Secure implementation of IOT based on RFID with key authority mechanism

Jebah Jaykumar, Prameetha Pai, Prarthana T.V

Abstract—Internet of Things (IOT) based on RFID has been a focus of research in recent years. This emerging area has been identified with several security issues based on RFID. In this paper we design a secure architecture for Internet of Things based on RFID using secure key authority. Experimental results show that this method boosts authentication and provides a strong cryptography for secure transmission of RFID tag information across the entire network.

Index Terms ----The internet of things; RFID; Key-Authority; Security; Attacks

1 INTRODUCTION

Internet of Things gives objects the capacity to identify itself, perceive the surrounding data, interact with servers over the internet and make queries to change their state. These objects can be personal objects such as smart phones, digital cameras or elements in our environment.

The Internet of Things is a scenario in which objects, animals or people are provided with unique tags and these tags have the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. Thus internet of things refers to the ways of connecting things for intelligent control and management. Radio-frequency identification (RFID) is seen as prerequisite for the Internet of Things. RFID is used for sensing the objects and also for transfer of information about the object onto the network wirelessly till it reaches its destination.

The basic ideology behind the working of RFID technology is explained in section II, section III briefs on how RFID is used in implementing internet of things, the security issues is briefed in section IV, section V shows how key authority technique can be used for Secure implementation of RFID for IOT and section VI has conclusion with the basic summary of the advantages of using this method of authentication.

- *Jebah Jaykumar,Assistant Professor,BNM Institute Of Technology,Bangalore,India, j.jebah@gmail.com*
- *Prameetha Pai, Assistant Professor,BNM Institute Of Technology,Bangalore, India,prameetha@gmail.com*
- *Prarthana T.V,Assistant Professor,BNM Institute Of Technology,Bangalore,India, prarthanatv@gmail.com*

2 RFID TECHNOLOGY

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. Data stored on RFID tags can be changed, updated and locked. RFID tags can be broadly classified into 3 types: active, semi-passive and passive. Active and semi-passive RFID tags use internal batteries to power their circuits. An active tag also uses its battery to broadcast radio waves to a reader. The semi-passive tag relies on the reader to supply its power for broadcasting. Passive RFID tags rely entirely on the reader as their power source. The active and semi passive tags contain more hardware than the passive RFID tags, hence they are more expensive compared to passive tags. Therefore Active and semi-passive tags are reserved for costly items and passive tags are used for relatively cheaper items. Nevertheless , all the 3 category of tags are manufactured to be disposable, along with the disposable consumer goods on which they are placed.

These tags can be of 3 storage types

1. read-write: Data can be added or overwritten.

2. read-only: This cannot be overwritten they contain only the data that is stored in them when they were made.

3. write-once, read many(WORM): Tags can have additional data added once, but they cannot be overwritten.

At a basic level, each tag works in the same way. The working is shown in figure 1 and the procedure can be explained as follows:

Data stored within an RFID tag's microchip which is placed in the object waits to be read.

The tag's antenna receives electromagnetic energy from an RFID reader's antenna.

Using power from its internal battery or power harvested from the reader's electromagnetic field, the tag sends radio waves back to the reader.

The reader picks up the tag's radio waves and interprets the frequencies as meaningful data.

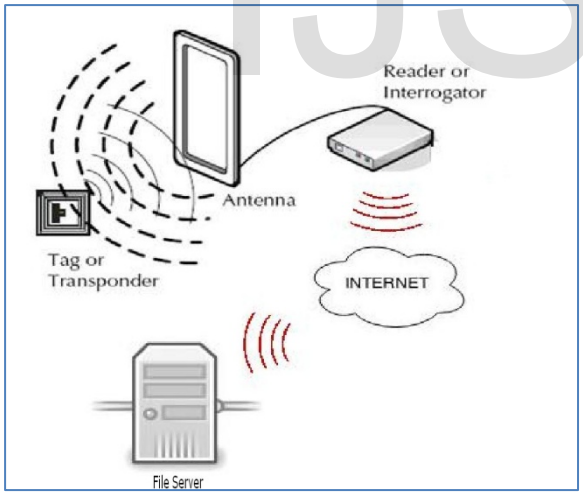

FIGURE 1: WORKING OF RFID

3 STRUCTURE OF IOT BASED ON RFID

RFID is often seen as a prerequisite for the Internet of Things.

The typical internet of things based on RFID is composed of three major components including RFID system, middleware system and Internet system.

a) RFID system consists of readers, tags and antennas. Identification of target is done with a unique Electronic Product Code (EPC) saved in RFID tag. RFID tags are wireless devices which communicate with RFID readers. Readers include transport, receiver and microprocessor responsible for reading or writing tag information. Radio-frequency signals between RFID tag and the reader are transmitted by Antennas. This layer collects information and identifies the physical world.

b) The middleware system is responsible for information transmission, initial processing of information, and classification of data. This layer includes key server and Object Naming Service (ONS) server.

c) The Internet system is responsible for analysis, processing, control and decision making of information to implement customized services ordered by users and controlling the connection between things and things. This layer includes the internet and database (PML database).

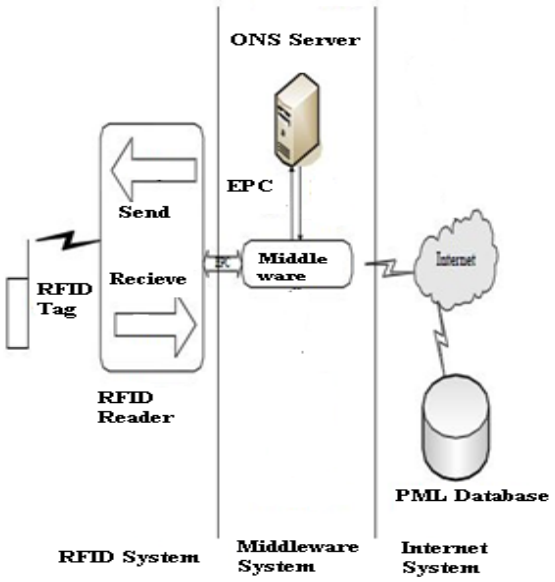

FIGURE 2: WORKING OF IOT

Through the EPC code saved in RFID tag, the reader collects data from the tag. The middleware

system can find the relevant information of the object by finding the corresponding IP address on the Object Naming Server on the internet through this EPC code and the information is processed and managed by the middleware system.

4 RFID BASED SECURITY ISSUES

The security of RFID tags and the information transmission is of prime concern and during the recent years a large number of research papers have appeared dealing with the security issues of RFID.

[1] [3] [5] [6] have shown in depth, the security issue in the internet of things based on RFID. Based on the study made on these references the various security issues are populated and present in table1.

TABLE I. SECURITY ISSUES

Threats	Category
Illegal use of Tags and Tag cloning	RFID System Security Threat
Destruction Of Data	
Personal ID Leak	
Denial of Service(DOS)	Communication Security Threat
Wireless Attack	
Wired Communication Attack	

1) Illegal Use of Tags and Tag Cloning :

Unauthorized users may illegally use the RFID tags, and the EPC code sent by the tags may be collected by attackers, leading to tag cloning.

2) Destruction of data :

The attacker may destroy the reader data by using electromagnetic waves.

3) Personal Identification leak :

The traceability and identification of tags through EPC code can lead to leakage of identity.

4) Wireless attacks : Since RFID readers and tags use wireless communication, the open wireless signals lead to easy monitoring and jamming of wireless communication signals by the intruder.

5) Wired communication attack :

The connection between reader and middleware system are imposed with the risk of compromising with data confidentiality and integrity.

6) Denial of Service (DOS) :

The attackers controlling a large number of fake tags and readers can make the connection to use up the network bandwidth and resources.

5 SECURE ARCHITECTURE FOR IOT BASED ON RFID AND KEY AUTHORITY

In this scenario we propose a central authority maintaining a dynamic directory of public keys of all participants. In addition, each participant reliably knows a public key for the authority, with only the authority knowing the corresponding private key.

The following steps occur:

1. The RFID reader sends a time stamped message to the key authority containing a request for the current public key of server.

2. The authority responds with a message that is encrypted using the authority's private key, PRauth. Thus, reader is able to decrypt the message using authority's public key. Therefore reader is assured that the message originated with the authority.

The message includes the following:

i) Servers public key (PUb) which the reader can use to encrypt messages destined for server.

ii) The original request used to enable the reader to match this response with corresponding earlier

request and to verify that the original request was not altered before reception by the authority.

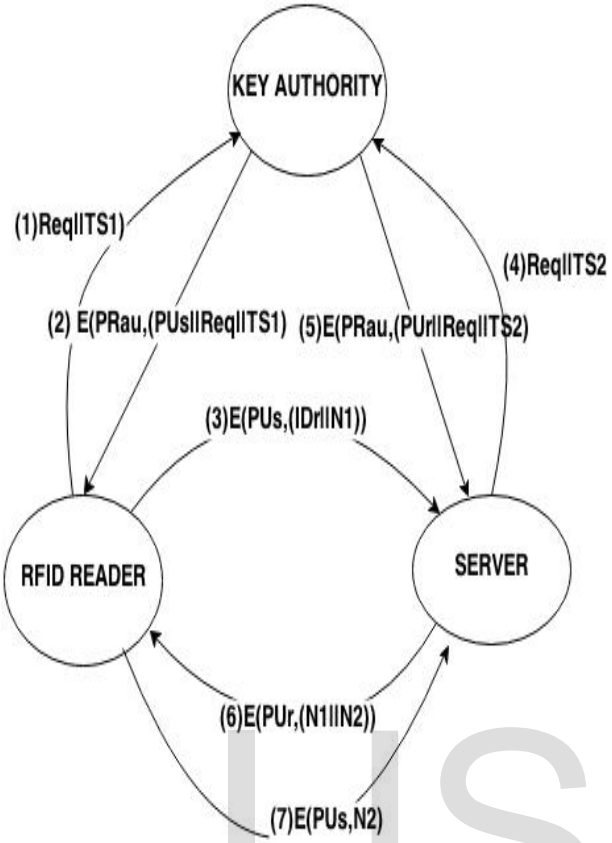

FIGURE 3: SECURE IMPLEMENTATION OF IOT USING RFID WITH KEY AUTHORITY MECHANISM

iii) The original timestamp given so reader can determine that this is not an old message from the authority containing a key other than server's current public key.

3) Reader stores servers public key and also uses it to encrypt a message to server, containing an identifier of reader (IDr) and a nounce N1 which is used to indentify this transaction uniquely.

4& 5) Server retrieves a reader's public key from the authority in a similar way.

6) Server sends a message to reader encrypted with PUa and containing readers nounce N1 as well as a new nounce generated by the server N2, because only server could have decrypted message(3), the presence of N1 in message(5) assures reader that the correspondent is the sender.

7) Reader returns N2, which is encrypted using server's public key to assure the server that the correspondent is a reader.

6 CONCLUSION

RFID is an easy-to-use and versatile acquisition information technology. The use of this technology is constantly evolving and expanding at an exponential rate. This paper applies the key authority into the internet of things. Aiming the security problem of the internet of thing, this paper provides security architecture of the internet of things based on key authority. Experiments show that: the method proposed in this paper greatly improves the system efficiency, at the same time, almost hasn't decreased the security performance of the system.

REFERENCES

[1] Shao Xiwen, "Study on Security Issue of Internet of Things based on RFID," Proc. IEEE 2012 Fourth International Conference on Computational and Information Sciences(ICCIS), IEEE Press, Aug.2012, pp. 566–569, doi:10.1109/ICCIS.2012.301.

[2] Xiao Nie;Xiong Zhong "Security In the Internet of Things Based on RFID: Issues and Current Countermeasures" in Proc. 2nd International Conference on Computer Science and Electronics Engineering ICCSEE 2013. International Conference, 2013.pp.1181-1184.

[3] Dang Nguyen Duc; Hyunrok Lee;Konidala, D.M.; Kwangjo Kim "Open Issues in RFID Security", in Proc. Internet Technology and Secured Transactions, 2009. ICITST 2009.International Conference, Nov. 2009, pp.1-5.

[4] Kai Fan, Jie Li and Hui Li "ESLRAS: A Lightweight RFID Authentication Scheme with High Efficiency and Strong Security for Internet of Things", 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, pp. 323 –328,doi: 10.1109/iNCoS.2012.48

[5] LI U Li min , X IAO De bao, LI L in , SH UI Hai hong "Information Security and Its Countermeasures of RFID System of Internet of Things Sensing Layer", JOURNAL OF WUHAN UNIVERSITY OF TECHNOLOGY, Vo l. 32. No. 20. Oct. 2010, pp.79-87.

[6] Ton van Deursen, "50 Ways to Break RFID Privacy," IFIP AICT(Advances in Information and Communication Technology) Vol. 352, pp. 192–205, 2011.

[7] Serge Vaudenay ,"On Privacy Models for RFID", Advances in Cryptology – ASIACRYPT 2007, Lecture Notes in Computer Science Vol. 4833, pp. 68-87, 2007.

[8] Tao Yan, Qiaoyan Wen ,"A Secure Mobile RFID Architecture for the Internet of Things", Proc. IEEE Information Theory and Information Security (ICITIS), IEEE Press, Dec. 2010,pp.616 619,doi:10.1109/ICITIS.2010.5689514.

[9] Xiaolin Jia, Quanyuan Feng, Taihua Fan, Quanshui Lei,"RFID Technology and Its Applications in Internet of Things (IOT)", in Proc. 2012 2nd International Conference on Consumer Electronics,Communications and Networks(CECNet), April 2012, pp. 1282 –1285.

[10] Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in Proc. 8th ACM Conf.Comput. Commun. Security, V. Atluri, Ed., 2003, pp. 103–111.

[11] Korkmaz, E.; Ustundag, A.,"Standards, Security & Privacy Issues about Radio Frequency Identification (RFID)" ,RFID Eurasia, 2007 1st Annual, pp. 110,doi:10.1109/RFIDEURASIA.2007.4368148.