IJMTST

Volume: 2 | Issue: 10 | October 2016 | ISSN: 2455-3778

A Novel RFID Readers Employee Management System

Avula Surendra[1] | K. Madanna[2]

[1]PG Scholar, Department of ECE, Geethanjali College of Engineering & Technology, Kurnool, AP, India.
[2]Associate Professor, Department of ECE, Geethanjali College of Engineering & Technology, Kurnool, AP, India.

ABSTRACT

Radio Frequency Identification (RFID) is a new generation of Auto Identification and Data collection technology which helps to automate business processes and allows identification of large number of tagged objects using radio waves. RFID based Employee Management System (EMS) would allow complete hands-free access control, monitoring the whereabouts of employee and record the attendance of the employee as well. The access tag can be read up to 5 (~16 feet) meters from the RFID reader, which usually eliminates the need to handle the tag or to walk very close to the reader. This freedom is particularly important to handicapped workers, staff carrying packages. The proposed system is based on UHF RFID readers, supported with antennas at gate and transaction sections, and employee identification cards containing RFID transponders which are able to electronically store information that can be read / written even without the physical contact with the help of radio medium. This paper presents the experiments conducted to set up RFID based EMS.

KEYWORDS: *API, GUI, RFID, Readers, Tags/Transponders, UHF*

I. Introduction

The objective of the paper is to discuss the issues of Radio frequency identification (RFID), what are the concepts of employee management system, cloud based employee management system and give proposed cloud based RFID authentication protocol. RFID is a technology, which has gained increased attention of researchers and practitioner's. This enables acquisition of data about an object without need of direct line of sight from transponders and readers [4]. To make RFID system more secure, authentication is one solution. It also maintains the security and privacy of system. Tag identification without authentication raise a security problem. Attackers sometime may tap, change and resend messages from the tag as if it has the tagged object. An Employee management system using RFID becomes efficient on cloud system because it has several advantages like (1) Verifier is enabled to authenticate the tagged objects using any reader over internet. (2) Pay on demand resource distribution is effective for small and medium scale organizations. (3) Cloud is more robust due to resource sufficiency. However, this cloud-based RFID is in sufficient in two aspects. (1) Most current works focused on functionalities without giving importance to security and privacy. (2)No study shows that classical RFID schemes meet the security and privacy requirements of cloud based systems. This system can be effectively used for calculating the attendance, salary of a particular employee for particular month and for track keeping of him/her. Classical RFID schemes when moved to cloud, they are having the problems of insecure database, privacy of tags and a reader gets revealed which is not acceptable. Because cloud is publically available to any one and the clients cannot fully trust on the cloud service providers. So to recover from these drawbacks, cloud-based RFID authentication protocol should get developed. It also secures the database using hashing technique like SHA1 and maintains the privacy of tags, readers [3]. Successful implementation of this system brings the advantages like deployment cost saving, pervasiveness of authentication. Tag verification complexity reduces to O(1). It preserves the privacy of tag and reader holders. It makes the database more secure.

II. Related Work

2.1 Traditional RFID

There is an extensive work on RFID authentication schemes which are, backend server based and server-less [1] [2]. The back end server based RFID is shown in Figure 1. It is composed of tags, readers and backend server. Readers identify and verify the tags by querying to backend server. However, the drawback is limited mobility of readers.

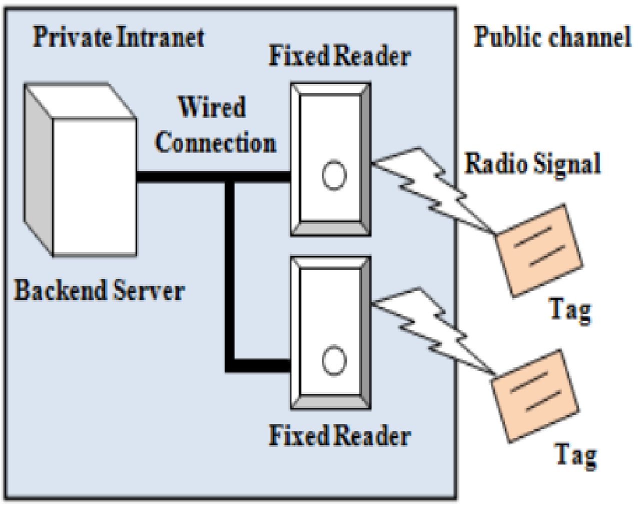

Figure 1: the backend-server-based RFID architecture.

The server-less RFID scheme is shown in Figure 2. It is composed of tags, readers and CA (Certification Agency).

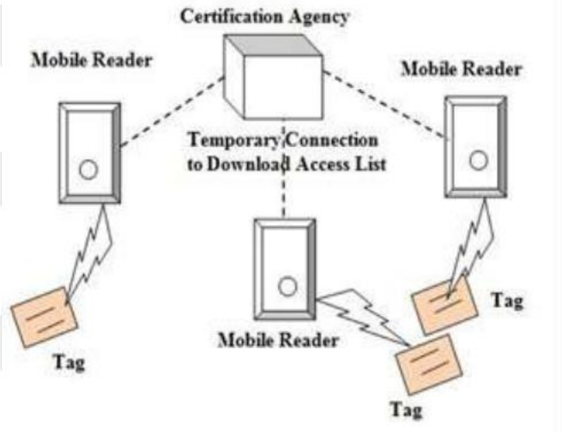

Figure 2: Server-less RFID architecture

There are two phases in server less scheme: initialization and authentication [5]. The mobile reader accesses the CA (Certification Agency) and downloads the AL (Access List) through the secure connection in an initialization phase. The mobile reader is generally a portable device such as notebook computer or smart phones. It might be stolen. Then AL is stored in it. It may wrongly be used to imitate the tags. Credentials of tag authentication are derived with the help of tags key and RID. It makes AL exclusively usable for the reader. But as a result, it is not possible for tag to create a valid request without the RID. In the authentication phase, the reader challenges a tag with RID, waiting for tags response with H (RID, Kt). The reader then searches its AL and finds the matched value to verify the Kt. It then identifies the TID. Sever-less RFID architecture provides readers with the scalability. However, there are drawbacks in server-less authentication protocol. (1) All they transmit RID in plaintext. (2) Searching through AL has complexity of O (N), where N denotes the number of tags. (3) Computational processes of searching and verifying are executed all by single personnel portable device, which reduces the performance significantly.

2.2 Requirements of cloud based RFID

Cloud based RFID has many advantages, but has the challenges of security and privacy. Existing authentication protocols are inapplicable to cloud based employee management system because of lacking two primary capabilities. Firstly, instead of providing protection to front end communication, protection of backend communication is important in Cloud based authentication schemes. Also in cloud based schemes, mobile readers often accesses the public cloud using open wireless connections. There are two solutions for this issue. (1) Establish VPN connections among readers and cloud in a network layer. (2) In application layer design an RFID authentication protocol protecting backend security [1]. Secondly, these schemes are required to prevent the privacy of tags/readers from untrustworthy cloud. Therefore, readers/tags should provide the confidentiality about data storage, which is against the cloud.

III. Proposed Solution

3.1 VPN Agency

Existing cloud based RFID system has four participants. They are tag owner, verifier, VPN agency and cloud provider [1] [6]. The VPN agency has VPN routing between readers and the cloud. Cloud service of RFID authentication is given by cloud provider to the verifier and tag owner. VPN routing makes communication between the reader and cloud as secure as in privet intranet. Attackers are able to intercept, block and resend the TCP/IP packets in the network layer. On the other hand, network-layer-anonymity of readers accessing the cloud is achieved.

3.2 Encrypted Hash Table

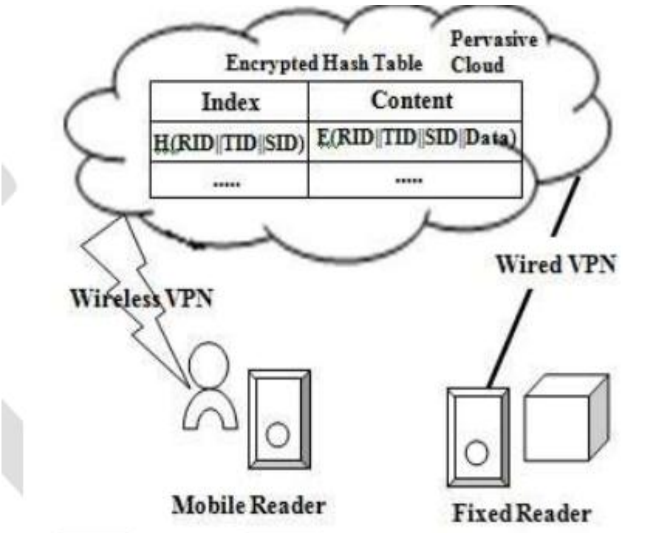

Figure 3: Proposed Cloud-based RFID authentication scheme

An EHT is proposed to prevent client's data confidentiality and access anonymity from revealing to the cloud provider. It is illustrated in Figure 4. The index which is a hash digest H (RID||TID||SID) uniquely denotes the session with SID from the reader with RID to tag with TID. The record indexed by H (RID||TID||SID) is E (RID||TID||SID||Data). It is a cipher text according to the reader defined encryption algorithm with a reader managed key. The RID field is used to check the integrity of the cipher text after decryption by reader. Mutual authentication is done using TID between reader and the tag. The SID field is the identifier which is a term in a reader defined sequence. The data field stores any application data such as location of tag and access time.

3.3 Proposed Cloud-based RFID authentication Protocol

The proposed cloud based RFID authentication protocol is illustrated in Figure 4 [1]. For simplicity, replace RID by R, replace TID by T and SID by S. Encrypted function E (RID||TID||SID||Data) in EHT is now simplified to E (R||T||S). Other notations listed in this section are as shown in Table 1. S+1 is the next incremental term after Sth term in the sequence defined by reader. 1st step is for the reader to obtain T and S. The tag generates H (T||R||S) as an authentication request and sends generated authentication request to the reader. H (R||T||S) acts as an index to the cipher text E (R||T||S).

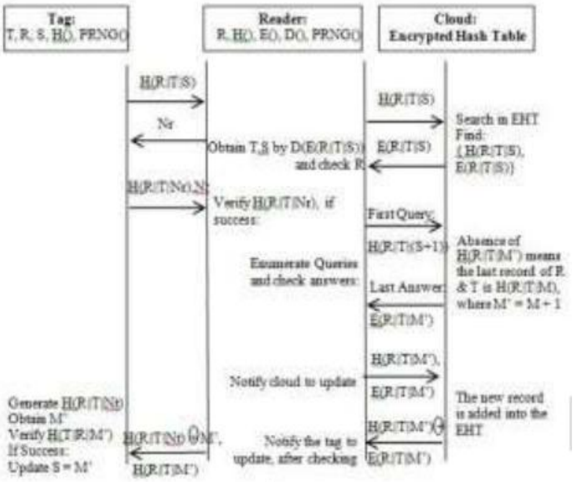

Figure 4: Proposed cloud based RFID authentication Protocol.

The reader does the following operation. (1) It reads the cipher text from the cloud EHT and decrypts it in the useful form (2) It then verifies R for integrity and obtains T and S. Authentication of the tag take place in 2nd step. The reader challenges the tag by generating a random number Nr. The tag calculates hash based on challenge Nr received from reader. The tag uses H (R||T||Nr) to generate random nonce Nt and sends Nt as its challenge to the reader. Synchronization of S between the encrypted hash table (EHT) and the tag take place in 3rd step. The reader checks the integrity after reading the next record indexed by H (R||T||(S+1)) from the EHT. Tag has been desynchronized if the valid record is present in EHT. The reader continues the same action until it finds the last valid record, assuming its SID is M. In 4th step the cloud EHT gets updated. In EHT, cipher text E (R||T||M') having index H (R||T||M') is added by reader, where M'=M+1. A message of H (R||T||M') + H (E (R||T||M')) is send back to the reader from the cloud to confirm that the updating is successful. 5th step is to send a comprehensive response to be verified by the tag. In response to tag's random challenge Nt, reader calculates H (R||T||Nt). For simple encryption, response is XORed with M'. Encrypted M' is sent to tag with index H (R||T||M') and get verified by a tag. 6th step does authentication of the reader and also it repairs the desynchronization. To obtain M', tag calculates H (R| |T||Nt). Calculated value gets XORed with the received value H(R||T||Nt) M'. It then calculates and verifies H(R||T||M'). If success, it means the M’ is not modified. By updating S=M’ on the tag, synchronization is achieved.

IV. Implementation

4.1 Mathematical Model

In the proposed cloud based RFID authentication scheme readers anonymously access the cloud through wireless or wired connections. An encrypted hash table stores the client’s secrets in encrypted form so that secrets should not be easily revealed to the cloud [3]. The first RFID authentication protocol is proposed which preserves the privacy of readers and tags.

Defining System:

Consider an organization with N employees S = {}

Identifying input:

Let, S = {Db, U, T, A, R, Cp} Where,

Db = System database with two tables:

- Employee
- RFID track

U is set of users such that,u1, u2, u3... un ϵ U

T is set of users track such that, t1, t2, t3 ....tn ϵ T

A is set of user’s attendance such that, a1, a2, a3 ...an ϵ A

R is set of user’s RFID tag such that, r1, r2...rn ϵ R

Venn diagram of the System:

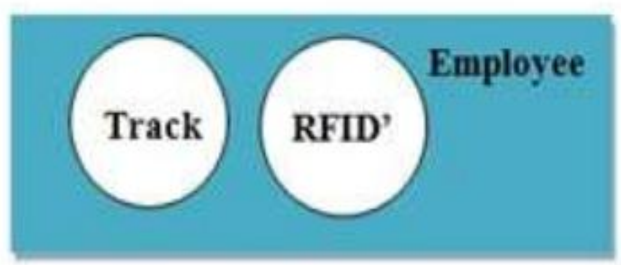

Figure5: Set diagram of employee management system

Functionalities:

The functions of the system are as follows:

(1) U = new Employee (u_id, u_name, u_add, RFID’)
Where,
RFID’ = SHA1 (RFID tag)

SHA1 algorithm:

Input: Max 264-1 bit uses 512 bit block size

Output: 160 bit digests

Steps:

Padding message with single one followed by zeros until the final block has 448 bits and appends the size of original message as an unsigned integer of 64 bit.

Initialize the 5 hash blocks (h0, h1, h2, h3, h4) to the specific constants defined in SHA1 standard

Hash (for each 512 bit block)

Allocate an 80 words array for the message schedule

First 16 words are obtained by splitting message into 32 bit block.

Rests of the words are generated by following algorithm:

Word [i-3] XOR Word [i-14] XOR Word [i-16] then left rotate it by 1 bit.

Loop 80 times doing the following:

Calculate SHA function() and constant K(these are based on current round number).

e = d

d = c

c = b(rotated left 30)

b = a

a = a(rotated left 5) + SHA function() + e + k + Word[i]

Add a, b, c, d and e to the hash output.

Output the concatenation (h0, h1, h2, h3, h4) which is the message digest.

(2) t = new Track Info (RFID’, location, date, time)
Keep track of particular employee at different time.

(3) a = get Attendence Info (RFID’, Date)
Calculate employee attendance for particular period.

4.2 Block Diagram of the System

Block diagram of employee management system using cloud based RFID authentication is illustrated in Figure 6. System contains the following parts:

(i) RFID Reader:

It is used to read the tags using radio channels and passes to the verifier for the authentication.

(ii) Webcam:

Webcam is used to take the snapshot when reader tries to read the tag.

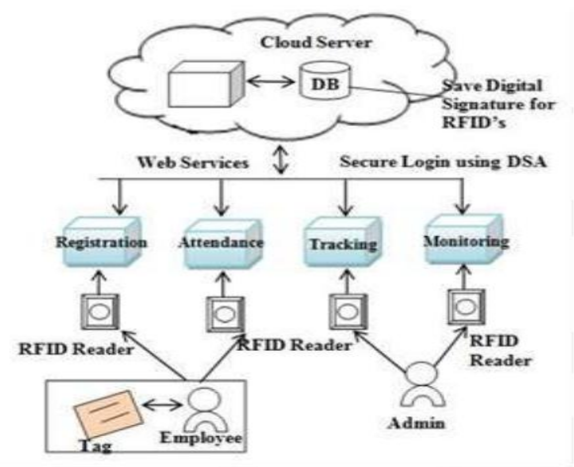

Figure 6: Employee management system using Cloud based RFID authentication

iii. Cloud Service provider:

Cloud service providers are those who provide private/public cloud. Different terminals can be connected to the cloud through the internet network. Deploying employee database, tracking database, admin web service module on the public cloud enable users to access database and web service from anywhere/anytime using Internet.

iv. Admin:

Admin may be the individual machine which has administrative functionality. Admin is connected to cloud service provider via internet connectivity. Admin's web service is deployed on the public cloud which client can access.

v. Client:

Client may be the individual machine or a thin client. Client is connected to cloud service provider using internet connectivity.

V. Implementation

In this system of employee management, a new cloud based RFID authentication protocol is developed which provides security and confidentiality. It helps for calculating attendance, salary of an employee and also keeps a track of him/her. It provides other advantages like deployment cost savings, pervasiveness of service and scalability. Also, Comparison of the tag verification complexity in traditional sever based model, server-less model and cloud-based RFID model is shown in Figure 7. Both server-based and server less RFID authentication protocols depends on search through the database or AL to find matching TID. It makes computational complexity to verify tags as O (n), where n is number of tags. It means these two protocols are not well scalable. In proposed protocol index H(R|T|S) is generated by tag, it is then send to reader. Reader then read the matched record from EHT instead of searching through all TID's. Hence, complexity of proposed scheme is only O (1). That means, itis better scalable than most of the other protocols.

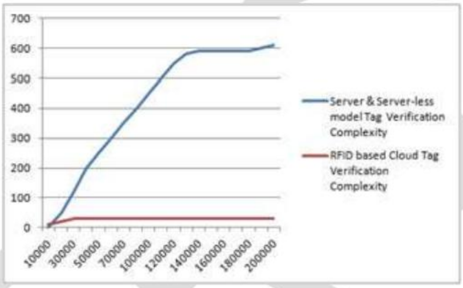

Figure 7: Comparison in the complexity of protocols

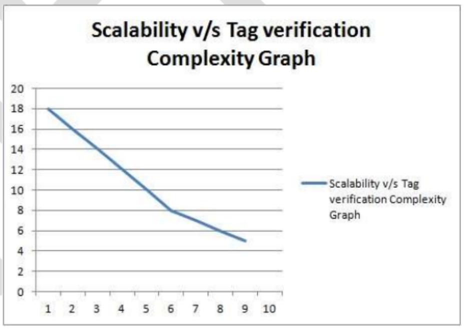

Figure 8: Scalability v/s tag verification complexity graph

VI. Conclusion

RFID Based Employee Management System is systematically characterizes the reliability of RFID systems and its dependence on various practical factors. The results will provide important guidelines for real world deployment of RFID-based tracking applications as well as simple yet effective solutions to guarantee reliability. Reading items and objects in motion can be done accurately using RFID. A system developed with a log in windows enables security and the overall cost of implementing the system may seem high but after a year of running the system, very high benefits will be realized. The whole system is very convenient and saves much on time.

References

[1] D. Lakshmi and M. Kumar, "A Pilot Project for Postal Parcel Tracking Using UHF RFID Tags", Proceedings of Annual Seminar on C-DAC Noida Technologies (ASCNT), pp 28-33, February, 2008.

[2] Charles A. Walton, "Portable Radio Frequency Emitting Identifier", U.S. Patent 4,384,288 issue date May 17, 1983.

[3] C. Englund and H. Wallin, "RFID in Wireless Sensor Network", Tech. Report, Department of Signals and Systems, Chalmers University of Technology, Sweden, pp.1-69,2004.

[4] Lalit Kumar and ChandanMaity, " Design and Development of Low Cost UHF Reader", Proceedings of Annual Seminar on CDAC Noida Technologies (ASCNT), C-DAC, Noida, pp. 215-222, March, 2009.

[5] SourishBehera and Rajesh Kushwaha, " RFID Based People Management System", Proceedings of Annual Seminar on C-DAC Noida Technologies (ASCNT), C-DAC, Noida, pp. 227-234, March, 2009.

[6] Bill Glover and Himanshu Bhatt , "RFID Essentials", O'Reilly Media, A Text Book, Edition 2006 ISBN 0-596-00944-5, pp. 88- 89,2006.

[7] Unnati A. Patel, "Student Management System Based on RFID Technology", International Journal of Emerging Trends & Technology in Computer Science

(IJETTCS) , Vol. 2, Issue 6, ISSN 2278-6856,pp. 173-178, November – December 2013.

[8] Paolo Magrassi," The Role Of Auto Identification Technologies", Strategic Analysis Report, Gartner Research Group, Stamford, USA, 2002.

[9] Miles and Stephen Bell ,"RFID Technology and Applications", RFID Jounal, London: Cambridge University Press, Orlando, pp. 6– 8,2011.