RFID Protocol for Medical Privacy Protection in IoT” is a bonafide work carried out by Osman Christopher Dsilva 1DS16Cs074 in a partial fulfilment for the 8th semester of Bachelor of Engineering in Computer Science and Engineering of the Visvesvaraya Technological University, Belgaum during the year 2019-20. The seminar report has been approved as it satisfies the academic requirements in respect of Seminar Work prescribed for Bachelor of Engineering Degree.

**Signature of Examiners with date Signature of HOD**

**Acknowledgement**

I would like to extend my sincere & heartfelt obligation towards all the personages who have helped me in this endeavor. Without their active guidance, help, cooperation & encouragement none of this would have been possible.

I am extremely thankful to my guide Prof. Amutha S. for her valuable guidance and support on completion of this seminar.

I extend my gratitude to Dr. Vindhya P Malagi, Associate Professor DSCE for her guidance and coordinating the seminar on time and in an organized way.

I also extend my gratitude to Dr. Ramesh Babu D.R. Head of Department, Computer Science for providing me this opportunity to conduct the seminar which helps everyone to speak in confidence.

And finally thankful to Dr. C.P.S. Prakash Principal, DSI for providing such platform to grow and conduct research and gain knowledge.

**Osman C. Dsilva**

**1DS16CS074**

**Abstract**

Nowadays the privacy data of people is at serious risk of disclosure due to people relying on digital data. This digital data is prone to get leaked because of malicious attacks by hackers. For example, personal medical privacy data can be easily leaked to insurance companies and this compromises the privacy of the patients. The Internet of Things technology has been rapidly in developed and people are inventing new ways to communicate and access data through the internet.

RFID is one of the core technologies of the Internet of things. The use of RFID system in the medical system can help solve this problem of medical privacy. RFID tags which are used to collect and process data can be used by the reader to get information about the patient. The whole process of information interaction is mainly in the form of cipher text.

In the context of the Internet of Things, this paper presents a lightweight RFID medical privacy protection protocol. The protocol ensures security privacy of the collected data via secure authentication. The security analysis and evaluation about the scheme indicate that the protocol can effectively prevent the risk of medical privacy data being easily leaked.

**Introduction**

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

Today, the privacy of individuals has become the legal provisions in many countries, and more and more people begin to concentrate on their medical privacy data. There is a wide range of risks to the security of these privacy data, which might be used for academic research without desensitizing, or be uploaded to third-party websites, or be obtained by some other agencies.

With the rapid development of big data and cloud computing technologies, Internet of Things (IoT) technology has been beginning to approach people's daily lives gradually. IoT, just as its name implies, means "everything is connected to the internet”. Social science research shows that IoT technology is another wave of information industry after the era of personal computer (PC) network and mobile internet.

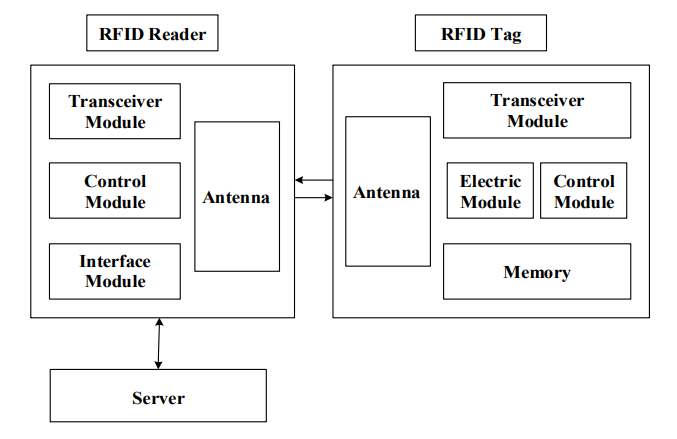
Classic RFID system is composed of three parts, including RFID tag, reader and server. Among the system, tag is responsible for collecting information and doing some simple processing, the server is used to process the data and store them, and the reader can identify the tag, and play a role of an intermediary for communicating between tag and server. RFID is a non-contact identification technology, with the feature of automatic identification, high storage capacity, portability and security, because of which it can be applied in medical field.

In medical system, RFID tags can be attached to the surface of an object or implanted into it, and collect its information. For patients, the tag can collect physical health data, and communicate and interact with the server. It makes remote real-time monitoring and telemedicine become a reality, providing new technical support for wireless body area networks (WBAN) and mobile health networks (MHN).

Along with the advantages of medical RFID system is security issue. As it is known, personal physical healthy information is closely related to individual privacy. The attackers today begin to infiltrate the cyber world, and they steal or falsify the patients’ medical privacy data, and undermine the system's normal workflow, leading to the serious result of the disclosure of medical privacy data. Therefore, security has become one of the key issues to be addressed for RFID applied in medical system safely.

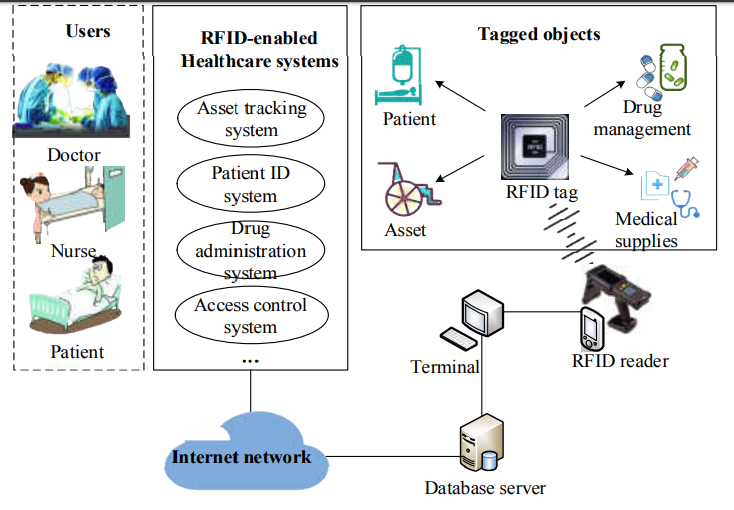
**Working of RFID**

In general, the RFID system typically consists of three parts, as described in the figure below. RFID tag, as the data carrier, is usually along with the target object. RFID reader is capable of reading and writing the tag, which can be designed as mobile and fixed. The back-end server is typically used to store and process communication data of the system. The whole RFID architecture has features of large data storage capacity, readable and writable, strong penetrating power, far read and write distances, fast reading speed, long service life and good environment adaptability. In medical field, RFID technology is widely used, including the location tracking of medical assets, neonatal and patient identification, medical tracking and validation, patient information management in health centers and surgical process management.



**RFID based Medical System**

RFID system has received considerable attention in the medical health field for almost a decade now, which is expected to efficiently track hospital supplies, medical equipment, medications and patients. The following figure introduces a RFID-enabled medical health system, in which the RFID tags are attached to some objects, such as medication management devices, medical auxiliary equipment, medical assets, and even the patients themselves. For example, an authorized doctor can remotely get the patient's vital signs and give the patient reasonable advice so that the patient can get better rapidly. Therefore, the RFID-enabled Healthcare System supplies a better method of controlling and administration in medical healthcare field. The application of RFID technology in the medical field means it is necessary to ensure reliable and secure access to medical information of patients as well as sensitive information management. Therefore, the RFID system is required to meet the security authentication and communication between the server and tags. More importantly, it must be ensured that user’s sensitive privacy information will not be leaked. Moreover, RFID authentication is the primary method to make an RFID system safe and protect privacy well.



**Problems that need to be overcome and security requirements**

As it is known, personal physical healthy information is closely related to individual privacy. The attackers today begin to infiltrate the cyber world, and they steal or falsify the patients’ medical privacy data, and undermine the system's normal workflow, leading to the serious result of the disclosure of medical privacy data. Therefore, security has become one of the key issues to be addressed for RFID applied in medical system safely.

Security requirements:

* Anonymity
* Replay attack resistance
* Synchronization
* Forward security
* Mutual authentication
* Non-denial of service.

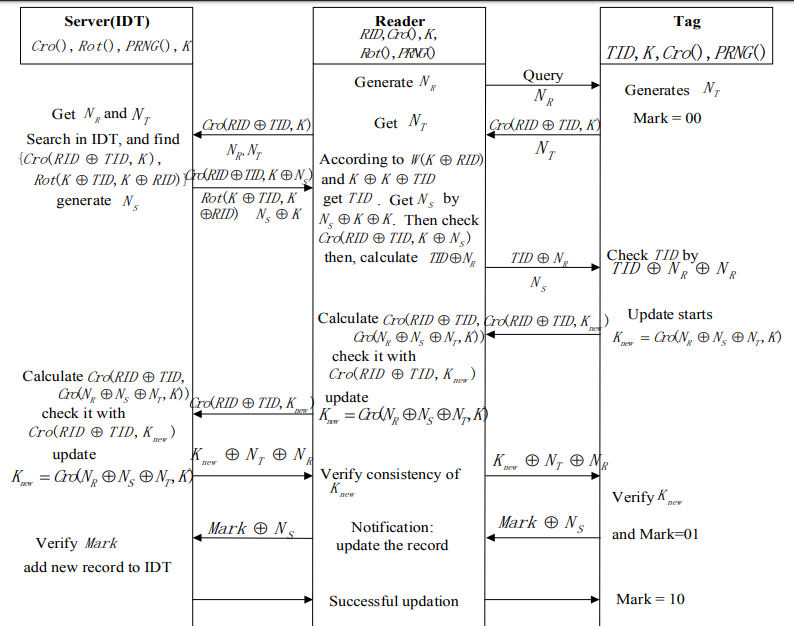
**Existing Research**

* Chien [1] proposed a mutual authentication protocol , which ensures synchronization and anti-replay attacks as well as being conformation to the standards of EPC Class 1 Generation 2, but it lacks of RFID tags anonymity, which are crucial in the healthcare system, the anonymity of the patient's identity is closely related to the safety of the vital signs.
* From this analysis research [2], we can know the Gossamer protocol lacks the features of forward security and anti-DoS attacks despite its anonymity.
* Sarah presented a cloud-based RFID protocol [3], it is with good scalability and storage performance. However, like Chien's scheme, it lacks anonymous protection of tags.
* Another authentication technology proposed by Zhou [4] mainly focuses on using fewer resources on a tag for authentication.

**Proposed Lightweight RFID Scheme**

In this scheme, IDT (Index Data Table) is adopted, which will improve the efficiency of information retrieval in server. In this table, the index content is located and obtained efficiently through the index value, and every couple of index value and index content is unique. The way they work is similar to the key-value mode, and both of them are stored in a form of cipher text rather than plaintext by some cross and rotation operation.

The proposed lightweight RFID authentication protocol is showed in the figure below.



**The details of the protocol is as follows**

Step 1: The reader generates a random number and sends it along with the query to the tag. The tag receives this number and sets its flag to 00 to denote start of the session. It then computes the bit cross and sends that along with the random number generated by the tag to the reader.

Step 2: The server obtains the random numbers generated by the reader and the tag and then searches the corresponding index content in the IDT. After the match is found the sender sends bit cross and bit rotation values along with a random number generated in the server back to the reader.

Step 3: The reader then checks for the identification of the tag and obtains

the random number of the server and send this to the tag. The tag then checks for

the identification to ensure that the reader is reading the right tag.

Step 4: In the next step a session is started and the session value is updated. The cross operation is done in the reader and the session value is updated. This process is repeated in the server as well.

Step 5: Finally we need to check the consistency of the session value by sending

the new session value to the tag and the tag will verify the session. If everything is verified the authentication is successful and a notification is sent to the server to provide the required data to the reader.

**Results and Analysis**

Tag Anonymity:

The tag identification it is transmitted in the form cipher text and never disclosed publicly because it is never communicated directly between the tag and reader, and it is only stored locally in the tag and used for a legal identity authentication in step 3 in the protocol. Therefore, the tag anonymity in this scheme is satisfied.

Consistent Synchronization:

The ‘Mark’ used in this protocol is 2-bit flag which can be used for signing the current system synchronization status, is very simple and effective.

Replay attack resistance:

In this scheme, the tag, reader and server generate random numbers moreover, those random numbers will change in the next session. Therefore, if the attackers somehow get those messages, they cannot attack the next session with that information so that the further session is secure still. Therefore, this scheme can withstand replay attacks.

Forward secrecy:

Since the random numbers are generated for every new session it means any secret message containing those parameters or consisting of them is fresh in current session, so it is difficult for the attacker to obtain any useful previous information according to the current messages. Therefore, this proposed scheme is of forward secrecy.

Mutual authentication:

In this scheme the reader is authenticated by the server in step 2. In addition the tag authenticates the reader in step 3 and the tag is authenticated by the reader in step 4. Hence this protocol ensure mutual authentication.

Anti- DoS attacks:

Denial of Service (DoS) attack is a common attack in the RFID system. Its goal is to stop the server system from responding or even make it crash directly. In the proposed protocol, a new data storage format is designed that exists in the form of a group of index values and index content in IDT, and the homologous content can be retrieved based on the index value without violent matching by using traversal search. It is obviously reduces the performance overhead greatly, and will not easily suffer DoS attacks.

**Computation cost and communication cost of the new protocol**

The computation cost is very low when considering a FPGA to run the protocol and hence we call it lightweight. The previous protocols have a very high computational cost for authentication. The calculation of the bit cross operation is consumes less computational resources.The communication costs for the new protocol when compared to other protocols results in the new scheme spending 5 times which represents the communication times and this when compared to other protocols the new scheme is not very outstanding at communication consumption.

**Conclusion**

The application of RFID system to the medical field, can realizes the convenience and safe management of medical privacy information. In this paper, we present a lightweight mutual security authentication protocol that can be applied to mobile medical fields.

Medical privacy information is of paramount importance to users or assets, and in this scheme, the consistency and synchronization of the authentication information is guaranteed. Moreover, it can resist against the typical attacks. It is important to emphasize that in the medical context, personal identity information is extremely important and closely related to patient’s privacy, and the proposed scheme ensures the anonymity of the tag, in line with the security requirements of medical system. In addition, this protocol uses the innovative index group to carry on the storage of authentication data, which is easy to retrieve and locate.

In further studies and research we can find better ways to improve the communication consumption cost for more efficient authentication for RFID based communication.

**References**

[1] H. Y. Chien and C. H. Chen, “Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards,” Computer Standards & Interfaces, 2007, 29(2): 254-259.

[2] Z. Bilal, A. Masood, F. Kausar, “Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol,” in Proc. NBIS, 2009, pp. 260-267.

[3] S. Abughazalah, K. Markantonakis, K. Mayes, “Secure improved cloud-based RFID authentication protocol,” in Proc. DPMASSSA, 2015, pp. 147-164.

[4] J. Zhou, “A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification,” Journal of Communications, 2015, 10(2): 117-123.