International Journal on Applications in Engineering and Technology
Volume 2: Issue 8: August 2016, pp 20 - 22. www.aetsjournal.com ISSN (Online) : 2455 - 0523

A Survey on Implementing Internet of Things Using Banker's Algorithm for Automobile Industries

S.Jeevitha , D. Satheesh Kumar , P.Ezhilarasu , M.Mansurabegam

***Abstract*—** The Internet of things (stylised Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and smart devices"), buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data**.** In this paperwe need to utilize Dynamic Service Dependency Verification has been implemented using IOT. The first process of this paper initiate with hardware interface. The hardware has been designed using 8051 microprocessor. More interactions can be done using 8051 pin interaction. In added with various sensors can be connected through the controller board interface. Multi sensors have been interacted in this hardware. The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered in product design. To improve security, an IoT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted.

***Keywords*—** Internet of Things (IoT), sensor, Dynamic Service Dependency, Internet host, Security

I. INTRODUCTION

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energy-efficiency. Other personal IoT devices like wearable fitness and health monitoring devices and network-enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost.

IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized.

In this paper, Dynamic Service Dependency Verification has been implemented using IOT. The first process of this paper initiate with hardware interface. The hardware has been designed using 8051 microprocessor. The microprocessor contains 40 pin. More interactions can be done using 8051 pin interaction. In added with various sensors can be connected through the controller board interface. Multi sensors have been interacted in this hardware. The hardware interactions are follows.

- Controlling Indicators
- Doors Open and close
- Controlling Car Engine
- Blow horn
- Headlights

All the above mentioned hardware process has been implemented in a single interface controller board. Secure Service Virtualization in IoT by Dynamic Service Dependency Verification is ensured by the hardware phase initially.The main objective of this paper is to develop a web based application to communication with an internet server in a secured manner. The uploaded information will be the data

S. Jeevitha , PG scholar, Department of Computer Science and Engineering , Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (email : jeevithaess@gmail.com)

D. Satheesh Kumar , Assistant Professor, Department of Computer Science and Engineering , Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India (email : hicetsatheesh@gmail.com)

Dr.P Ezhilarasu , Associate Professor, Department of Computer Science and Engineering , Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email : prof.p.ezhilarasu@gmail.com)

M. Mansurabegam , PG scholar, Department of Computer Science and Engineering , Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (email : mansurabegam24@gmail.com)

from a hardware resource. During the communication process the data will transferred secured. The enhancement in this paper is, upgrading wireless sensor network into a centralized server. This application will be secure channel between a sensor node and an Internet host.

II. VARIOUS METHODS IN IOT

Table 1
Methods using Internet of Things

S.no	Title	Process	Future work
1	Real-time location and inpatient care systems based on passive RFID[1]	To create standards-based secure access to patient's personal data and medical records by using RFID tags and Web Service with the help of hardware kit.	To speed up and increase reliability of involved processes
2	Adoption and Implementation of RFID technologies in healthcare[2]	This paper despite the rising implementation of RFID technology-based healthcare services, few empirical studies have been conducted to assess the potential of this technology within the healthcare sector.	Better designed RFID systems with low cost and privacy issues addressed are needed to increase acceptance of RFID in healthcare.
3	Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards[3]	To improved Yoon's protocol resolving the security and privacy problems efficiently. The improved protocol resists against replay, impersonation, DATA forgery, DoS attacks and provides forward secrecy and untraceability.	Raises the security level and conforms to the EPC Class 1 GEN-2 standards.
4	LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. Low-cost Radio Frequency Identification (RFID) tags.[4]	A real lightweight mutual authentication protocol for low-cost RFID tags that offers an adequate security level and can be implemented even in the most limited systems, as it only needs around 300 gates.	Make it suitable for very low-cost RFID tags
5	EMAP: An efficient mutual authentication protocol for low-cost RFID tags[5]	An extremely efficient lightweight mutual-authentication protocol that offers an adequate security level for certain applications and can be implemented even in the most limited low-cost RFID tags, as it only needs around 150 gates	Needed the most limited low-cost RFID tags, as it only needs around 150 gates
6	Security and privacy aspects of low-cost radio frequency identification systems.[6]	It describe privacy and security risks and how they apply to the unique setting of low-cost RFID devices.	Privacy and Security risks are analyzed
7	CONTROL INFORMATION FLOWS WITHIN THE INTERNET OF THINGS[7]	It exploring the potential of decentralised Information Flow Control (IFC), where management policy is encapsulated within tags that are attached to data (and processes). Policy is enforced at each point of flow, in accordance with these tags.	Presenting certificate-based approach for secure tagging, to enable robust, verifiable and distributed data flow policy
8	provably secure additive and multiplicative privacy homomorphism [8]	security provided by the proposed scheme is based on the fact that the subset of keys consistent with the known pairs is kept large and any two different keys yield different clear texts from the same cipher text with a high probability	Data processing is to be encrypted and provide more security.

III. CONCLUSION

In this paper we defined that all emergency warning can be done by controlling car through Internet of Things Where the sensors can be used to identify the warnings. In feature we concentrate on car crash analysis and accident recovery process by using banker's algorithm in automobile industries.

REFERENCES

[1] P. Najera, J. Lopez, and R. Roman, "Real-time location and inpatient care systems based on passive RFID ",april 2010

[2] W. Yao, C. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare" October 2011
[3] H. Chien and C. Chen., "The Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards", 2007.
[4] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. Low-cost Radio Frequency Identification (RFID) tags ",2006.
[5] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "EMAP: An efficient mutual authentication protocol for low-cost RFID tags ",February 2012.
[6] S. Weis, S. Sarma, R. Rivest, andD. Engels "Security and privacy aspects of low-cost radio frequency identification systems ", march 2010.
[7] J. Domingo-Ferrer, "provably secure additive and multiplicative privacy homomorphism",2002.
[8] L. D. Xu, W. He, and S. Li, "Internet of things in industries: a survey," IEEE T Ind Inform, vol. 10, no. 4, pp. 2233-2243, 2014.