SMART ATM: IoT Communication Model

***Madhu Sharma**

****Manoj Kumar Sharma**

*****Vijay Singh Rathore**

Abstract:

Usage of ATM is one the most widely acceptable system for monetary transactions. But, in today's scenario, the ATM cash transaction system is facing various security challenges. Duress Cash withdrawal is one of among the current physical security problems. In this paper, the Internet of Things (IoT) Communication Model of Safe Mode Alarm Reporting Technique (SMART) that has already been introduced to meet the issue and provide security mechanism for user's physical and monetary security. The Model has been presented with the details of the protocols involved at different layers of data communication. The communication network Analyzer tool viz. Cooja simulator has been used to analyze the different parameters of IoT communication system..

General Terms

Automated Teller Machine (ATM), Global Positioning System (GPS), Internet of Things (IoT).

Keywords

Safe Mode Alarm Reporting Technique (SMART), Communication Model, Component Requirement Model, Constrained Node, Unconstrained Node.

1. INTRODUCTION

Automated Teller Machine is a publicly and globally employed system to aid the smoother monetary transactional services and activities for its clientele. The ATM's physical and logical security systems are both needed to be timely updated, to meet out the challenges of robbery at ATM[1]. Various research activities are progressively aiming to develop and implement the solution systems for duress cash withdrawal cases [2]. SMART ATM has been introduced to meet the challenge of duress cash withdrawal [3]4][5][6]. Also, as per current demand and greater need of connectivity among different type of objects, the concept of Internet of Things (IoT) has emerged, embedded with the World Wide Web and mobile technologies. Also, as per societal and environmental accessibility needs and industrial applications, the data monitoring and controlling is required at any time, from any place, and by anyone. Thus, here in this paper an IoT Communication Model of SMART ATM has been introduced. Section II of the paper presents the brief introduction of the SMART ATM and Internet of Things; Section III depicts the IoT Model of the SMART ATM and Section IV presents the result and discussion relevant to system's data communication simulator and Section V concludes the discussion.

2. SMART ATM AND INTERNET OF THINGS

2.1 Safe Mode Alarm Reporting Technique (SMART) ATM

SMART ATM has been introduced to protect user from duress cash withdrawal. In SMART, firstly, the entry of PIN2 ('Pintu') by the victim in ATM, activates alarm, which would be treated as bank robbery and the amount of cash demanded and dispensed for withdrawal from ATM, would not be deducted from victims account, but from the bank itself. Since, the relevant bank itself is responsible to provide security to customers over ATM, and if it would not able to provide security, the bank would have to bear the loss because of the FOBIA. Secondly, SMART activates the GPS system by which the nearest GPS enabled police stations or PCR Vans, or Policemen with GPS enabled devices are identified and message would be sent to those nearest GPS enabled devices for help [15][16]. Security alert message would also be sent to the registered emergency numbers and bank officials for emergency situation information.

2.2 Internet of Things (IoT)

As per current demand and greater need of connectivity among different type of objects, the concept of Internet of Things has emerged, embedded with the World Wide Web and mobile technologies. Also, as per societal and environmental accessibility needs and industrial applications, the data monitoring and controlling is required at any time, from any place, and by anyone[7]. In particular, the Internet of Things (IoT) applications are capable of providing assistance in the following areas [8][9][10]:

- Data monitoring, anytime from any place, by anyone, speedily, economically and smartly.
- Easier Decision-making after gaining all the related information of the application.
- Advance Information reception and hence prevention from destructions due to catastrophic events.
- Assist in understanding the efforts required to gain the target value.
- Security of data on network.
- Helps in development of remote areas, including rural and poor areas.

IoT focuses on connectivity of Smart Things in social, environmental and user contexts, which have intelligence, unique identification or address based on standard protocol, and exhibits virtual identity.

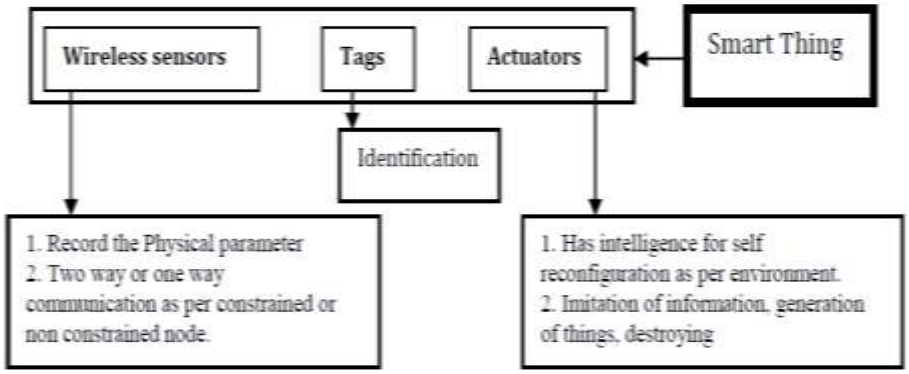

Fig 1: Conceptual Representation of Smart Things [9]

Wireless sensors consisting tags symbolize physical entities and physical entities consisting actuators, symbolize a smart physical thing. Figure 1.1 represents a smart thing. An actuator controls the parameter and can be called as an agent, which can be an artificial intelligent agent moving or stationary, or any other autonomous entity with the capability of taking decisions and setting the environment accordingly, as per the application of the environment. Sensors sink data from the environment to measure the state of an environment, whereas, the actuators source the data to the environment to set its state.

IoT Elementary Architecture:-

- It has a component arrangement based on the key functions of IoT
- Availability of object information to the user from any point and at any time
- It includes connectivity of object-to-object or object-to-internet
- Usage of Low-waist TCP/IP protocol with constrained objects

IoT Generic Architecture:-

In addition to elementary/basic architecture, the generic architecture exhibits the following:

- Unique object naming for all objects
- Heterogeneous interoperability of data, services and technologies through the provision of communication in any type of network with various protocols stacks
- Security in all types of networks as well as node's self-security
- Service discovery from the user or device side
- Device adaptability through the provision of connectivity of any object at any level.
- Provision of all data related methods like data transferring, data mining, data filtering etc. for user or object / device query

Data storage, Energy consumption and Scalability are the issues which are required to be covered in IoT architecture.

3. IoT COMMUNICATION MODEL

3.1 Component Requirement Model

Initially, the Requirement analysis has to be followed which includes the identification of the system's behavior, components, set of inputs and outputs. As per the concept of IoT and execution process sequence and the corresponding requirements, the system's components are categorized in terms of packages as:

- User Package
- Internetwork Package
- Thing Package

Package Users: User are interfaced to Things through various devices and applications like laptops, mobiles, PDAs, etc. through corresponding applications. These users including applications and devices are connected to Things through web services. Services are handled and executed by server and things, when requested by user and then by things, when required by server. Thus, there is involvement of two heterogeneous environments along with a middleware for bridging the communication among Things and Server. Middleware is an abstraction layer consisting software component, which pelts details about hardware devices or other software from an application. In SMART ATM framework, the ATM, SMART Applications (Server side, Client side), Mobile Phones, Computers, Web services, Service discovery, Event Manager, Filter Manager, Local database, Security, Power controller, Self-Awareness, Tracking tracing and controlling are the Key components of the User Package.

Package Internetwork: It consists of the combination of networks, i.e. global internetwork consisting of core and peripheral networks. Things networks are global and peripheral networks and can include heterogeneous network technologies and scenarios and so on different protocols accordingly. Each network need to fulfil their own Quality of Services (QoS) as well as applications QoS requirements. Heterogeneous, homogeneous, Centralized, distributed, mobile Network, GPS Satellite Network, Personal Area Network (Bluetooth), Server services, Central database, ONS, Death report, Server Grid, QoS Manager, Protocols, Device discovery, Event Manager, Filter Manager, Local database, Power controller, Security, Self-Awareness, Virtualization are the key components of Package Internetwork.

Package Things: Things are basically the Smart things which have the capability of reading, authenticating and then authorizing the communicating entity. Here, the things are ATM, ATM Vault (Normal & Emergency both), Alarms in PCR Vans, Alarms at Bank & Police Station and Mobile Phones.

The internetwork operates on the basis of the information and services requested and responded through servers and clients. Few of the Key IoT Component Server's utilities are depicted in table 1.

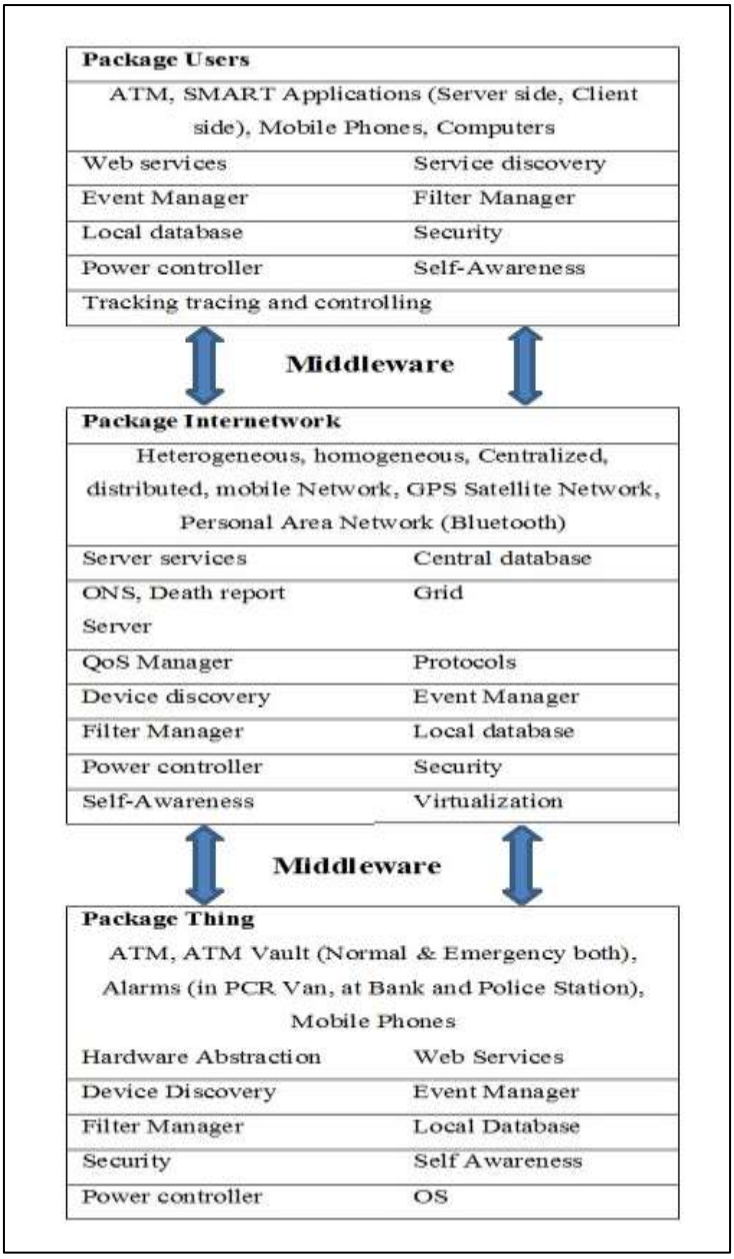

Fig 2: SMART ATM IoT components requirement block diagram

Table 1. IoT Component Servers

Server	Facility
Object Naming Server (ONS)	Provides Things identification
Death Report Server (DRS)	Provides information of Things after their death
Other Servers	Provides Routines services like backup, emails, prints etc.

3.2 Nodes and Protocol Stack

The different entities of SMART ATM are categorized as peripheral and Core Nodes. Peripheral Nodes are constrained nodes and core nodes are unconstrained nodes. Constrained nodes have limited resources in terms of memory, processing, power, size etc. like sensors, mobile phones etc. whereas, the Un-constrained nodes are usual systems like desktop computers, laptops etc.

The constrained and un-constrained nodes identified for SMART ATM are as follows:

Table 2. SMART ATM Nodes

Constrained Nodes Peripheral Nodes	Un-constrained Nodes Core Nodes
ATM Normal Vault (NV) Controller-Fixed sensor node	ATM, Vault Controller (VC)
ATM Emergency Vault (EV) Controller -Fixed sensor node	SMART Server (SS)
Alarms in PCR Van_1...$PCRVan_n$ – Moving sensor nodes (PCRAN)	GPS Server (GPSS)
Alarms at Bank & Police Station - Fixed sensor nodes (FAN)	Bank Server (BaS)
Bank & Security Officials Mobile Phones Mob1...Mobn - Moving sensor nodes (MN)	Base Station (BS)
SMART Note Chip (SN)	Computer Systems (CS)

With the difference in resources the constrained and un-constrained resources require different protocol stack. The protocol stack identified for SMART ATM constrained and un-constrained Nodes are as follows:

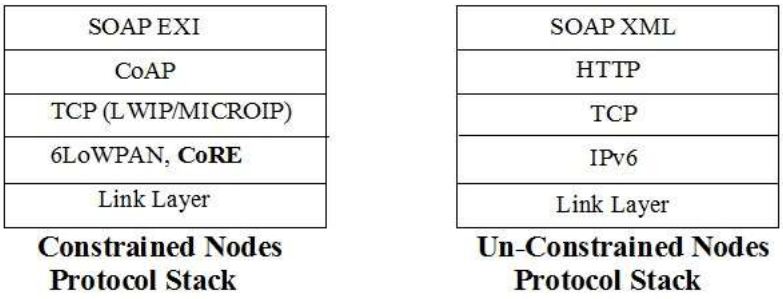

Fig 3: Unconstrained (core) and constrained node protocol stack

4. RESULT AND DISCUSSION

For system's data communication simulation, Cooja simulator has been used. Cooja is an open source network simulator for Contiki operating system, to simulate the Internet of Things (IoT) scenario consisting of sensor nodes, termed as motes[11][12][13]. Here, the IoT scenario consisting various differently located devices viz. ATM, Server, Mobile phones carried by officials in PCR Vans, Bank's Server, Bank's officials mobile phone, Security officials mobile phones and physical alarm at Bank, PCR vans, Police station and SMART note, all are represented through motes in Cooja environment. All motes of the system are assigned unique IP address and are simulated to work in an IPV4 or IPV6 based

Wireless network [14]. The study, observation and analysis process relevant to the packet delay and packet loss with specific communication protocol at all connected motes in Cooja Environment is expected to further strengthen the concept and design process of the system.

5. CONCLUSION

Internet of Things accommodates wide ranging application in today's world. Every object having being recognized by a unique IP address facilitates a global accessibility approach. The sketch of SMART ATM's IoT Communication Model and protocol stack provides a vision of real world applicability of the proposed Model. Also, the performance analysis of the IoT scenario is done for the strengthening of the proposed model. Research on various security mechanisms has been implemented, but, still there is need of more work for providing solution to the problems like duress cash withdrawals.

Research Scholar, Suresh Gyan Vihar University, Jaipur

**Professor, Suresh Gyan Vihar University, Jaipur*

***Director and Professor, Sri Karni College, Jaipur*

6. REFERENCES

[1] Rao, K. S. (2015), Automated Teller Machines Usage in India: Emerging Challenges. Sumedha Journal of Management, 4(1), 31.

[2] Tim Prenzler (2011), Strike Force Piccadilly and ATM Security: A Follow-up Study", Oxford Journals, 5(3), 236-247.

[3] Sharma M. (2015), Imminent Gadgets and Methods for an Effective SMART ATM, Proceedings of 4th National Conference by St. Xavier's College pp. 45-49.

[4] Sharma M., Rathore V.S. (2014), A review on security and reporting mechanisms for coerced cash withdrawal from ATM, International Journal of Enhanced Research in Science Technology & Engineering,, (5), 422-425 .

[5] Sharma M., et. al. (2014), An Investigative study on Physical Security and Reporting Mechanism in ATM, Proceedings of BICON-14 on New Horizons of Information Technology by using Engineering and Mathematical Approaches, 133-137.

[6] Sharma, M., & Rathore, V. S. (2014). A Framework for Safe Mode Alarm Reporting Technique (SMART) in ATMs. International Journal of Computer Applications, 96(1).

[7] Buede, D. M., & Miller, W. D. (2016). The engineering design of systems: models and methods. John Wiley & Sons.

[8] Atzori, L., Iera, A., & Morabito, G. (2014). From" smart objects" to" social objects": The next evolutionary step of the internet of things. IEEE Communications Magazine, 52(1), 97-105.

[9] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[10] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), 22-32.

[11] Maurya, M., & Shukla, S. R. (2013). Current wireless sensor nodes (Motes): Performance metrics and Constraints. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 2(1).

[12] Nasseri, M., Al-Olimat, H., Alam, M., Kim, J., Green, R., & Cheng, W. (2015, April). Contiki cooja simulation for time bounded localization in wireless sensor network. In Proceedings of the 18th Symposium on Communications & Networking (pp. 1-7). Society for Computer Simulation International.

[13] Shahra, E. Q., Sheltami, T. R., & Shakshuki, E. M. (2017). A Comparative Study of Range-Free and Range-Based Localization Protocols for Wireless Sensor Network: Using COOJA Simulator. International Journal of Distributed Systems and Technologies (IJDST), 8(1), 1-16.

[14] Léone, R., Leguay, J., Medagliani, P., & Chaudet, C. (2015, February). Demo Abstract: Automating WSN experiments and simulations. In EWSN 2015.

[15] Nate, M. S. S., Navele, M. P. S., Mote, M. V. B., & Naik, L. S. (2016). SMART REMINDER APPLICATION WITH GPS SYSTEM.

[16] Vatansever, S., & Butun, I. (2017, January). A broad overview of GPS fundamentals: Now and future. In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual (pp. 1-6). IEEE.