A Mobile Community Service Based On Near Field Communication

N. Akshaya[1], R. Indhu[2], R. Ishwarya[3], R. M. Radha Lakshmi[4], P. Nalayini[5]

[1,2,3,4]Student Members, Department of Computer Science and Engineering

[5]Staff Member, Department of Computer Science and Engineering

Kings College of Engineering, Thanjavur, Tamil Nadu.

Abstract *- In the Internet of Things vision, a network of physical devices that are embedded with electronics, software, sensors and connectivity that enable greater functions and services through the exchange of data skilled through interconnection. The control and protection of user data is a very important aspect in the design and deployment of the Internet of Things (IoT). One of the issues is a lack of an established mechanism that deals with the issue of conviction and aloofness. An analogous framework for multilevel conviction and aloofness does not exist for IoT. IoT is susceptible to various contraption issues and has some major privacy concerns for the end users.We come up with the conviction between devices taking into account the nature, complexity and category of the interconnected devices. Our structure is applied to a Smart Military scenario in order to exhibit a hardware embedding intelligence into machines in the defense applications.*

Keyword - Internet of Things (IOT), Conviction, Armor, Aloofness, Near Field Communication.

I. INTRODUCTION

Near Field Communication (NFC) is an emerging wireless short-range communication technology that is based on existing standards of the Radio Frequency Identification (RFID) infrastructure. In combination with NFC-capable smart phones it enables intuitive application scenarios for contactless transactions, in particular

services for mobile payment and over-the air ticketing. The intention of this project is to describe basic characteristics and benefits of the under laying technology, to classify modes of operation and to present various use cases. Both existing NFC applications and possible future scenarios will be analyzed in this context. The control and protection of user data is a very important aspect in the design and deployment of the Internet of Things (IoT). The heterogeneity of IoT technologies, the large number of devices and systems, and the different types of users and roles create important challenges in this context. In particular, requirements of scalability, interoperability, trust and privacy are difficult to address even with the considerable amount of existing work in the research and standardization community.

I. RELATED WORK

A Technical point of view, the Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities are Communication and Cooperation, Identification, Sensing, User Interfaces etc,. Our focus in this paper is on the support provided by our project for the specification and enforcement of usage control policy rules that are Integration in to systems of security technologies, e.g., advanced encryption and access control, and intelligent data aggregation techniques. Our project supports integrated modeling of the IoT system design and runtime view points to support integrated specification of security requirements, risk management, and usage control policy specification. From the remote identification of objects and an Internet “with” things, we are moving towards a system where (more or less) smart objects actually communicate with users, Internet services and even among each other. Important are wireless communications standards such as IEEE 802.15.4 that cover the layers below IP and consume relatively little power – ZigBee implementations require approximately 20 to 60 mW (for 1 mW transmission power, a range of 10 to 100

meters and a data transmission rate of 250 kbit/s). More recent Wireless Personal Area Network (WPAN) standards such as ZigBee and others still under develop- ment may have a narrower bandwidth, but they do use significantly less power. Our usage control framework also includes authentication and tamper detection using trusted computing technology. We are not aware of other frameworks that provide equivalent expressiveness, are efficient for runtime monitoring, and are integrated with trusted computing technology.

II. PROPOSED SYSTEM

A miniature based armor with multilevel conviction and aloofness for the internet of things is organized as follows to handle security aspects of the IoT systems. We tend to propose during this paper a miniature primarily based armor with structure conviction and aloofness .This research supports integrated modeling of the IoT systems style and run time read points to support integrated specification of security necessities, risk management, and usage management policy specification. This research integrates and revealed approaches for policy refinement, policy social control technology at completely different levels of abstraction with sturdy guarantees, policy specification, and identity management with trust negotiation. Describes the IoT framework we tend to adopt and extend during this paper. Details the safety style support, runtime design, and social control elements enforced during this project. In our extended IoT framework is applied in smart military case study with an illustration of the liability to handle the dynamic security aspects of this situation together with performance analysis result implementation. Finally, presents the conclusions and future developments.

A. Advantages

We propose a conviction management scheme and aloofness, Represents the category information about the provider of the information. Improved smart military case study was proposed and detailed security architecture with conviction management and types of attacks representation.

B. Accurate Data

Data from the sensor nodes shows the stable readings.

Low cost : Implementation cost is low.

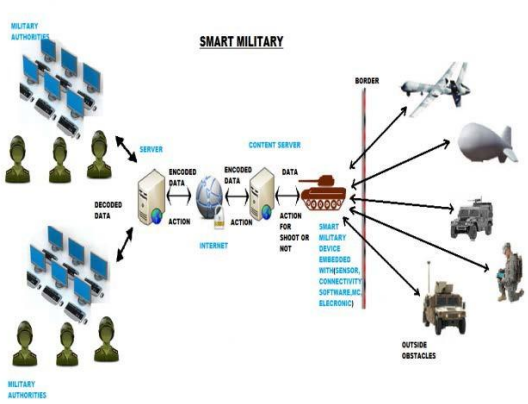


Fig 1: Implementation Method

C. Block Diagram

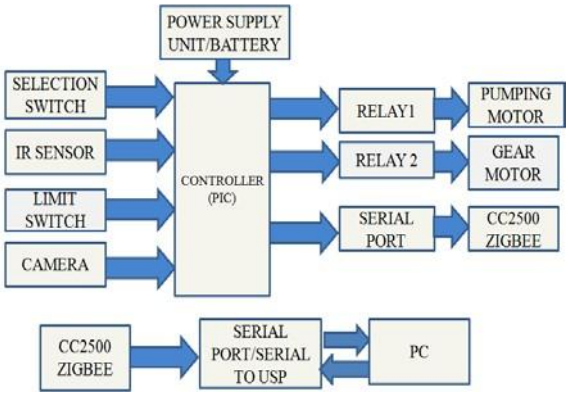


Fig.2 Architectural Framework of Proposed System
PIC MICROCONTROLLER

D. Programmable Interface Controller

It is a electronic circuits that can be programmed to carry out a vast range of tasks. They can be programmed to be timers or to control a production line and much more, This is used to connect computer to the microcontroller circuits

1) ***Reprogrammable controller***: The PIC16F877A has 8kb flash memory which can be used to erase and rewrite the programs for the controller. Hence the devices can be re- programmed up to 100,000 times,

2) Low power consumption: The controller works with a low power supply such as 5V DC.

3) Easy programming, cheap and reliable: It is easy to program the PIC microcontroller in embedded C language or assembly level language.

4) Inbuilt ADC: The single 10 bit Analog to Digital Converter can have up to 8 inputs for a device

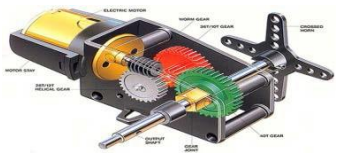
multiplexed from input pins. The Port A is dedicated for this function. The ADC can be used during sleep but you have to use the RC clock mode. One benefit of this is that there will be no digital switching noise so you will get better conversion accuracy.

5) infrared sensor : An infrared sensor is an electronic device that emits and/or detects infrared radiation in order to sense some aspect of its surroundings. Infrared sensors can measure the heat of an object, as well as detect motion. Infrared waves are invisible to human eyes. The wavelength region of 0.75μm to 3 μm is called near infrared, the region from 3 μm to 6 μm is called mid infrared and the region higher than 6 μm is called far infrared**.**

6) Zigbee : ZigBee is a low-cost, low-power, wireless mesh network standard targeted at the wide development of long battery life devices in wireless control and monitoring applications

7) Servo motor: A **servomotor** is a rotary actuator or linear actuator that allows for precise control of angular or linear position, velocity and acceleration.

Servo motor is a special type of motor which is automatically operated up to certain limit for a given command with help of error-sensing feedback to correct the performance. A servomotor is a rotary actuator that allows for precise control of angular position. It consists of a motor coupled to a sensor for position feedback. It also requires a servo drive to complete the system. The drive uses the feedback sensor to precisely control the rotary position of the motor.



8) Relay: A relay is an electrically operated switch. Relays are electromechanical devices that use an electromagnet to operate a pair of movable contacts from an open position to a closed position. The advantage of relays is that it takes a relatively small amount of power to operate the relay coil, but the relay itself can be used to control motors, heaters, lamps or AC circuits which themselves can draw a lot more electrical power.

9) Selection switch: A manually operated multi-position switch. Such a switch is usually adjusted by a knob or handle, and may have detents to hold in a given position. Used, for instance, in devices or instruments with multiple functions, ranges, or modes of operation. Such a switch is usually rotary. Also called selector.

10) Limit switch: A limit switch is an electromechanical device that consists of an actuator mechanically linked to a set of contacts. When an object comes into contact with the actuator, the device operates the contacts to make or break an electrical connection.

11) Camera: A device for recording visual images in the form of photographs, film, or videos

SOFTWARE REQUIREMENTS

Programming Language: asp.net, sql Languages

Algorithm : Decision making Algorithm

Decision making Algorithm

Decision making algorithm is the process of making choices by identifying a decision, gathering information and assessing alternative resolutions. Using step by step decision making process

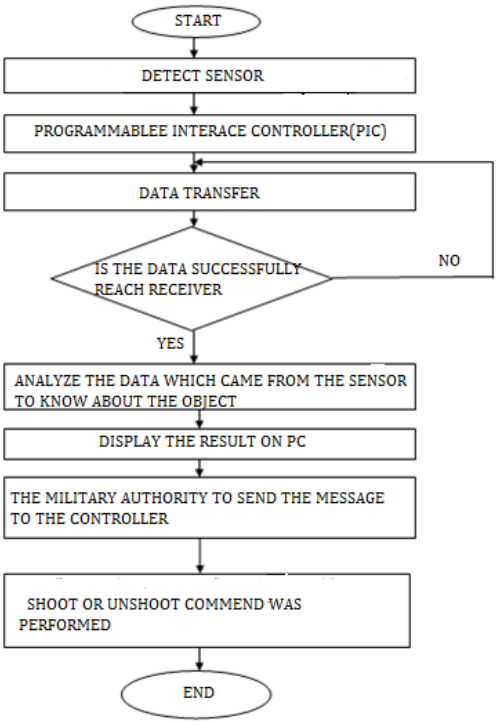


Fig: 3.Data Flow Diagram

III. CONCLUSION

The smart military device can replace men in situations when human life or health is endangered. This project has been applied to a Smart Military scenario to evaluate its feasibility and performance. Our case study shows the flexibility and efficiency of our project to support the specification and evaluation of security policies specified using rule templates. Our short term objective is to release a miniature based armor with multilevel conviction and aloofness for the internet of things especially for smart military device as an open source project to enable community driven specification of policy templates and implementation of technology.

REFERENCES

[1]. *Ahamad.M, Neiger.G, Burns.J, Kohli.P and Hutto.P, "Causal memory: definitions, implementation, and programming," Distributed Computing, vol. 9, no. 1, 1995.*

[2]. *Anderson.E, Li.X, Shah.M, Tucek.J and Wylie.J, "What consistency does your key-value store actually provide," in Proc. 2010 USENIX HotDep.*

[3]. *Armbrust.M, Fox.A, Griffith.A, Joseph. A Katz.R, onwinski.A, Lee.G, Patterson.D, Rabkin.A, Stoica.I, "A view of cloud computing," Commun. ACM, vol.53, no. 4, 2010.*

[4]. *Brewer.E, "Towards robust distributed systems," in Proc. 2000 ACM PODC.*

[5]. *Fidge.C, "Timestamps in message-passing systems that preserve the partial ordering," in Proc. 1988 ACSC. [6]Golab.W, Li.X and Shah.M, "Analyzing consistency properties for fun and profit," in Proc. 2011 ACM PODC.*

[6]. *G. Baldini, I. Kounelis, I. N. Fovino, and R. Neisse, "A framework for privacy protection and usage control of personal data in a smart city scenario," Critical Information Infrastructures Security, vol. 8328, pp. 212– 217, 2013.*

[7]. *F. Schafrik, "A practical guide to developing enterprise architecture," Available at : http://www.ibm.com/developerworks/rational/library/enterprise architecture maximum-value/, 2011.*