Efficient Record Management using RFID - Arduino Technology

Ratnakumari Challa
Department of CSE
RGUKT, IIIT, Kadapa, India

B. Reddaiah
Department of Computer Applications,
Yogi Vemana University,
Kadapa, India

K. Srinivasa Rao
Department of Computer Applications,
Yogi Vemana University,
Kadapa, India

ABSTRACT
Increase in on-line activities or E-commerce there is a need of efficient and secure management of records that store the data of various transactions and its assets. It is very difficult to manage large number of records manually where different operations are to be carried-out in limited period of time. It basically increases time and effort in traditional transaction management and in goods management process in business field where human resource are applied, and there is a problem of knowing the stock details like expiration through manual record checking. So, this work provides a technique to give efficient record management and secured transactions by retrieving efficient information from the tag contained in goods or stocks. It gives quick information about stock while verification. So, it provides information like Product name, Tag -id, DMFG, expiry date and details about how long the product can be used. Through this work time can be saved in processing the records and cost in doing business activities will be minimized.

Keywords
E-commerce, Record management, Tag-id, DMFG, RFID, Arduino.

1. INTRODUCTION
Radio frequency identification (RFID) technology taking fast grip in today's technology. It is also providing huge benefits in industrial and E-commerce business by providing good security and assets management. RFID audit is attainment with added importance in maintaining records. Radio frequency identification systems that are in existence are helpful for automatic retrieval of data that relates to products, people, or animals known as objects [1]. The below figure 1 shows the architecture of the RFID technology based System.

The object is incorporated by means of a tiny circuit called RFID tag. The facts that are put into it can be spontaneously recovered by a reader device tag. This helps the object to identify [1] some of applications of RFID system like slow read rates, reduced shipping (or) storage security, locating lost or misplaced tapes and tracking tape movement between data centers, off-site storage. Clients can similarly earn the benefits from goods being capable of communicating with their surroundings [3]. Further some more applications for RFID systems exists as access control, animal tracking, evidence for origin of goods, toll systems, car immobilization etc. There are uniform methodologies to secure money by means of RFID tags [3].

RFID technology offers lots of benefits in several areas. Manufactures, developers and vendors save money by improved automation of production and warehousing [1]. Each RFID structure is built with a tag that is attached to the object to recognize and a reader, which is capable of retrieving data from the tag. The reader might be capable of writing facts to the tag's memory [4]. Moreover to put into practice an application with data collected from the tags, Host commands are used by host. These are changed into reader requirements and broadcaster via radio frequency. If a tag is within the reader's area, it redirects a response. Reply given by Tag might be processed by the host equivalent to the current application [5]. Inspection is an on-site authentication activity of process or quality system.

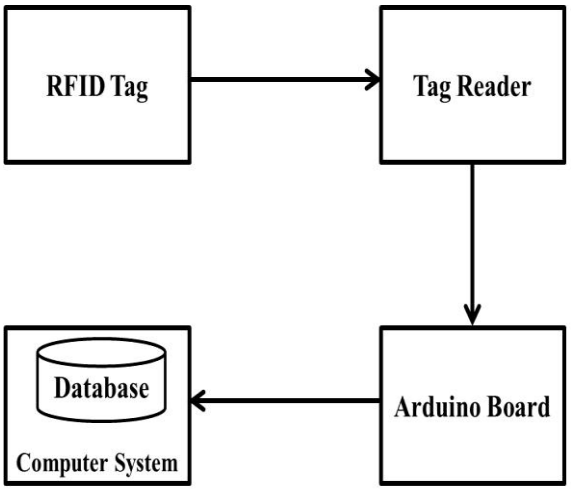

Fig.1 Architecture of RFID based system

Audit can be applied and used by whole enterprise or can be particular to a defined function, processor product step [3]. Authorized investigation and authentication of accounts and records, particularly of financial account's report or statement reflects an audit [3]. Present RFID audit delivers yearly audit through reports of each item that is storage. Certified and regulatory organizations may have this report to validate that the files are retained and stored properly [2]. With RFID audits, one has the prospective to change the procedure of verifying documents [2]. In general from the traditional tags we can yield more information from record verification while scanning. So it gives some more additional knowledge and facts that belong to the product. It provides information about the product in the form of Product name, Tag id, DMFG, expiry date and how long we can use the product. Auditors can make the quick business decisions by scanning the goods. It is very expensive to know the information about DMFG and expiry date of a product. The main goal of this work is to provide better information about goods and to draw the quick business decisions. Business auditors can predict the goods

state and take quick decisions with in a fractional time on transaction. These decisions can be taken for effective and efficient stock maintenance.

2. RELATED WORK

Services that are provided by cloud technology are by means of public networks or through private networks of enterprises. Through cloud applications like e-mail, web conferencing, customer relationship management (CRM) are executed. Cloud computing is the process of controlling, configuring, and using the applications through network. Cloud provides infrastructure for storing the data, software and platform through network [7, 8].

With the services provided by cloud by using network which cannot be trusted cloud computing has the following challenges.

1. Security and confidentiality
2. Portability
3. Interoperability
4. Evaluating the performance
5. Consistency and ease of accessibility

AES and DES algorithms are used to overcome security and privacy challenges [6]. AES is an algorithm used for encrypting data in the cloud to provide security to the data for ease of use.

2.1 Benefits of Radio frequency identification solutions

a) Lower costs and higher productivity

b) Increased revenues

c) Shorter processes

d) Better security

e) More accurate, relevant and current management information.

2.2 Cryptographic as Background

Ingredients play a vital role in cryptographic systems. In these ingredients key used to process the text is very important. Key plays a very important role throughout cryptography. Because of this importance of key cryptography is divided into two categories based on key that is used in processing text. They are symmetric key systems and asymmetric key systems [10].

2.2.1 Private key Cryptography

The first category of cryptographic system is called symmetric system also termed as private key cryptography. Here single key is used generally known as secret key for encryption as well as decryption. With this approach data confidentiality can be achieved for user data that is intended to be transmitted over un trusted network [10]. Even though it is good for confidentiality it does not address authentication. This is the main setback in this approach. Other than that this key cannot be trusted for more period of time, as there is every possibility that the hacker may find the key. There is also a problem in developing the key and distributing the key in between sender and receiver. Because of these reason users has to change the form of key frequently.

2.2.2. Public key Cryptography

The second category of cryptographic system is called asymmetric system also termed as public key cryptography. Here two keys are used generally known as public key and private key [9, 10]. In these if one key is used for encryption the other should be used for decryption. Public can be given to any user in the network while private key cannot be shared and it is confidential. With this approach data confidentiality for user's data and authentication for the user can be achieved in a trusted network.

Even though both confidentiality and authentication is achieved still this approach has its own problems in terms of security. Here key development needs to have additional amount of arithmetical operations. This increases the complexity, which reduces the performance of the system that is used.

3. AES ALGORITHM

Advanced Encryption Standard (AES) is a private key approach. AES algorithm is intended to mix up data by substitution ad transposition techniques. Single key is used in messing up the data and that will be privately stored or transmitted over un-trusted network. When it is transmitted at the other end the user with key only can decrypt the messed data into original form.

Other algorithms are public key encryption on methods, like RSA which unscramble and scrabble with different keys. AES has a fixed block size of 128 bits and a key size of 128, 192 and 256 bits. Messages which are longer than 128 bits are broken into blocks of 128 bits. If the message is not divisible by the block length, then padding is appended. For encrypting the message the AES encryption algorithm take key and messages as input and produces output as encrypted message. Symmetric authentication can be performed with encryption algorithms or can be based on keyed hash functions. Various reasons made the AES algorithm our favorite to use for the proposed authentication protocol. This encryption algorithm was chosen 2001 as encryption standard and is considered to be highly secure. Protocols for symmetric challenge response techniques based on encryption. Unilateral authentication work as follows.

There are two partners A and B. Both possess the same private key K. B sends a random number rB to A. A encrypts the random number with the shared key K and sends it back to B. B proofs the result and can verify the identity (in other words the possession of K) of A.

$$A ? B : rB \quad (1)$$

$$A ? B : EK (rB) \quad (2)$$

The mutual authentication protocol works similarly. B sends a random number to A. A encrypts rB and a self-generated random number rA with the shared key K and sends it to B. B decrypts the message and can proof if rB is correct and gets rA. B changes the sequence of the random numbers encrypts it with K and sends it to A. A proofs the result and verifies the identity of B.

$$A ?B : rB \quad (3)$$

$$A ?B : EK (rA, rB) \quad (4)$$

$$A ?B : EK (rB, rA) \quad (5).$$

4. PROPOSED WORK

In this section, proposed Arduino and RFID based record management system will be presented in figure. 2 and described the functions of each component. This is implemented for managing the records efficiently and to provide the security for the record information. The total process involved in record management and processing

system is presented in various stages, like Reading Tag information stage, information processing stage, information transmission stage and display/presentation stage. Firstly, in reading tag information stage, it scans the RFID tag and reads the tag information by the RFID reader. The information is sent to the Arduino (Microcontroller Process) where the tag information is processed using Arduino programming. Processing of information in processing stage includes formatting the information in order to store it in the database, encrypting the sensitive details before storing in the database, retrieving data from the database, decrypting the data and display the information to the users. Any encryption algorithm can be used to secure the data before transmission. In transmission stage, processed information is transmitted to the database server using Ethernet shield. Finally in the display stage, processed records are displayed or presented to the user by a web based application.

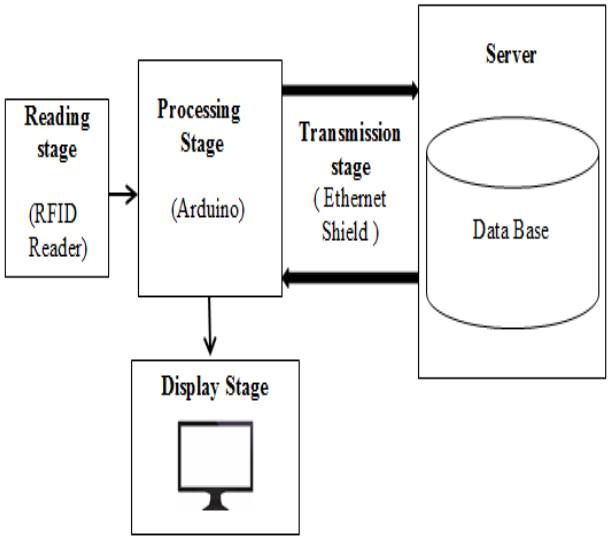

Fig.2 RFID-Arduino based Record Management System

Arduino microcontroller is being used in the system. It is an open source single board microcontroller with open source electronic wiring platform. It provides a convenient way to use hardware and software. It facilitates easy way to provide input / output hardware connections to the various hardware devices and to program for processing of the inputs to produce the required output.

Arduino connections are made to the various components of the system. The first pin is power supply, connected to 3.3V, second pin is RESET, connected to D9, third pin is connected to GROUND, Forth pin NC, is not used, Fifth pin is MISO, connected to D12, Sixth pin is MOSI, connected to D11, Seventh pin is SCK, connected to D13, and last pin is SAD, connected to D10. Ethernet shield is configured with Arduino. It is the most reasonable and convenient way to provide wired connection with the server. The input data is processed by Arduino and sent to the server for storing or archiving it in the database as shown in the figure 3. In place of Ethernet shield, Wi-Fi shield can also be used for providing wireless connection between Arduino and server in the limited range.

←T→	Index ▲ 1	rfid	Date
Edit Copy Delete	63	100	2017-04-20 06-06-35
Edit Copy Delete	64	50	2017-04-20 06-09-42

Fig.3 RFID based Records stored in the database

5. OBSERVATIONS

The observations from the practical implementation of proposed system made to conclude that it is difficult to maintain the stock or goods through the traditional stock or goods management process which involves fractional time limit transactions. Here this system uses RFID technology which is fast and secure in goods management field. Traditional goods management cannot provide good knowledge about items. Now, though RFID-Arduino based system, it is efficiently maintaining and managing the record information (like manufacturing date, item expire date and left out time for item usage etc).

6. RFID - ARDINO BASED SYSTEM APPLICATIONS

This RFID-Arduino based record management system is useful in many real time applications. Few applications are presented as follows:

• Airport luggage Tracking system: Each controlled bag can be equipped with an RFID tag and can be tracked throughout the whole airport. All assigned tag numbers are stored in a central server.

• Student information System: Attendance system, Assessment and resident students Out pass system: Each student has an ID card which is equipped with RFID tag. Every student details can be recorded and maintained easily.

• Library System: An RFID library solution improves the efficiency of circulation operations. While barcodes require line of sight, RFID tags can be read from multiple angles which means the checkout and check-in process is significantly faster. Also, as noted above in the retail section, taking inventory of books on the shelf is dramatically faster.

• Faculty information system: Each faculty has an ID card which is equipped with RFID tag. Every faculty details can be recorded and maintained easily.

• Courier System: Each parcel is equipped with an RFID tag. During transportation, RFID systems can be used to track and route the parcel throughout the process from shipment to delivery.

• People Tracking: Hospitals and jails are most general tracking required places. Hospitals use RFID tags for tracking their special patients. Many jails US states like Michigan, California, and Arizona are already using RFID tracking system to keep a close eye on jail inmates.

• Document Tracking: Availability of the large amount of data and document brings lots problem in document management system.

• Healthcare: Patient safety is a big challenge of healthcare, reducing medication errors, meeting new standards, staff shortage and reducing costs are the plus points of use of RFID solutions. RFID wristbands containing patient records and medication history address several of these concerns.

• Manufacturing: RFID technology provides an easy way to manage a huge and laborious manufacturing process. This type of process helps in better analysis, reduced time in locating parts and products and production process based sensors can be installed to alert any.

• RTLS (Real Time Location System): In some applications, you need to track the real-time location of assets, employees, or customers. Whether you're measuring the efficiency of worker movements, the effectiveness of a store floor plan, or tracking the location of valuable resources, RFID systems provide visibility in any number of locations.

7. CONCLUSION

The proposed system provides practically efficient solutions through the auditing process in goods management. Efficient information about stocks and goods can be retrieved within fractional time using RFID and Arduino technology. The proposed system calculates the important information like item expiration and left out time to item usage beyond the traditional stock management process. The practical implementation of proposed system is low cost and time saving.

8. REFERENCES

[1]. Martin Feldhofer, Sandra Dominikusand and Johannes Wolkerstorffer ," Institute for applied Information Processing and Communications, Strong Authentication for RFID systems using AES algorithm".

[2]. International Organization for Standardization. ISO/IEC 9798-2: "Information Technology - Security techniques - Entity Authentication Mechanisms Part 2: Entity authentication using symmetric techniques", ISO/IEC, 1993.

[3]. A. Juels and R. Pappu. "Squealing Euros: Privacy protection in RFID-enabled bank notes", In Financial Cryptography, 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003, Revised Papers, volume2742 of Lecture Notes in Computer Science, pages 103–121. Springer, 2003.

[4]. International Organization for Standardization. ISO/IEC 18000-3.Information Technol-ogy AIDC Techniques — RFID for Item Management, March 2003.

[5]. A. Juels, R. L. Rivest and M. Szydlo. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", In Proceedings of the 10th ACM Conference on Computer and Communication Security, pages 103–111. ACM Press, 2003.

[6]. S. E. Sarma, S. A. Weis and D. W. Engels. "RFID Systems and Security and Privacy Implications. In Cryptographic Hardware and Embedded Systems – CHES2002", 4th international Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers, vol-ume 2523 of Lecture Notes in Computer Science, pages 454–470. Springer, 2002.

[7] S. Srinivasan, Basic Cloud Computing Types, Springer, 142 P. 10, 2014.

[8] Imran Ashraf, An Overview of Service Models of Cloud Computing, International Journal of Multidisciplinary and Current Research, Aug 2014.

[9] Xiaoyan Yang, Xuanpin and G Li, Jifang Li, "Application Study on Public Key Cryptography in mobile Payment, Proceedings of the 5th WSEAS Int. Conference on Information Security and Privacy", Venice, Italy, November 20-22, 2006.

[10] ShafiGoldwasserand MihirBellare, Lecture Notes on Cryptography, Cambridge, Massachusetts, July 2008.