A RFID Based Security Enhancement System for Military Application

S. Karthikeyan[1] P. Manoj Kumar[2] U. Pavithran[3] E. Balaji[4]
[1,2,3,4]Department of Electronics and Communication Engineering
[1,2,3,4]Velammal Institute of Technology, Panchetti, Thiruvallur District, Chennai

Abstract— The government of India felt the necessity of specialist border guard¬ing forces to man the country's International Border & LOC with Pakistan and Bangladesh (after 1971), China & Nepal, which were previously protected by various state armed police forces earlier. Their role during the peace time is to secure the borders, guarding the local population in the border areas, and prevent trans-border crimes, unauthorized entries/exits from India, besides smugg-ling and illegal activities. Each Indian soldier is having unique RFID which is to be inserted in the body. When foreign body with unspecified ID or without ID crosses the border, they are been tracked by RFID Reader. In addition, GPS location tracker is been attached with the module. This GPS tracker tracks the exact location of the unauthorized invaders. This information's are sent to the registered phone numbers of military officials, which involves addition of GSM in the module, thereby protecting our country from enemies attack.

Key words: GPS, GSM module, RFID reader and PIR sensor

I. INTRODUCTION

The government of India felt the necessity of specialist border guard¬ing forces to man the country's International Border & LOC with Pakistan and Bangladesh (after 1971), China & Nepal, which were previously protected by various state armed police forces earlier. Their role during the peace time is to secure the borders, guarding the local population in the border areas, and prevent trans-border crimes, unauthorized entries/exits from India, besides smugg-ling and illegal activities. The border guarding forces, while facing Pakistan, Nepal, Bangladesh and China have to be provided with best of armaments and support systems to keep soldiers fit for all times, in all weathers in the field and to operate, in the latest tactical environment to face the fire of Pakistan. Their role during the peace time is to secure the borders, guarding the local population in the border areas, and prevent trans-border crimes, unauthorized entries/exits from India, besides smugg¬ling and illegal activities. This project helps Indian soldiers to protect our country. In this project, each Indian soldier is having unique RFID which is to be inserted in the body. When foreign body with unspecified ID or without ID crosses the border, they are been tracked by RFID Reader. In addition, GPS location tracker is been attached with the module. This GPS tracker tracks the exact location of the unauthorized invaders. This information's are sent to the registered phone numbers of military officials, which involves addition of GSM in the module, thereby protecting our country from enemies attack.

II. EXISTING SYSTEM

- In the past decade, the terrorist are easily penetrate in to ours site and making the trouble unfortunately.
- Due to this many soldiers are gets dying, injuring and weapons and materials are impacting.

A. Drawbacks

- Materials are damaging and country environment is occurred in impact.
- There is no automatic system to track the terrorist.
- The insecurity occurring for living peoples in the valley area.

III. PROPOSED SYSTEM

- Here the system will give intimation message to each soldiers
- The system will update the information about the penetrating of enemies inside our area.
- This system uses unique RFID tag. So duplicate tags will be found easily.
- The intimation message will send to all registered mobile numbers.

A. Advantages

- It is an automatic system.
- It intimates quietly to ours soldiers about entering of enemies.
- Low cost and Easy to implement.
- This system uses Arduino Uno. It has reduced instruction sets. So that the speed of the process is high.
- This system needs only basic model phones like nokia1100.

IV. FUNCTIONAL BLOCK DIAGRAM

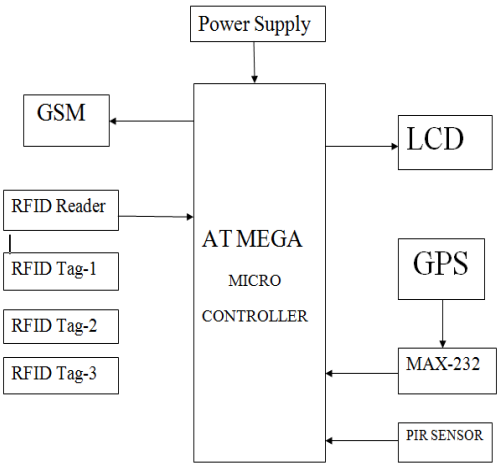

Fig. 1: Functional Block Diagram

V. WORKING

The working of the blocks in this proposed model is explained below.

A. Power Supply Unit

All digital circuits require regulated power supply.

1) Step down Transformer: Step down transformer is used to reduce the voltage according to the required voltage of the circuit. Most of the circuit needs 5V to 12V only.
2) Bridge Rectifier: The output from the transformer is in AC, but the supply for circuit in DC. So it needs to rectify the AC output to DC output. So the diodes are used to build a Bridge rectifier circuit to convert the 12VAC to 12VDC. A smoothing capacitor can be used at the output side of the rectifier to get a constant voltage. Bridge Rectifier consists of four diodes namely D1, D2, D3 and D4. During the positive half cycle diodes D1 & D4 conduct whereas in the negative half cycle diodes D2 & D3 conduct.

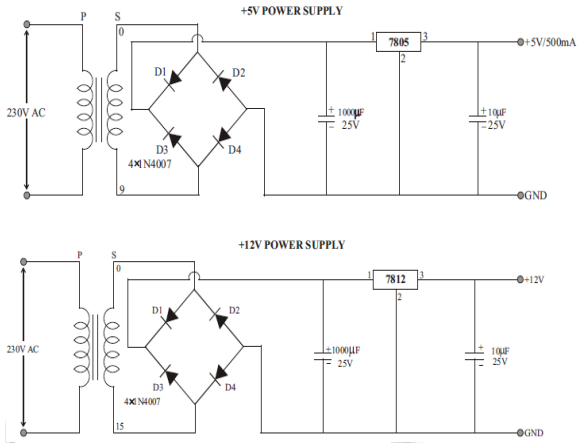

Fig. 2: Power Supply Unit

3) Voltage Regulator 7805: The output DC voltage now available is 12V but it has to be converted into 5V since the transistor base voltage should be in the range of 5V-6V. Voltage regulators are used in the circuits to provide a constant required voltage and to avoid major fluctuations in the voltage to the circuit. It has 3 pins. The input pin, ground pin and output pin. The input voltage must be within the range of 5V to 30V. So the voltage regulator regulates the voltage to 5V.

B. Passive Infrared

PIR sensors allow you to sense motion, almost always used to detect whether a human has moved in or out of the sensors range. They are small, inexpensive, low-power, easy to use and don't wear out. For that reason they are commonly found in appliances and gadgets used in homes or businesses. Whenever the human or animal is crossing border, PIR sensor sense and will find whether it's human or animal. If it is human, the reflected radiation will be high. If it is not human, the radiation will be low. The radiation is based on the temperature. Human having high temperature than animals. If it is human, PIR sensor sends the data to RFID reader.

Fig. 3: PIR Module

C. Radio Frequency Identification

The reader transmits radio frequency when powered ON. When the tag is placed near the reader, the RFID tag will receive the radio frequency via the antenna inside tag. The radio frequency received will be converted into electrical power that is enough for the tag to transmit the data back to the RFID reader. Further, the reader will transmit the tag ID to the external device by serial communication. Then RFID reader sends the radio frequency signal to find whether the entered person is our soldier or not. If the person having RFID tag, it checks whether RFID tag is matched or not. After that, RFID reader sends the signal to the microcontroller (ATMega162v) about penetration of human in the border. Even though the person do not having RFID tag, the RFID reader will send the signal to the microcontroller.

Fig. 4: RFID Reader Module

D. Microcontroller

The AVR core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers. The device is manufactured using Atmel's high density non-volatile memory technology. microcontroller gets the exact location of the person who already entered in our country using GPS. GPS is mainly used for navigation and finding exact location (latitude and longitude). After that, microcontroller intimates the GSM to send message about penetration of human to the registered phone numbers. This message helps to Indian soldiers to attack them if they are enemies.

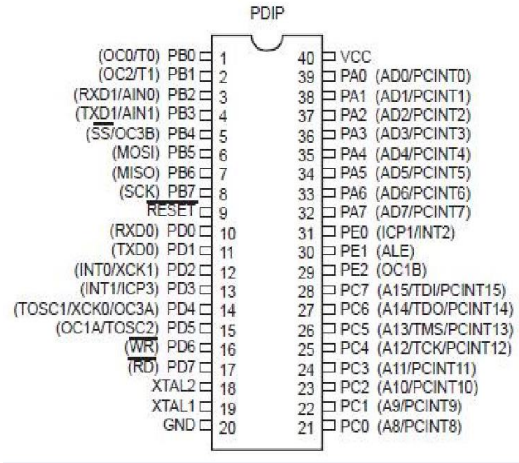

Fig. 5: Pin Diagram

E. GSM Module

GSM (Global System for Mobile Communications: originally from Group Special Mobile) is the most popular standard for mobile telephony systems in the world. The GSM Association, its promoting industry trade organization of mobile phone carriers and manufacturers, estimates that 80% of the global mobile market uses the standard Its ubiquity enables international roaming arrangements between mobile network operators, providing subscribers the use of their phones in many parts of the world. GSM differs from its predecessor technologies in that both signaling and speech channels are digital, and thus GSM is considered a second generation (2G) mobile phone system.

Fig. 6: GSM Module

F. GPS Module

The Global Positioning System (GPS) is a satellite-based navigation system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defense. GPS was originally intended for military applications, but in the 1980s, the government made the system available for civilian use. GPS works in any weather conditions, anywhere in the world, 24 hours a day. There are no subscription fees or setup charges to use GPS.

Fig. 7: GPS Module

G. LCD

Liquid crystal displays (LCDs) have materials which combine the properties of both liquids and crystals. Rather than having a melting point, they have a temperature range within which the molecules are almost as mobile as they would be in a liquid, but are grouped together in an ordered form similar to a crystal. An LCD consists of two glass panels, with the liquid crystal material sand witched in between them.

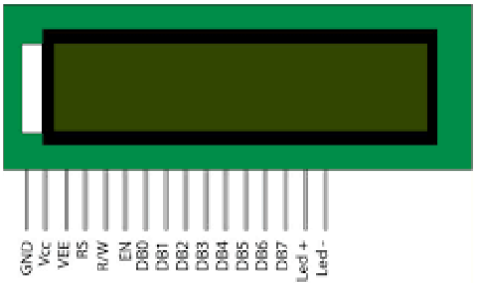

Fig. 7: LCD

VI. EXPERIMENTAL RESULTS

Fig. 8: Case 1: Authorized Person Entered

Fig. 9: Case 2: Enemy Entered

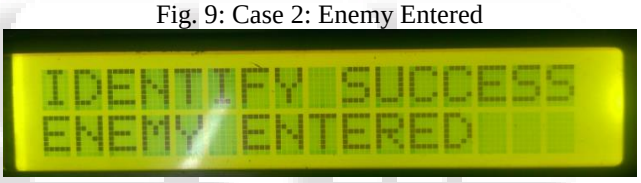

Fig. 10: Case 3: Unauthorized Person Entered

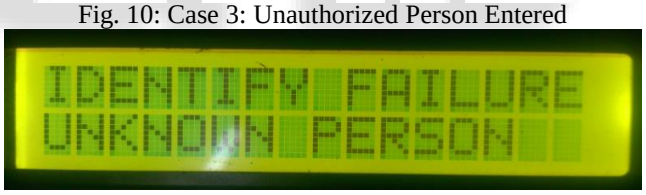

Fig. 11:

Fig. 12:

VII. CONCLUSION

This security system has been proposed. Based on this system, the cost and the security accuracy were improved. The proposed system successfully sends the intimation message to the registered mobile numbers. This intimation message gives the information about the penetration of person and exact location of the person. If the entered person is an enemy or enemies, this system helps our soldiers to attack them and protecting our country.

REFERENCES

[1] E. Chin, A. P. Felt, K. Greenwood, D. Wagner, Analyzing Inter- Application Communication in

Android, in: Proceedings of the 9th international conference on Mobile systems, applications, and services, MobiSys '11, ACM, New York, NY,USA, 2011, pp. 239–252. doi:10.1145/1999995.2000018. URL http://doi.acm.org/10.1145/1999995.2000018

[2] V. Rastogi, Y. Chen, X. Jiang, Droidchameleon: Evaluating Android anti-malware against Transformation attacks, in: Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ACM, 2013, pp. 329–334.

[3] P. Faruki, V. Ganmoor, V. Laxmi, M. S. Gaur, A. Bharmal, An- droSimilar: Robust Statistical Feature Signature for Android Malware Detection., in: A. Eli, M. S. Gaur, M. A. Orgun, O. B. Makarevich (Eds.), SIN, ACM, 2013, pp. 152–159. URL http://dblp.uni-trier.de/db/conf/sin/sin2013.html#FarukiGLGB13

[4] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, I. Molloy, Android Permissions: a perspective combining risks and benefits, in: Proceedings of the 17th ACM symposium on Access Control Models and Technologies, ACM, 2012, pp. 13–22.

