Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

ASSISTIVE TOOLS FOR MACHINE COMMUNICATION FOR PREVENTING CHILDREN AND DISABLED PERSONS FROM ELECTRIC HAZARD USING CYBER PHYSICAL SYSTEM

Dr.S.Hemalatha [1], Mr.G.Dhamodhara kannan [2], Mr.M.Nagagopal [3], Mr.M.Vigneshwar [4]

[1]*Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai – Tamilnadu, India.*

pithemalatha@gmail.com

[2] *UG Scholar, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai - Tamilnadu, India.*

dharankannan97@gmail.com

[3] *UG Scholar, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai – Tamilnadu, India.*

Naga.gopal326@gmail.com

[4] *UG Scholar, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai - Tamilnadu, India.*

iasvigneshviki@gmail.com

ABSTRACT--**This paper proposes survey on the modern technological electrical devices are replaced the human daily house hold work. All the houses are having different electrical devices depends on the needs. In Parallel causes of electric hazard are also increasing. A survey reveals the major causes of electric hazard pointing objects are children and disable persons. Because of lacking of awareness about electric devices and it cautions. Consequently there is a need to develop the monitoring devices to prevent the electric hazard for the children and disabled persons. Machine learning techniques are used to learn the machine activities and able to control machine. Cyber physical system provides communication between heterogeneous systems. This two technology is incorporated in to the proposed work to provide the device which able to control the electric hazard for children and disabled person. The proposed work consists of motion sensors which monitor the movement of the object continuously. If the object nearing to the any electric machine like washing machine , fridge and iron box etc., immediately the circuit will turn off unless the object moving away from the electric device. Also the device can able to generate the sound signal and give caution to the children and disable about the dangerous of the electronic device. Along with machine learning and cyber physical system the proposed work uses the Internet of Things to connect the devices status and object status to the responsible persons who are all in the inaccessible location. The IoT can assist in integration of communications, control, and information processing across various systems. The Internet of Things allows objects to be sensed and controlled remotely. Wireless Home Automation system(WHAS) using IoT is a system that uses computers via GPRS to control basic home functions and features automatically System using GPRS through internet from anywhere around the world, an automated home is sometimes called a smart home. a home automation system using cloud combined with IOT that make use of Wireless Sensor between the controller and user section. By using this technological devices will provide secure life to the children and disabled persons.**

KEYWORDS- Cyber Physical System (CPS) ,Wireless Network, Machine-to-Machine (M2M), Home Automation System, Machine Learning, Electric Hazard.

I. INTRODUCTION

The Cyber Physical System area unit the mixtures components and physical entities that may act with human through several modalities. the security includes the malicious tries by somebody that disrupts or destructs the functions of physical system that affects child and disabled persons from electrical hazards. A variety of sensors and actuators monitor the behaviour and phenomena in the physical world and the resultant data are moved to the cyber world, where they are analysed to infer the state of the physical world and generate corresponding digital representations of the involved physical entities. The digital representation is used to derive knowledge about the state of the physical world and to optimize and control it through actions implemented through actuators. The related research area that is concerned with the integration of physical processes and computation in order to merge the physical and cyber world is termed CPS. The Internet of Things (IoT) paradigm, which seeks to interconnect computers to objects with self-configuring capabilities, plays an important role in the convergence of the physical and cyber worlds by ensuring secure and energy-

efficient transfer of information (in both directions). The confluence of CPS with IoT has resulted in an impactful association of the physical world observations, sensed by the connected smart objects, with the computational processes of the cyber world. It has enabled modelling and reasoning of the physical phenomena, which coupled with efficient communication and data processing, can result in effective actuation. The variety of devices that can monitor the physical environment, encompass fixed sensor network installations.(e.g Wireless Sensor Networks (WSNs) for environment monitoring , smart home installations and sensor deployments for air quality monitoring).

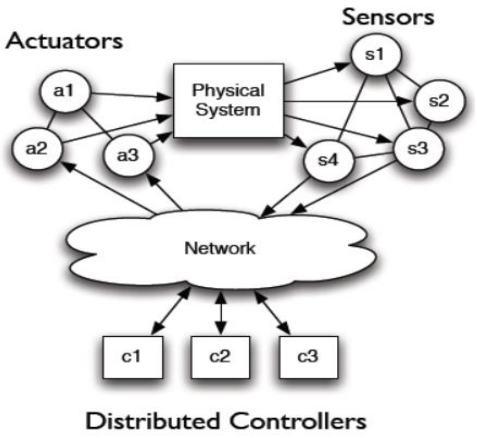

Figure 1.General Architecture Diagram of CPS

The high installation cost of fixed sensor networks and insufficient spatial coverage has led to mobile sensing initiatives, primarily by city authorities , which involve sensors mounted on public transportation vehicles (e.g., for environment monitoring).The objects could be physical devices that have identities, attributes and intelligent interfaces to be seamlessly integrated into the Internet through communication standard and interoperable communication protocols. With the CPS, the human lives will have another revolution. There are three major types of the components to form three tiers in a CPS. One type of the components is a group of sensors to form an environmental tier. The second type is the actuators, which form a service tier. And the last type is the controllers forming the control tier. The environmental tier is in charge of information collection from various physical systems. The major functions of the environmental tier in a CPS would be implemented by machine to machine (M2M) communication, where intelligent devices including sensors communicate with each other by utilizing both wireless and wired technologies. A M2M communication system consists of three interlinked domains: 1) A sensor area domain including sensor networks with M2M gateways, 2) A communication network domain including wired/wireless networks and 3) An application services domain consisting of the end users and applications required in the CPS [1]. The most relevant characteristic of a CPS is the tight integration between the physical process under control and the controlling digital computing system. Key issues in CPS are sensing and actuation, the modelling of the physical system, real-time computing, and networking. Example applications for CPS are in the field of manufacturing control, energy systems, automotive and avionics systems, traffic control, medical systems, cooperative robotics and smart buildings [2]. The exponential growth of wireless communication devices and the ubiquity of wireless communication networks have recently led to the emergence of wireless machine-to-machine (M2M) communications as the most promising solution for revolutionizing the future "intelligent" pervasive applications [5]. We begin with our vision of the future embedded mobile Internet. Then we look at several M2M use cases that offer significant market potential. We discuss the requirements and challenges associated with mass-scale M2M networks, and describe potential system architectures and deployment options that can enable the connectivity of billions of low-cost devices. We describe the salient features of M2M traffic that may not be supported efficiently by current standards and provides an overview of potential enhancements [6]. Home networks are rapidly developing to include a large diversity of devices/machines/terminals, including mobile phones, personal computers, laptops, TVs, speakers, lights, and electronic appliances. With the dramatic penetration of embedded devices, machine-to-machine (M2M) communications will become a dominant communication paradigm in home networks, which currently concentrate on machine-to-human or human-to-human information production, exchange, and processing. M2M communications is characterized by low power, low cost, and low human intervention [1, 2]. M2M communications is typically composed of a number of networked devices and a gateway. The gateway is responsible for the connection among the devices, and the connection between the M2M communications area and other networks [7].Furthermore, a common M2M service platform is also needed to facilitate multi-industry M2M applications such as smart grids and smart cities, and to enable seamless M2M deployments among heterogeneous M2M systems [8].Devices-to-Device(D2D) enables devices to communicate directly with each other without traversing fixed network infrastructures such as access points

or base stations [9]. To achieve 1000-fold capacity increase in 5G wireless communications, Ultra Dense Network (UDN) is believed to be one of the key enabling technologies. The next generation of wireless communication systems might be implemented and operating. According to a report released by the 5G Infrastructure Public Private Partnership (5G-PPP) community, the next generation of wireless networks need to support more than 10,000 devices per square kilo meter and offer high date rate of 1 Gbps with a very low transmission delay of 1 to 10ms.The key technical requirements for 5G are believed to enable high per-user throughput, high network throughput, ubiquitous connections, and low latency[10]. To achieve 1000-fold capacity increase in 5G wireless communications, Ultra Dense Network (UDN) is believed to be one of the key enabling technologies. The next generation of wireless communication systems might be implemented and operating. According to a report released by the 5G Infrastructure Public Private Partnership (5G-PPP) community, the next generation of wireless networks need to support more than 10,000 devices per square kilo meter and offer high date rate of 1 Gbps with a very low transmission delay of 1 to 10ms.The key technical requirements for 5G are believed to enable high per-user throughput, high network throughput, ubiquitous connections, and low latency[10]. The electronic hazards are very dangerous especially for the child and disabled person to avoid external hazards using communication between machines which implemented by cyber physical system.

II. PROBLEM DEFINITIONS

The electronic hazards area unit terribly dangerous Devices sometimes have restricted resources therefore moving a part of the service implementation to a cloud infrastructure may be a distinguished resolution. On the other hand having to interface with several devices can be terribly cumbersome, particularly for the child and disabled person during this planned project support to watch child and disabled person to avoid external hazards using communication between machines that enforced by cyber physical system.

III. LITERATURE SURVEY

[1]Shuo Chen, Maode Ma and Zhenxing Luo Proposes to guard the user's communication from illegitimate attacks within the M2M communications. The framework will guarantee a secure session among device nodes. the appliance of AIBEAWKE mechanism possesses associate degree attested cryptography feature and is while not key written agreement downside. the appliance of the economical AES might save the computation resource of the device nodes. The planned secret key management within the AIBEAWKE mechanism conjointly the regular key generation mechanism couldn't solely distribute and update the cryptography key handily however also cut back the chance of key outflow. the safety analysis indicates that the mutual authentication will be achieved and also the ability of withstanding multiple attacks might be supported by the planned

[2]Tullio Facchinetti and Marco L. Della Vedova Evaluate the physical system is sculptural as a collection of periodic activities that may be regular by adapting ancient period of time planning algorithms. The goal is to limit the height of power consumption, whereas guaranteeing a particular behaviour of the atmosphere. Such behaviour is encapsulated within the variation of state variables connected with the physical method in restraint. The planned methodology has been applied to masses related to physical state variables having constant dynamics with random disturbance on the state variable evolution. The innovative approach bestowed during this paper fosters the chance to use period of time planning techniques to prepare the activation of electrical masses in an exceedingly grid. Future works can address the discharge of some assumption created during this paper, the study of different system models to explore the appliance of the planned techniques to energy systems normally (gas, water, compressed gas, etc.), and therefore the integration of renewable sources within the model. Another doable issue to appear at is to model period of time parameters as multiple of a finite time quantum, because it happens in sensible implementations, rather than permitting them to require any real worth. during this case, it ought to be evaluated however the selection of the time quantum impacts on the system performance. Moreover, a crucial improvement can deal exhausting user needs, wherever violations to user needs aren't tolerated

[9]Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott Propose the progressive solutions to tackle security and privacy challenges in Device-to-Device (D2D) communication. They span across a range of D2D network communication, peer discovery, proximity services, and placement privacy. the present solutions in keeping with security and privacy necessities. supported the analysis, It will derive "best practices" and determine open issues that be with relation to lessons learned, the foremost thought embody device diversity, resource limitation, user incentive, resolution deplorability, demand conflicts, analysis tools and legal concern. It will function a reference guide for researchers and developers to facilitate the planning and implementation of D2D security and privacy solutions.

[10]Shuyi Chen, Ruofei Ma, Hsiao-Hwa Chen, Hong Zhang, Weixiao Meng, and Jiamin Liu Propose in most of the previous works, UDNs were thought of primarily for H2H communications solely, while not considering M2M communications. M2M communications can play a crucial role in future 5G systems. Thus, it's necessary for UDNs to support M2M communications, in conjunction with H2H communications. so as to support M2M communications in UDNs expeditiously, completely different strategies were known in terms of

implementations of PHY, MAC, network, and application layers, severally. Two necessary problems, security/privacy and network virtualization, were conjointly mentioned during this paper, and it absolutely was noticed that security/privacy of M2M communications are a significant issue in UDNs. even supposing network virtualization could be a trend for UDNs, it's laborious to be enforced for M2M communications in a very efficient manner.

[11]Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo, Suggest a We have analysed fundamental monitoring limitations for cyber-physical systems under attack modelled by linear time invariant descriptor systems with exogenous inputs. In particular we have characterized undetectable and unidentifiable attacks from system theoretic and graph-theoretic perspectives, we have designed centralized and distributed monitors , we have provided illustrative examples. Future and on-going work includes a detailed analysis of the convergence of our distributed monitors, the design of distributed identification monitors, and the design of monitors robust to system noise and unmolded dynamics.

IV. SYSTEM DESIGN

4.1. PROPOSED SYSTEM

The aim of this work is to design and develop a control system using IOT and Zigbee technology to remotely control the machine over a infrastructure. The device comprises four main units, namely: the mobile phone or a computer system, the IOT Module, the switching unit and the Zigbee module. One feature that makes the developed system better than other related existing works is its ability to use two means of control. It makes use of Zigbee when the operator is within the coverage area of the network of about 100 metres to the device, at no cost, otherwise it uses IOT containing certain codes to control the machines. A SIM card is placed in the IOT Module from the transmitter are sent to module via Web Application. They gives an impressive performance with both IOT and Zigbee technology.

4.1.1. ADVANTAGE

- We propose an end to end GPRS communication for machine to machine communications.
- It makes the machines to possess its own deciding time, throughput, efficiency , error ,accessing method with new algorithms.
- IOT principles makes simpler controlling in industry machines with predefined time with its own available controller.

4.2. EXISTING SYSTEM

The conventional method employed folks and massive producing for industries is the use of security purposes who move from one point to another to switch on and off the machines. This approach is obviously terribly tedious and difficult to do on daily basis. Aside from this, it is not efficient enough as the person to blame of the duty may fail to perform it at the right time, that may lead to physical have an effect on.

4.2.1. DISADVANTAGES

- Cyber physical management is completed through one end as dominant server application and other end as machine.
- We would like external analysis process system that specified probabilities for miscommunication and hacking our information by accessing the server.
- The time and alternative parameters area unit controlled by external server.

V. MODULES

5.1. SENSOR INTERFACE

The sensing element Interfaces may be a prescript designed for information transfer between machines or user terminals and good sensors. AN Infrared sensor is an device , that emits so as to sense some aspects of the environment. AN IR sensor will measure the warmth of an object likewise as detects the motion. These varieties of sensors measures solely infrared emission , instead of emitting it that's referred to as as a passive IR sensor. sometimes within the spectrum, all the objects radiate some type of thermal radiations. These varieties of radiations are invisible to our eyes, which will be detected by an infrared detector. PIR sensor detects somebody's being on the move inside approx 10m from the sensing element. this is often average worth ,the essentially fabricated from a pyro electrical sensor, that detects levels of infrared emission ,They are flat management and stripped effort, have a large lens vary, and are easy to interface with the other interfaces.

5.2. MACHINE-TO-MACHINE DATA POSTING

Data posting within the approach Sharing the data that get as input from one or another. Here Machine to Machine information posting, because the sensors that observe the individual near to that devices rather to previous communications. Here we tend to used GSM allows GPRS and that makes them to address and sends its query's from sensors to the machines that concerning it's through the information packets. Machine to machine (M2M) refers to technologies that enable each wireless and wired systems to communicate with different devices of a similar kind. Machine-to-Machine (M2M) technology permits organizations to collect information from the sting of the enterprise and apply it in ways in which completely impact the business. Exchange of data between machines that's established between the central system (server) and any variety of equipment , through one or many communication networks.

5.3. DATA GETTING AND ANALYSIS

Data analysis ought to be taken rigorously. once testing multiple models quickly there's a high attain finding a minimum of one among them to be important, but this may ensue to an error it's necessary to invariably modify the importance level once testing multiple models they supply varied analytic procedures "provide the way of drawing inductive inferences from information and identifying the signal (the development of interest) from the noise (statistical fluctuations) present within the information that gets through address to the machine and the performs the decision creating whether goes to prevent fully instead to do some others actions and again they'll reply back to the machine that send address in between the cloud storage are be in hot water the long run responses as they done the nearby machines that response for the motions and obtain that 10m than build a live standing update.

5.4. APPLIANCE CONTROL AND RESPONSE

In Home all those Machines are sensible and at first we provide the management to the persons who having to change ON and OFF the overall Work, when authentication the complete system performs its communication conjointly we tend to connected the cloud storage, that storage the communications and how its response additionally the message be sent to manage persons whether or not been any motion close to machines also we had interfaces if we would like to feature new machines then it will be more simply. It will inform the user by causing message back to the remote devices still as emergency department if necessary.

VI. CONCLUSION

The Main aim of our Projects The electronic hazards are very dangerous especially for the child and disabled person.in this proposed project support to monitor child and disabled person to avoid external hazards using communication between machines which implemented by cyber physical system.

VII. REFERENCES

[1] Tullio Facchinetti and Marco L. Della Vedova , "Real-Time Modeling for Direct Load Control in Cyber-Physical Power Systems (2011)," IEEE Transactions On Industrial Informatics, Vol. 7, No. 4, November 2011, pp. 689-698.

[2] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical Systems: A New Frontier," Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTU), June 2008, pp. 1-9.

[3] Shushan Zhao, Akshai Aggarwal, Richard Frost, Xiaole Bai , "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Network," IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012, pp.380-400.

[4] Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shensu, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications," IEEE Communications Magazine, April 2011, pp.28-35.

[5] Geng Wu, Shilpa Talwar, Kerstin Johnsson, Nageen Himayat, and Kevin D. Johnson, "M2M: From Mobile to Embedded Internet (2011)," IEEE Communications Magazine ,April 2011, pp. 36-43.

[6] Yan Zhang, Rong Yu, Shengli Xie, Wenqing Yao and Yang Xiao, "Home M2M Networks: Architectures, Standards, and QoS Improvement,"IEEE Communications Magazine , April 2011 , pp.44-52.

[7] Jorg Swetina, Guang Lu, Philip Jacobs, Francois Ennesser, and JaeseungSong "Toward A Standardized Common M2M Service Layer Platform: Introduction To OneM2M ," IEEE Wireless Communications , June 2014, pp.20-26.

[8] Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," IEEE Communications Surveys & Tutorials, Vol. 19, No. 2, Second Quarter 2017 , pp.1054-1079.

[9] Shuyi Chen, Ruofei Ma, Hsiao-Hwa Chen, Hong Zhang, Weixiao Meng, and Jiamin Liu, "Machine-to-Machine Communications in Ultra-Dense Networks—A Survey," IEEE Communications Surveys & Tutorials, Vol. 19, No. 3, Third Quarter 2017, pp.1478-1503.

[10] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo, "Attack Detection and Identification in Cyber-Physical Systems" IEEE Transactions On Automatic Control, Vol. 58, No. 11, November 2013, pp.2715 - 2729.

Dr.S.Hemalatha did her Bachelor degree in Computer Science and Engineering and Masters in Computer Science and Engineering University of Madras and Anna University Chennai , India in 2000, and 2004 respectively. She completed PhD in Computer Science and Engineering from Anna University, India in 2016. She has totally 17 years of experience in different engineering colleges and currently she is working as a Professor in Computer Science and Engineering in Panimalar Institute of Technology, Chennai, India. She has published 45 national and International journals and 30 papers in international conferences. She is the recipient of Distinguished Professor award from CSI Mumbai chapter in the year 2016, Professional achiever award from IEEE madras section in the year 2017. She has guided many UG and PG level projects and being a committee member for Research Scholars in Anna University. Her research areas are Network Security, Mobile Communication and Mobile Application Development. She is a member of CSI, IEEE and ISTE.

Mr.G.Dhamodhara Kannan, is a final year Computer Science and Engineering student in Panimalar Institute of Technology. He is a member of Computer Society of India.

Mr.M.Nagagopal , is a final year Computer Science and Engineering student in Panimalar Institute of Technology. He is a member of Computer Society of India.

Mr.M.Vigneshwar , is a final year Computer Science and Engineering student in Panimalar Institute of Technology. She is a member of Computer Society of India