Radio Frequency Identification Based Theft Deterrent System by Providing GSM Service

Mr.M.S.Chaudhari (H.O.D.c.s.e.dept,P.B.C.C.E.,Nagpur) ,

Prashant Nagmote

(M.TECH 2nd sem c.s.e,P.B.C.C.E,Nagpur)

**Abstract**

Safety of precious belongings is the first priority of every person. Thus in this paper we have proposed theft deterrent system using Radio Frequency Identification (RFID). In addition to this, Global Systems mobile Communication (GSM) based altering module is provided as a feedback in order make the user aware of possible intrusion. The system is provided with tag ID while its timer sensed from RFID readers are registered in the server. The connectivity is allowed for the specific distance only. When the object is taken away for the distance greater than maximum allowable range, an alarm system will be activated to generate altering signals. In order to provide the assistance to owner who is at the remote place; altering massage will be sent via the GSM module within a short period of time. This closed loop system of RFID and GSM modules combine forms a prosperous wireless theft prevention system.

**Keywords**- RFID, GSM, wireless network, security system.

**1. Introduction**

 Taking into account the risk of theft and the potential losses that theft can cause, there are steps that individuals and organizations can implement to prevent it. There are several ways

 to prevent the luxurious belongings from missing or stolen which includes technical as well as non-technical solutions. Non-technical solutions include common sense, such as keeping the object within sight, choose an inconspicuous carrying case, keep it close at hand, etc. Now a day laptops have become a valuable part of the computing field. They allow users powerful mobility with the same capacity and software of many desktops. They also allow connectivity even apart from the office, thus making people free to take their setup among them. This is extremely valuable for employees who must travel usually while reside in continual communication with their institutions. Unluckily, the information of any organization that makes laptops so precious to employees and organizations also make them profitable for thieves. In 1999 alone, over 319,000 laptops were reported stolen, and this number is increasing year by year. Thus, we have chosen laptop as an object for which we are going to design the security system.

 In this paper, we present the theft deterrent using wireless security system (WSS). In another word, RFID assistant is being provided for the purpose of security. The idea is simple; RFID tag is attached to the laptop and RFID reader is attached to server [1][2].. If the laptop is taken out of maximum possible distance of the reader by illegal user then the alarm system will be activated, drawing attention to the attempted laptop theft. This unexpected loud noise makes people awake and takes notice, something that desire thieves find very discouraging. The owner of laptop will be alerted within seconds through sending short messaging service (SMS) from the server via GSM module system [3]. This paper is organized as follows: Section I presents the Introduction, Section II presents the overview of RFID technologies, Section III introduces the system architecture while Section IV, we demonstrate the system. Finally the conclusion is presented.

**2. Methodology**

 Radio-frequency identification (RFID) is wireless non-contact system for the purposes of automatic identification and tracking that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object. The RFID device provides a unique identifier for that object as that of bar code. But the RFID have following significance advantage over the barcode

• In case of RFID reading is done automatically using RF waves without human intervention.

• Reading by barcode take more time while in RFID reader can fatly read the tag.

• RFID tag has read/write memory capability.

 Thus, the features such as the ability for a reader to read data off an RFID tag located certain meters away make RFID tags an adorable replacement for bar codes, which require line-of-sight to a reader before being read. The basic ground behind RFID systems is that it traces items with tags. These tags include transponders which emit messages readable by specialized RFID readers. Most RFID tags consist some sort of identification number. A reader retrieves information about the ID number from a database and acts on it accordingly. RFID tags have writable memory, which used to store information for transfer to various RFID readers in various locations. This information can trace the movement of the tagged item, making that information ready for use to each reader.

 On the basis of source of electrical power used RFID tags mainly divided into two categories such as active and passive. An active RFID tag has their own power source, usually obtain from on-board power source such as battery while passive tags obtain the power from the signal of an apparent reader. RFID readers also isolate in active and passive reader depends upon on the type of tag they read. Several customer protection groups issued the Principles of Fair Information Practice for RFID technology based on the OECD guidelines for the protection and privacy of transponder in order to provide basic rules for organizations to deploy their RFID systems.

Few terminologies are given below.

i. Openness - The developments, practices, and policies with respect to use the RFID systems must be open.

ii. Purpose specification - Purposes for which RFID tags and readers are used should be specified and disclosed.

iii. Collection limitation - The subsequent use of collected data should fulfil the purposes disclosed while data are collected.

iv. Security safeguards - Personal data should be protected by reasonable security safeguards from adaptation, disclosure, illegal access, and so force.

v. Accountability - Organizations that use RFID systems should be accountable to individuals in complying with these principles

**3. System Architecture**

 The system proposed in this paper will use RFID technology as a single hop network. The RFID reader can read RFID tags and hand over that information to server, which the user shall be able to manoeuvre the data collection and analyse the collected data as shown in Figure 1.



 RFID tag will be attached to the laptop and RFID reader will be connected to the server. The reader then scans the tag at every two seconds. If an unauthorized user removes the laptop out of the reader maximum possible area, the reader cannot detect the tag signal as a result alarm system will be triggered. Once the laptop moves back within maximum possible range of reader, the alarm system will be terminated. Thus, if someone tries to remove the laptop, the alarm sound will be activated, making owner aware. To improve the system, GSM terminal is used to send short massage to the laptop owner that the laptop had been stolen by unauthorized person. Typically GSM terminal consist of connector to external terminal equipment, and the Subscriber Identity Module (SIM) cardholder. The GSM terminal equipment is standing alone mobile equipment that is capable to handle SMS sending and receiving function. In this system, only SMS sending behaviour is adapted. The Short massage Inter-Working Mobile Switching Centre (MSC) passes the message to a Short Message Service Centre (SMSC). The SMSC then forwards the message to the destination GSM network through a specific GSM MSC called the SMS gateway MSC (SMS GMSC). Following the GSM roaming protocol, the SMS GMSC determines the serving MSC of the message receiver based on the information received from the Home Location Register (HLR) and forwards the message to that MSC.

 A flow chart showing the laptop security system model is shown in Figure 2. Firstly, an alarm system is programmed in a graphical user interface using C# programming language. This program is used to control the RFID reader, RFID tag and the GSM terminal. In normal practice, the reader is put in shutdown mode to save energy, and therefore it has to be reconfigured each time it is started before it can read tags. All the information read from the tag will be transmitted to the server in a RF link and shown in a GUI. Once the laptop is moved out of a certain distance from the server base station, the alarm system will be activated. An alarm sound is played to draw attention to the attempted laptop theft. At the same time, an alert message is sent to the laptop owner to awake them that their laptop had been stole.



**Conclusion**

 This paper has demonstrated the integrated design of the laptop security system with RFID technology and current mobility technology of SMS messaging to form the theft prevention using WSS. Basically, the RFID reader is functioning as a base station and connected to the server via serial communication port. Meanwhile, the program is can collect data from the reader and perform analysis. This paper has shown that with the proper implementation of such RFID and GSM technologies such that the laptop security is being good for long runs. The consumers need not worry about their laptop at anytime and anywhere. Besides, this idea also can implement to other valuable belongings such as laboratory equipment. What they need to do is just simply attached to the RFID tag to their belongings and run the security program. This system can also be enhanced by using Bluetooth wireless communications technology since the implementation of embedded Bluetooth devices is much easier and cheaper. \

**References**

 [1] J. Westhues. Hacking the prox card. In S. Garfinkel and B. Rosenberg, "RFID: Applications, Security, and Privacy”, pg. no. 291–300. Addison-Wesley, 2005.

[2] Muhammad Naveed, Wasim Habib, Usman Masud, Ubaid Ullah, and Gulzar Ahmad, "Reliable andLow Cost RFID Based Authentication System for Large Scale Deployment”, International Journal of Network Security, Vol.14, No.3, PP. 173{179, May 2012.

[3] S. I. Ahamed, F. Rahman, and E. Hoque, “ERAP:ECC based RFID authentication protocol," 12thIEEE International Workshop on Future Trends of Distributed Computing Systems, pp. 219-225, 2008.

[4] Huang, H., Xiao, S., Meng , X., and Xiong, Y., "A Remote Home Security System Based on Wireless Sensor Network and GSM Technology", Proceedings of Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.

[5] E. Syta, S. Kurkovsky, and B. Casano, “RFID-based authentication middleware for mobile devices", Hawaii International Conference on System Sciences, pp. 1-10, 2010.

[6] K. Wu, E. Bai, and W. Zhang, “A hash-based authentication protocol for secure mobile RFID systems," First International Conference on Information Science and Engineering, pp. 2440-2443, 2009.