Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

TO DESIGN A SECURED FRAMEWORK FOR HEALTH CARE USING SECURITY AND INTERNET OF THINGS TECHNOLOGIES

Dr.Karthik Pai B.H.[1] ,Dr.Anand R[2]

[1] *Professor & HOD, Department of ISE, NMAMIT, Nitte, Karkala - 574110*
[2] *Assistant Professor (III), Department of ISE, NMAMIT, Nitte, Karkala – 574110*

ABSTRACT - *Now a day's everywhere you heard the buzz words " IoT", "Cyber Security" and "Health Issues". Everybody is talking about these technologies for the past 5 years. From our day to day life to almost all the software organizations started the projects using IoT and Cyber Security Using Health Care. The purpose of this paper is to give some basic ideas and technologies about IoT, Cyber Security and E Health. IoT is defined as "create a universal environment in which computers understand the world without human intervention." IoT was simply the tool that would be used to merge the worlds of bits and atoms. The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data. Embedding computing power throughout our physical environment has given rise to cyber-physical systems (CPS) that effectively connect the physical and cyber worlds. CPS can be described as "smart systems that encompass computational (i.e., hardware and software) and physical components, seamlessly integrated and closely interacting to sense the changing state of the real world". Related to cyber security we are going to discuss about intrusion detection and prevention mechanisms using Internet of Things. Providing security is of paramount importance for IoT technology. In this paper, initially we deal with cyber security with IoT Devices, next we describe health care with IoT Technologies and finally we can integrate secured health care with IoT.*

Keywords : *Sensors, Devices, Security, E-Health, Protocols*

I INTRODUCTION

The Internet of Things (IoT) is an emerging paradigm that will change the way we interact with objects and computers in the future. It envisions a global network of devices interacting with each other, over the Internet, to perform a useful action. As such, quite a number of useful and beneficial applications of this technology have been proposed. In this paper we will identify the security issues for IoT technology as well as highlight what approaches we can propose to resolve them. This will allow us to see the state of this technology along with what still needs to be done in the future. A lot of research has been performed regarding security for IoT environments. The biggest challenge in developing a secure system for IoT is due to the constrained nature of IoT devices. Given the limited memory, energy, bandwidth and processing capabilities of IoT devices, they are unable to directly implement current existing security mechanisms used on the Internet. For example, the general method of ensuring the confidentiality of information is through the use of cryptography but most cryptographic mechanisms require a significant amount of resources in terms of processing power and energy. This is quite a challenging issue to overcome and has received a lot of attention in the software industries and academic community. Fig.1 represents how the machine to machine connections rapidly increases every year from 2013 to 2022. Study says that in the year 2022, 20 billions of devices connected and communicated to each other as well. To achieve cyber security in IoT is to successfully protect your organization's electronic network and data against unauthorized use. You begin this process by determining what constitutes authorized use. First, you need to define who can interact with what, and how, typically using next-generation firewalls with granular access control policies. Second, is to ensure the integrity of those approved interactions and make sure that they're not corrupted by hidden threats, which is no simple task. This is why you need more than a single technology to achieve cyber security. You should identify the intruders and attackers and prevent it using incident response system.

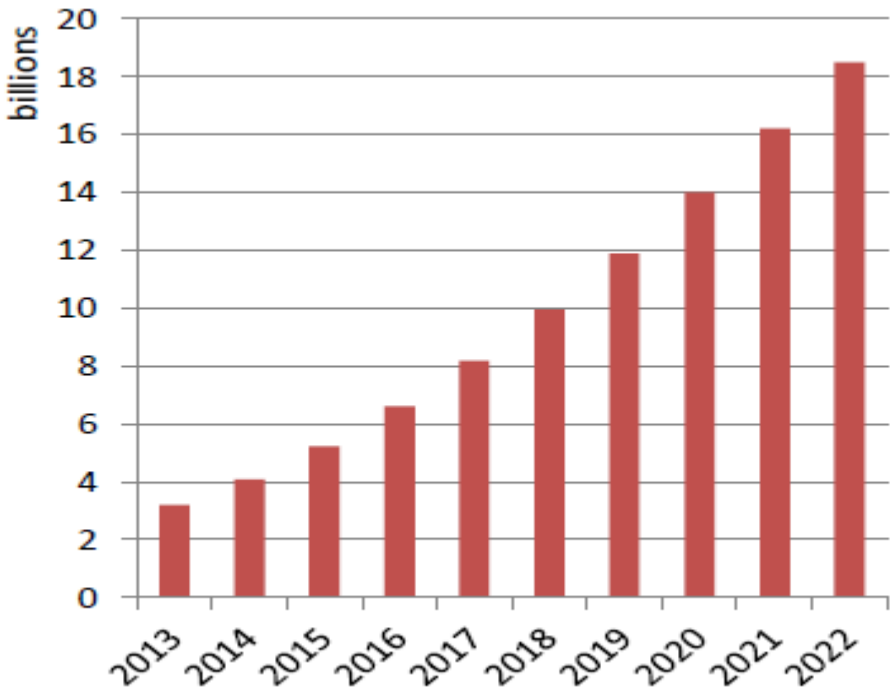

Fig.1 Machine to Machine Connections Courtesy: Machina Research

Health care technology has great potential to increase healthcare quality, expand access to services, reduce costs, and improve personal wellness and public health. However, E-Health also raises significant privacy and security challenges. With the advent of miniaturized sensors, low-power body-area wireless networks, and pervasive smart phones, the burgeoning field of mobile health (mHealth) technology has attracted tremendous commercial activity, consumer interest, and adoption by major healthcare providers.

II SECURITY IN INTERNET OF THINGS

The main purpose of this paper is to describe how we can implement security to devices using various protocols like HTTP and HTTPS. In this paper security is defined as the protection of data from unauthorized interference or monitoring by ensuring confidentiality, integrity, and authenticity of data. Confidentiality of data is defined as the protection of data from disclosure to unauthorised persons, parties or systems. Integrity is defined as the preventions of falsification or modification of data by unauthorized persons. Authenticity refers to the verification of the identity of a device or system. Intrusions refer to the network attacks against vulnerable services, data-driven attacks on applications, host-based attacks like privilege escalation, unauthorized logins and access to sensitive files, or malware like viruses, worms and trojan horses. These actions attempt to compromise the integrity, confidentiality or availability of a resource. Intrusions result in services being denied, system failing to respond or data stolen or being lost. Intrusion detection means detecting unauthorized use of a system or attacks on a system or network. Intrusion Detection Systems are implemented in software or hardware in order to detect these activities. The existing network security solutions, including firewalls, were not designed to handle network and application layer attacks such as Denial of Service and Distributed Denial of Service attacks, worms, viruses, and Trojans. Along with the drastic growth of the Internet, the high prevalence of the threats over the Internet has been the reason for the security personnel to think of IDSs. The unauthorized activities on the Internet are not only by the external attackers but also by internal sources, such as fraudulent employees or people abusing their privileges for personal gain or revenge. These internal activities cannot be prevented by a firewall which usually stops the external traffic from entering the internal network. Firewalls are made to stop unnecessary network traffic into or out of any network. Packet filtering firewalls typically will scan a packet for layer 3 and layer 4 protocol information. There are not very much dynamic defensive abilities to most firewalls. The traffic approaching the firewall either matches up to applied rule and is allowed through or the traffic is

stopped and the firewall logs the blocked traffic. IDSs can be categorized into two classes, anomaly based IDSs and misuse based IDSs. Anomaly based IDSs look for deviations from normal usage behavior to identify abnormal behavior. Misuse based, on the other hand, recognize patterns of attack. Anomaly detection techniques rely on models of the normal behavior of a computer system. These models may focus on the users, the applications, or the network. Behavior profiles are built by performing statistical analysis on historical data, or by using rule based approaches to specify behavior patterns. A basic assumption of anomaly detection is that attacks differ from normal behavior in type and amount. By defining what's normal, any violation can be identified, whether it is part of threat model or not. However, the advantage of detecting previously unknown attacks is paid for in terms of high false-positive rates in anomaly detection systems. It is also difficult to train an anomaly detection system in highly dynamic environments. The anomaly detection systems are intrinsically complex and also there is some difficulty in determining which specific event triggered the alarms. On the other hand, misuse detection systems essentially contain attack descriptions or signatures and match them against the audit data stream, looking for evidence of known attacks. The main advantage of misuse detection systems is that they focus analysis on the audit data and typically produce few false positives. The main disadvantage of misuse detection systems is that they can detect only known attacks for which they have a defined signature. As new attacks are discovered, developers must model and add them to the signature database. In addition, signature-based IDSs are more vulnerable to attacks aimed at triggering a high volume of detection alerts by injecting traffic that has been specifically crafted to match the signatures used in the analysis process. This type of attack can be used to exhaust the resources on the IDS computing platform and to hide attacks within the large number of alerts produced. Fig.2 represents the Common Layers for IoT Applications.

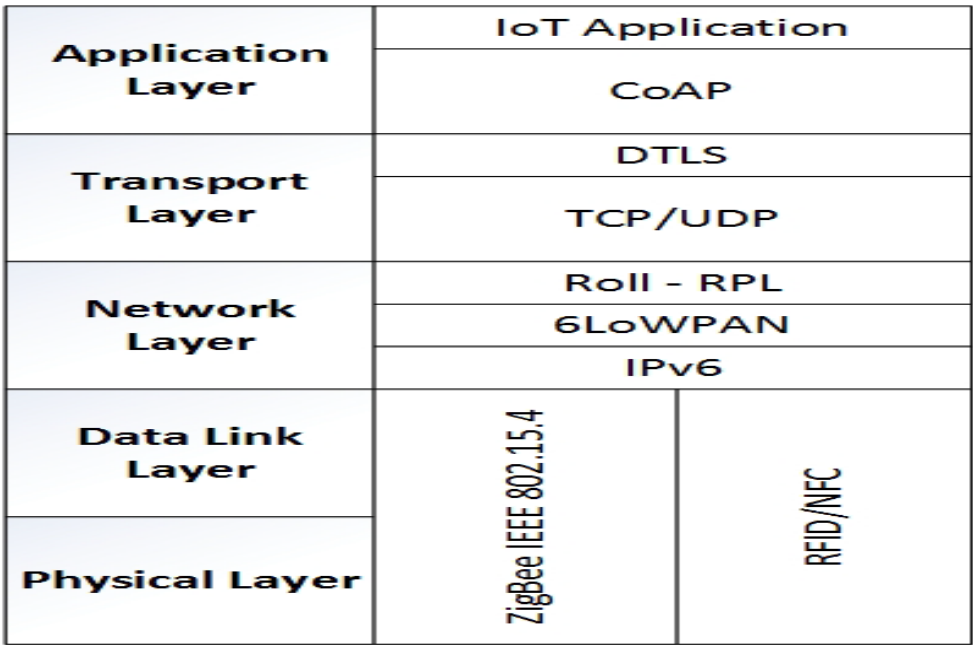

Fig. 2 Common Layers for IoT Applications

In the last two decades, a range of commercial and public domain intrusion detection systems have been developed. These systems use various approaches to detect intrusions. As a result, they show distinct preferences in detecting certain classes of attacks with improved accuracy while performing moderately for the other classes.

The main security issues in IoT is identified as :

- Authentication
- Authorization
- Confidentiality
- Integrity
- Privacy

- Anonymity
- Digital Forgetting
- Self Configuration
- Software Authenticity
- Hardware Anti-tampering
- Availability
- Key Management
- Trust Management

III CYBER SECURITY WITH IDPS SYSTEM

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

The typical components in an IDPS solution are as follows:

Sensor or Agent. Sensors and agents monitor and analyze activity. The term *sensor* is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term *agent* is typically used for host-based IDPS technologies.

Management Server. A *management server* is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

Database Server. A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers.

Console. A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities. Multiple detection and prevention capabilities are necessary to enable teams to identify vulnerable interactions and network components, effectively manage risk, and quickly mitigate attacks.

IV HEALTH AND SECURITY CHALLENGES

Health care technology has great potential to increase healthcare quality, expand access to services, reduce costs, and improve personal wellness and public health. These benefits will only be achieved, however, if individuals are confident in the privacy of their health-related information and if providers are confident in the security and integrity of the data collected. Health IT systems face daunting security and privacy challenges due to six recent trends:

- The locus of care is shifting as the healthcare system seeks more efficient and less expensive ways to care for patients, particularly outpatients with chronic conditions.

- Strong economic incentives to keep patient populations healthy, rather than caring for patients only when ill, are motivating healthcare providers to pursue innovative prevention plans and treatments of chronic conditions that entail more continuous patient monitoring outside of the clinical setting.
- Mobile consumer devices like smartphones and tablets are quickly being adopted by patients, caregivers, and healthcare providers for health and wellness applications in addition to their many other uses, making it difficult to protect sensitive health-related data and functions from the risks posed by general-purpose devices connected to the Internet.
    - Significant emerging threats target health IT systems, while new regulations strive to protect medical integrity and patient privacy.
    - Rapid technology advances that enhance mobile devices' utility— for example, computational models that convert wearable-sensor data into measures of addictive behaviors such as cocaine use or smoking— increase the range of potentially private events that can be inferred from seemingly innocuous sensor data.
    - Healthcare organizations lack the technology and expertise to adequately secure patient data. According to a recent survey, 69 percent of clinicians said their organization did not address demonstrated cyber vulnerabilities in medical devices.

Fig.3 represents how IoT can be linked with Automation, Health care, Entertainment, Defence and critical infrastructures like Grids.

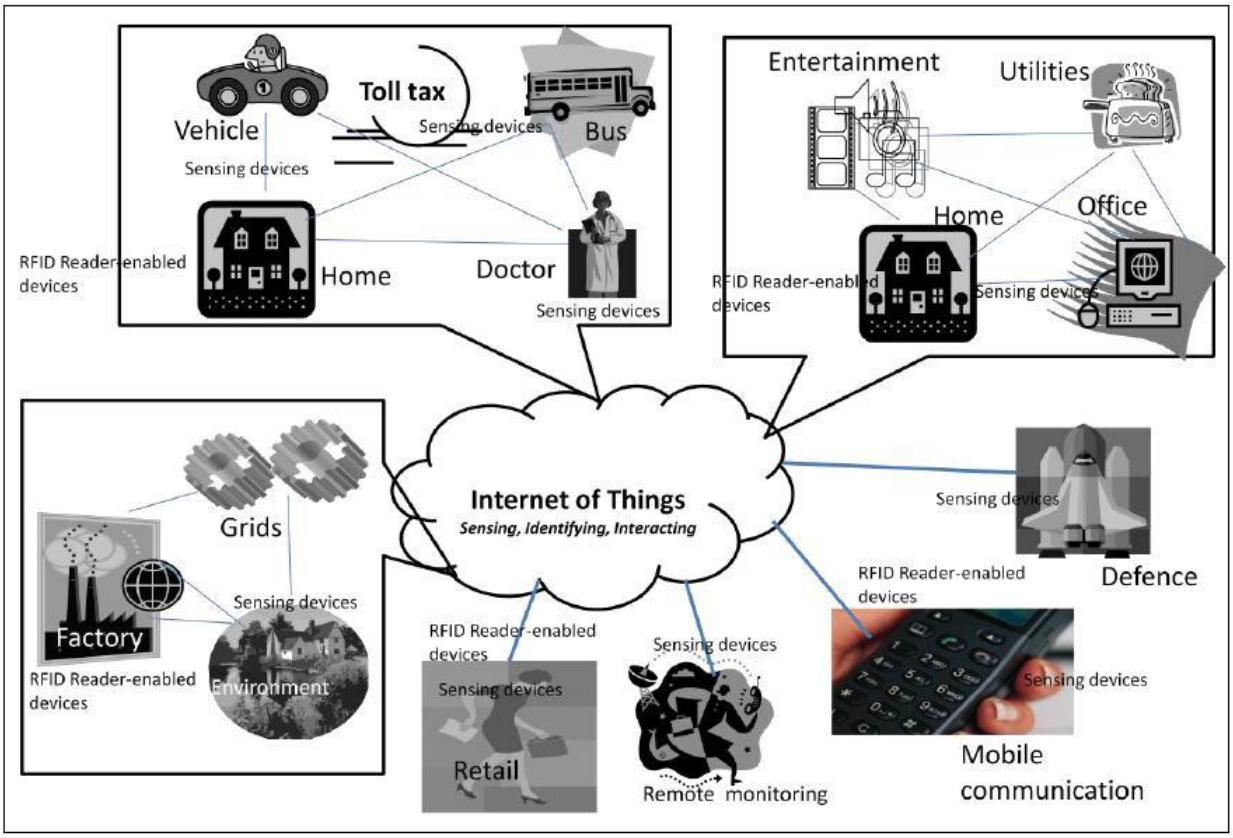

Fig.3 IoT with Health, Automation, Critical Infrastructure

V PROPOSED ARCHITECTURE FOR SECURITY WITH IoT

Our proposed system has a standalone host-based intrusion detection and prevention framework implemented at each node. The protection framework is composed of three components:

1. Intrusion detection and prevention module
2. Load balancer
3. Intrusion response module

Our main aim is to develop an IDS based on specification detection model that would be precise, not easily cheated by small variations in patterns, low in false alarms, adaptive and be of real time. Fig.4 represents our Intrusion Detection and Prevention Module.

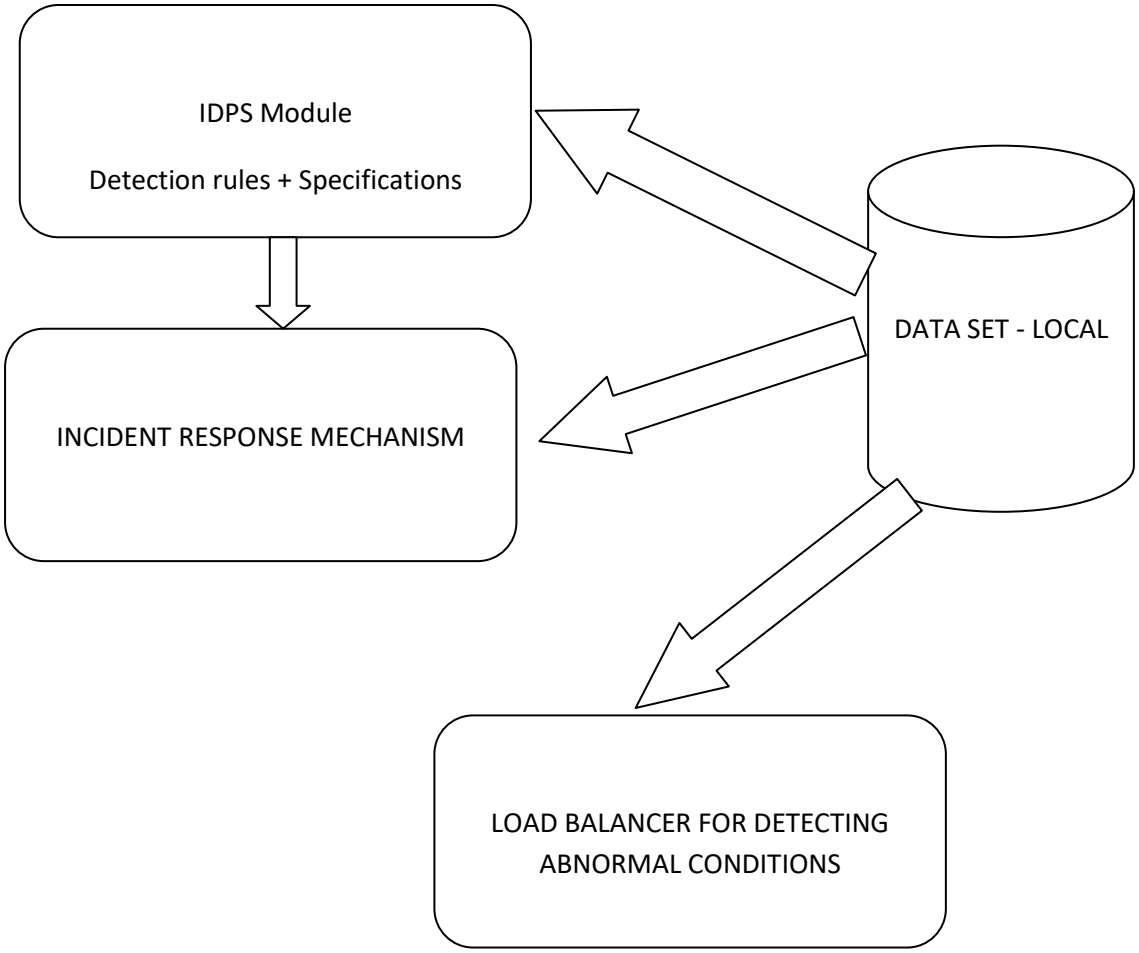

Fig.4 IDPS Module

IDPS Module

Intrusion detection and prevention mechanisms can detect malicious activities performed by external or internal attackers, by monitoring and analyzing network activities. The existing IDS architectures for ad hoc networks can be classified into stand-alone, cooperative and hierarchical. In stand-alone architecture, every node in the network performs detection based on its local data using an IDS agent installed on it. In cooperative architecture, each node has an IDS agent that communicates and collaborates with other nodes' agents, forming a global intrusion detection to resolve inconclusive detections. Hierarchical IDS is a sort of cooperative architecture suited to multi-layered networks. In this architecture, the network is divided into clusters, where some nodes are selected as cluster heads to undertake more responsibility than other cluster members. Each cluster member performs local detection, while cluster heads perform global detection. The detection and prevention module consists on specification-based IDS agent to monitor the interactions of the hosting node with the other nodes and to detect specification violation attacks.

Load Balancer

To avoid fast forwarding attacks such as rushing and wormhole, we add a load balancer module to each node. The principle of load balancer is to enable neighboring nodes of a fast-forwarding node to detect that malicious node has a high capacity of competition in route discovery. The goal of the load balancer is to select routes that do not pass through loaded neighbor nodes, which have a route-discovering rate higher than the threshold.

Response mechanism

Each time an intrusion (specification violation) is detected, the response mechanism immediately punishes malicious node by completely isolating it from the network. The malicious node is simply treated as non-existent. To minimize the negative impact or the adverse effect of isolation on the network operations, we use an isolation scheme with different isolation periods that consider repeated intrusions so as to isolate compromised nodes for a longer period.

Unique Challenges for IOT Security

- IoT relies on microcontrollers with limited memory and computational power
- This often makes it impractical to implement approaches designed for powerful computers
- This in turn requires constrained IoT devices to be hidden behind secure gateways
- Threats based upon gaining physical access to IoT devices
- More powerful Systems on a Chip (SOC) embedding hardware security support
- Ecliptic Curve Cryptography with reduced computational demands
- Anything that is exposed to the Internet must be securely software upgradable
- User experience must be good enough to avoid becoming a weak link in the chain
- The necessity of keeping up to date with security best practices

VI IoT IN HEALTH CARE SYSTEMS

Hospitals and hospital equipment are predicted to be areas where the IoT will have a vast growth the forthcoming years. Many IT Industries have already entered the field and are attempting to create solutions for increasing quality and efficiency in the treatment of patients. By connecting equipment which monitors and assists patients, both time and money could be saved, as well as making the diagnosing of the patients better and more accurate.

End-nodes For this application, the end-nodes are assumed to be of two types. First, a monitor device that measures a patient's heart rate and body temperature. This device performs simple sensing and displays the data, as well as transmitting the same data through a network interface. Second, is an infusion pump that has settings for the rate and amount of fluid, for example medicine, that is to be infused into a patient's circulatory system. While this device can perform sensing of the remaining level of medicine, it can also adjust its settings for medicine infusion according to instructions which are given by manually pressing a panel. Also, the rate and amount can be configured through a network service that receives requests with particular parameters. The network interface of these devices uses WiFi technology and is thus able to communicate over common wireless links.

Infrastructure For the end-nodes to work properly, this application relies on having a WiFi connection on the location where the devices are to be used. When connected, the equipment transmits packets to the default gateway of the WiFi connection, and here the packets are forwarded into the backbone network. As with the smart meter application, the backbone network used in the health equipment application is the Internet. However, in this scenario, connectivity to the Internet is not fully managed by the IoT platform, and a private Internet connection has to be present at the WiFi connection's default gateway. Further, this implies that the end-nodes not only can be used in hospitals or other health institutions but also in patients' homes, as long as the prerequisites are fulfilled.

Service platform When the devices transmit data to the processing center, which is done at given intervals, the center stores this and is able to track changes in heart rate, temperature, and medicine consumption over time. By linking the equipment to a patient register, health personnel can have a near real-time record of patients' status, and can access the information from any location. To protect the privacy of the patients, the processing center implements access policies which ensure that only those who need information about certain patients are able to see it. Upon accessing this information, the user can see charts

and diagrams to gain an overview of the patient's development for a given time period, for example through the night. Should a doctor access the processing center and, based on the "online and live health record", see that a patient has an obvious need for a changed amount of medicine, this can be achieved by adjusting the parameter of the connected infusion pump through the processing center's interface. The application logic and the infrastructure will then generate and transmit proper instructions to the end-node at the patient's location, and store all the performed actions in logs.

By using an application for connected health equipment on an IoT platform, the need for manually logging and storing records is reduced and potentially removed. It could open for more efficient and correct treatment of patients, and also to some extent allow patients to receive treatment where they desire. While only two types of devices are introduced here, the principle would be the same for any other equipment, and when diagnosing patients in the future, this could possibly be done based on a much higher amount of factors and perhaps even automatically.

VII PROPOSED ARCHITECTURE OF HEALTH CARE SYSTEM

IoT in health care ensures remote monitoring of patients. In this proposed system we are designing two applications:

i) Patient Health Care System – Collects all details about patients history.
ii) Hospital Information System – It has information about all the hospitals.

Above two systems should be integrated and launched in Cyber Physical System. Now any patients can be shown to any hospital, almost all the information available in Cyber. So that patients no need to carry about their reports. If they want to get second opinion about some other hospitals, they have to say their ID only. Since everything is available in Cyber, authorized Docters can see their report and give their opinions about the patient. Health Monitoring System Architecture :

1) Body Temperature Sensor – LM 35 is a very low cost and easily available sensor.
2) Heart Rate Sensor / Pulse Sensor is a plug-and-play heart rate sensor for Arduino.
3) Node MCU (Micro Controller Unit) is an IoT Module based on ESP8266 WiFi module.

- Ubidots is an IoT Application builder with data analytics and visualization.
- ThinkSpeak is an IoT Platform that lets you collect and store sensor data in the cloud and develop IoT Applications.
- ThingSpeak is an IoT analytics platform service that allows you to aggregate, visualize, and analyze live data streams in the cloud. You can send data to ThingSpeak from your devices, create instant visualizations of live data, and send alerts using web services like Twitter and Twilio.

Integration Health Care Data with Security and IoT Technologies

We can integrate our health care system to be secured using IoT Devices. Initially we have to identify the intruders / attackers or we can identify the vulnerabilities in our data. If anything goes wrong in our system, immediately we have to eliminate the vulnerabilities and keep the system to be secure. If any thing goes abnormal, through the sensors, immediately we have to inform to the concerned persons.

Expected Outcomes / Result

- ✓ Secure transmission of health care data in IoT can be achieved with the help of security.
- ✓ To achieve privacy such as confidentiality, data integrity and authenticity between the IoT Devices.
- ✓ Increase the speed of execution with limited resources constraint.
- ✓ Develop secure real time IoT applications so that every one can benefit the usage of IoT Technologies.

VIII CONLUSION AND FUTURE WORK

In this paper, we discusses how we can provide more security to health care data using cyber physical systems and IoT. Since all our data is in Cloud, cloud providers have to provide more security to the data. The Internet of Things complex nature, it is obvious that even software industries also do not fully understand how everything fits together. Therefore, the further development of IoT standards should be prioritized to ensure that secure systems are actually developed and implemented.

From our studies, we noticed that a fully holistic security solution is yet to be developed and evaluated. Given that all solutions evaluated make certain assumptions on the functioning of the system, a fully integrated solution needs to be developed and evaluated to determine if all the security mechanisms required can actually run on a constrained device. To be able to secure IoT applications better, future work could also take on subjects such as how to optimize encryption of sensor data, better prevention of traffic analysis, and the establishment of integrity combined with trust in the IoT. Furthermore, to better understand how the failure of various nodes in an IoT platform could affect the applications running on it, simulations of both random and targeted attacks could be made. Finally we can conclude our paper is, we can send and store data using encryption mechanism so that only authorized user can handle the data. Intruders or attackers can be identified and alert notification send to the concerned persons. We strongly believe that still some more security mechanism should be implemented while we are using IoT Technologies.

REFERENCE

[1] A.Skarmeta, J. Hernandez-Ramos, and M. Moreno, "A decentralized approach for security and privacy challenges in the internet of things," Internet of Things (WF-IoT), 2014 IEEE World Forum on, March 2014, pp. 67-72.

[2] Amnar Almomani, B. B. Gupta, Samer Atawneh, A. Meulenberg, Eman Almomani, "A Survey of Phising Email Filtering Techniques," *IEEE Communication Survey & Tutorials*, vol. 15, pp. 2070-2090, March 2013.

[3] Ahmed, K. A., Aung, Z., & Svetinovic, D. (2013). Smart Grid Wireless Network Security Requirements Analysis. *2013 IEEE* International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 871–878. http://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.

[4] A. Research, " The internet of things will drive wireless connected devices to 40.9 billion in 2020," 2014, accessed: 15-Feb-2014. [Online]. Available: https://www.abiresearch.com/press/ the-internet-of-things-will-drive-wireless-connect.

[5] Daniel Miessler. *IoT* Attack Surface Mapping. https://www.owasp.org/images/3/ 36/IoTTestingMethodology.pdf at DEFCON 23, 2015.

[6] D. Guinard, V. Trifa, F. Mattern, and E. Wilde, "From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices," , 2011, pp. 97–129.

[7] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, vol 4, pp. 2-7, September 2009.

[8] E. Rescorla, Inc. RTFM, N. Modadugu, and Inc. Google, "Datagram Transport Layer Security Version 1.2," Internet Engineering Task Force (IETF), 2012.

[9] H. Zhang, "A peer to peer security protocol for the internet of things : Secure communication for the sensible things platform," 2014.

[10] K. Narasimha Mallikarjunan, K. Muthupriya, S. Mercy Shalinie, "A Survey of Distributed Denial of Service Attack," *International Conference on Intelligent System and Control*, IEEE, pp. 1-6, January 2016.

[11] Lee Stogner, "An Introduction to the Internet of Things from the perspective of the IEEE Internet of Things initiative," International Conference on Collaboration Technologies and System, pp. 506-506, August 2015.

[12] P. Flood and M. Schukat, "Peer to peer authentication for small embedded systems: A zero-knowledge-based approach to security for the internet of things", pp. 68-72, 2014.

[13] R. Khan, Univ. of Genova (UNIGE), Genova, Italy DITEN Dept., S.U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference, Islamabad, 2010, pp. 257 - 260.

[14] Reem Abdul Rahman, Babar Shah, "Security analysis of IoT protocols: A focus in CoAP," *MEC* International Conference on Big Data and Smart City, IEEE, pp. 1-7, March 2016

[15] Telenor Connexion AB. Addressing a global health concern. http://www. telenorconnexion.com/stories/srett-medical, 2016.