International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Assistive Tools for Machine Communication for Preventing Children and Disabled Persons from Electric Hazard Using Cyber Physical System

[*1]Dr. S. Hemalatha, [2]Dr. T. Tamilselvi, [3]Dr. R. Saravana Kumar, [4]A. G. Noorul Julaiha M. E, [5]Dr. M. Thangamani, [6]Mrs. S. Lakshmi and [7]Dr. Kamal Gulati

Submitted: 01/11/2022 **Accepted:** 03/02/2023

Abstract: The determination of this research is to conduct a survey on how current technical electrical equipment are replacing human daily housework. Different electrical gadgets are installed in each home, depending on the necessities. At the same time, the number of people who are exposed to electric hazards is growing. According to a report, children and disabled people are the main sources of electric danger pointing devices. It cautions due to a lack of information regarding electric equipment. As a result, monitoring systems must be developed in order to prevent electric hazards for children and handicapped people. Machine learning techniques are used to learn about and control machine activity. Communication between heterogeneous systems is provided by a cyber-physical system. These two technologies are combined in the proposed effort to create a gadget that can manage electric hazards for children and the disabled. Motion sensors are used in the proposed work to continually monitor the object's movement. If an object comes close to an electric machine, such as a washing machine, refrigerator, or ironing board, the circuit will automatically cut off unless the object moves away from the electric equipment. In addition, the gadget may create a sound signal to warn youngsters about the dangers of electronic devices and disable them. The suggested work, in addition to machine learning and cyber physical systems, makes use of the Internet of Things to link the status of devices and objects to the responsible personnel, all of whom are in an inaccessible place. The Internet of Things may help with communication, control, and data processing integration across several systems. The Internet of Things allows things to be sensed and controlled remotely. The Internet of Things (IoT) Wireless House Automation System (WHAS) is a system that combines computers and GPRS to automate basic house functions and features. An automated house is frequently referred to as a smart home since it uses GPRS to connect to the internet from anywhere in the globe. A cloud-based home automation system with IoT that uses the Wireless Sensors which is used to connect the controller and the user section. Children and handicapped people will have a safer existence as a result of the use of technological equipment

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

1. Introduction

The Cyber Physical System is made up of components and physical phenomena that may interact with people in a number of ways. The phrase "security" refers to someone attempting to intentionally disrupt or damage the operation of a physical system, placing children and people with disabilities in danger from electrical threats.Sensors and actuators observe physical behaviour and events, and the resulting data is delivered to the cyber earth, anywhere it is analysed toward identify the status of the substantial earth and digital representations of the physical objects involved are constructed. The physical environment is optimised and managed using actuator-based operations and information about its status is generated using the digital representation. The goal of CPS, a similar academic field, is to use physical processes and computers to bridge the gap between the real and virtual worlds.

The IoT concept, which aims to connect computers to self-configuring objects, is critical for permitting safe

[1]*Professor/CSE, Panimalar Engineering College, Chennai, Tamil Nadu, India*
[2]*PhD, Associate Professor/CSE, Panimalar Engineering Colege, Chennai, Tamil Nadu, India*
[3]*Associate Professor /CSE, Dayananda Sagar Academy of Technology and Management, Bangalaore, India*
[4]*Assistant Professor/CSE, Rajalakshmi Institute of Technology*
[5]*Associate Professor/ Information Technology, Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India*
[6]*Associate Professor/ Department of Electronic and Instrumentation Engineering, Panimalar engineering College, Chennai, Tamil Nadu, India*
[7]*Associate Professor, Amity University, Noida, Uttar Pradesh, India*
[1*]*pithemalatha@gmail.com* / [2]*tamilselvime@gmail.com* /
[3]*saravanakumar.rsk28@gmail.com* / [4]*ag.nooruljuaiha@gmail.com* /
[6]*elzie.moses@gmail.com* / [7]*drkamalgulati@gmail.com* /
[7]*Orcid ID: 0000-0002-1186-1426*

and energy-efficient data transport in both the real and virtual worlds (in both directions).The coming together of CPS and IoT has resulted in a strong relationship between physical world observations and cyber world computing processes, as experienced by connected smart devices. It has made it possible to describe and reason about physical events, which, when paired with rapid transmission and data processing, might lead to effective actuation. Fixed sensor network installations are among the devices that may monitor the physical environment.(WSNs for environmental monitoring, smart house installations, and sensor deployments for air quality monitoring, for example).

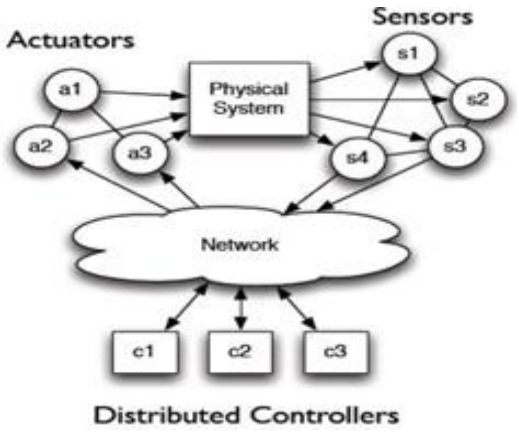

Fig. 1. General Architecture Diagram of CPS

Due to the expensive expense of installing fixed sensor networks and the lack of spatial coverage, local governments have begun to implement mobile sensing programmes, which include sensors installed on community transit vehicle .Physical devices with identities, properties, and intelligent interfaces that can be effortlessly incorporated into the Internet via communication standards and compatible communication protocols might be the objects.

Fig. 2. Components of CPS

Human life will undergo yet another transformation as a result of the CPS.Figure 2 depicts three basic sorts of components that combine to produce three levels in a CPS.A set of sensors forming an environmental tier is one sort of component.The actuators, which make up a service layer, are the second type.The controllers, who make up the control tier, are the last kind.The environmental layer is responsible for gathering data from various physical systems.Machine to machine (M2M) communication, in which intelligent equipment such as sensors interact with one another using both wireless and cable technologies, would be used to accomplish the key tasks of the environmental layer in a CPS.

A M2M statement system is composed of three interconnected domains:

A sensor area domain, which consists of M2M gateway sensor networks, a communication network domain, which encompasses wired and wireless networks, and an application services domain, which consists of the end users and applications of the CPS [1] are the three domains.

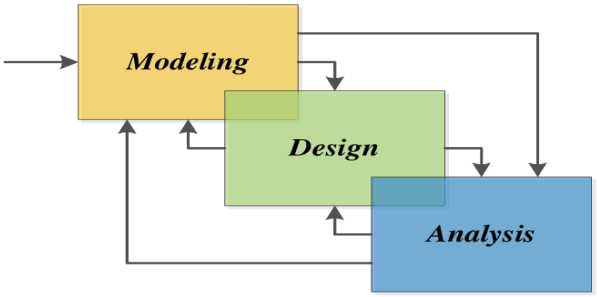

Fig. 3. CPS Design Process

The closest integration between the physical process under control and the governing digital computer system is the most important feature of a CPS. Sensing and actuation, as well as physical system modelling (shown in Figure 3), real-time computing, and networking, are all included in the CPS. (M2M) communications has lately emerged as the most promising technique for converting future "intelligent" ubiquitous applications [5] because to the exponential expansion of wireless communication devices and the ubiquity of wireless communication networks. Let's start with our concept of the embedded mobile Internet of the future. Then we'll look at a handful of M2M use cases that have a lot of potential. We examine the requirements and challenges of large-scale M2M networks, as well as several system designs and deployment strategies that might allow billions of low-cost devices to participate. We evaluate crucial parts of M2M traffic that present standards may be unable to manage efficiently, as well as a list of possible improvements [6]. Mobile phones, personal computers, laptops, TVs, speakers, lighting, and electronic appliances are all part of home networks, which are fast expanding to incorporate a wide range of devices/machines/terminals. due to the rapid adoption of embedded devices. Low power, low cost, and minimum human interaction characterise M2M communications [1, 2].

In M2M communications, a gateway and several networked devices are frequently utilised. Establishing connections between devices and between the M2M communications domain and other networks is the responsibility of the gateway [7]. Additionally, in order to encourage cross-industry M2M applications like smart grids and smart cities, as well as to enable seamless M2M deployments across diverse M2M systems, a standard M2M service platform is needed [8,].

Devices can connect via Devices-to-Device (D2D) communication without relying on the base stations or access points that currently support the network [9].

One of the key enablers of a 1000-fold capacity increase in 5G wireless communications is the Ultra Dense Network (UDN). The main technological needs for 5G are anticipated to be throughput, pervasive connectivity, and reduced latency[10].The Ultra Dense Network is one of the key enabling technologies for achieving a 1000-fold capacity increase in 5G wireless communications (UDN). In the near future, the next generation of wireless communication networks may be deployed and operational. According to a report published by the 5G Infrastructure Public Private Partnership 5G-PPP community, the next generation of wireless networks will need to support more than 10,000 devices per square kilometre and provide 1 Gbps data throughput with a transmission delay of less than one second. High per-user throughput, high network throughput, ubiquitous connectivity, and reduced latency are the major technical goals for 5G[10]. Children and disabled people who must connect with computers via a cyber physical system to avoid external assaults are especially vulnerable to electronic risks.

One of the essential enabling technologies for reaching a 1000-fold capacity increase in 5G wireless communications is the ultra dense network (UDN). The next generation of wireless communication networks could be installed and running soon. The next generation of wireless networks will need to accommodate more than 10,000 devices per square kilometre and offer 1 Gbps data capacity with a transmission delay of less than one second, according to a paper released by the 5G Infrastructure Public Private Partnership 5G-PPP community. The main technical objectives for 5G are high throughput per user, high network throughput, universal connection, and low latency[10]. Children and individuals with disabilities who need to use a cyber-physical system to access to computers in order to prevent external assaults are particularly susceptible to electronic

2. Problem Definitions

The electrical dangers are quite hazardous. Because devices have limited resources, migrating a piece of the check implementation to a confuse transportation may be a feasible choice .Having to interface with multiple devices, on the other hand, can be extremely inconvenient, particularly for children and disabled people. During this planned project, support will be provided to watch children and disabled people to avoid external hazards by using communication between machines enforced by a cyber physical system.

3. Literature Survey

[1] Proposes a solution for protecting user communication in M2M communications against unauthorised assaults. Device nodes will have a secure communication thanks to the framework. The AIBEAWKE approach has a well-known cryptographic feature and does not have a drawback of key written agreement. The device nodes' processing resources may be saved if the cost-effective AES is used. The AIBEAWKE mechanism's planned secret key management, as well as the regular key generation mechanism, might not only make cryptographic keys easier to distribute and update, but also lower the danger of key outflow. Mutual authentication will be realised, and the expected ability to withstand multiple assaults may be supported, according to the safety study. [2] Evaluate the physical system as a series of periodic activities that may be regular by changing ancient period of time planning techniques. The goal is to use as little energy as possible while guaranteeing that the environment reacts in a given manner. Such behaviour is encapsulated by the fluctuation of state variables linked with the physical approach under constraint. Masses connected with physical state variables with constant dynamics and random disturbances on state variable development were subjected to the proposed approach.

The unique concept provided in this paper enables time-based planning approaches to be used to prepare the activation of electrical masses in an exceedingly grid. Future work could concentrate on deconstructing some of the assumptions made in this paper, as well as investigating various system models to see how the proposed techniques can be applied to common energy systems (gas, water, compressed gas, etc.) and, as a result, the integration of renewable sources into the model. Another option to consider is modelling the period of time parameters as a multiple of a finite time quantum, rather than allowing them to have any actual value, since this is what occurs in realistic implementations. However, the influence of the time quantum decision on system performance should be addressed in this circumstance. Furthermore, if user expectations are not allowed to be violated, a crucial upgrade may address tired user requirements.

[9] Those that worked on the project include Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, SasuTarkoma, and JörgOtt. Propose new ways to deal with security and privacy concerns in Device-to-Device (D2D) communication. They cover a broad variety of subjects, including peer-to-peer network communication, proximity services, and privacy in placement. The present condition of security and privacy regulations
It will extract "best practises" and highlight unsolved difficulties relating to lessons learned, with device diversity, resource restrictions, user motivation, resolution deplorability, demand conflicts, analytic tools, and legal concerns being the most essential factors. It will act as a reference book for researchers and developers, enabling the design and implementation of D2D security and privacy solutions simpler.

For H2H communications, the majority of prior studies largely incorporated Shuyi Chen, Ruofei Ma, Hsiao-Hwa Chen, Hong Zhang, WeixiaoMeng, and Jiamin Liu, but M2M communications were not explored. M2M communications could be important in 5G networks in the future. UDNs must therefore manage M2M and H2H communications in addition to H2H communications. In order to enable M2M communications in UDNs as quickly as possible, many solutions for PHY, MAC, network, and application layer implementations were discovered. In-depth discussion of security/privacy and network virtualization was conducted in this article, with M2M interaction security/privacy being a significant issue in UDNs. Despite being a common trend among UDNs, it is difficult to deploy network virtualization for M2M communications in a cost-effective manner.

[11] A solution has been put out by Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. It has been researched how to monitor cyber-physical systems that are under attack using linear time invariant descriptor systems with exogenous inputs. We defined undetectable and unidentifiable assaults, designed centralised and decentralised monitors, and provided instances from a system theoretic and graph theoretic perspective. Future and ongoing work will include a thorough analysis of the convergence of our distributed monitors, the design of distributed identification monitors, and the manufacture of monitors that are robust to system noise and unmolded dynamics.

4. System Design

4.1. Proposed System

The goal of this project is to design and create a control system that uses IoT and Zigbee technologies to operate a machine remotely through a network.

Fig. 4. Zigbee module

For master to master or master to slave communications, Zigbee supports a variety of network configurations.

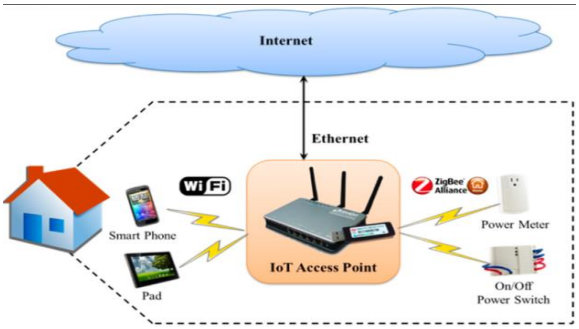

Fig. 5. Components of proposed work

- The gadget is made up of four basic components: a phone or computer system, an IoT module, a switching unit, and a Zigbee module.
- The ability to employ two modes of control is one aspect that distinguishes the created system from other similar existing works.
- It utilisesZigbee for free while the operator is within the network's service area of around 100 metres from the device; otherwise, it uses IOT with specific codes to manage the devices.
- The IOT Module is equipped with a SIM card, and data from the transmitter is transferred to the module via a web application.
- With both IoT and Zigbee technologies, they deliver outstanding results.

4.1.1. Advantage

- We present an end-to-end GPRS communication system for machine-to-machine communications, which allows machines to determine their own time, throughput, efficiency, error, and access method using novel algorithms.
- IoT principles simplify industry machine control with set time and its own available controller.

4.2. Existing System

- The traditional technique used people and large-scale production for industries, with security personnel moving from one location to another to turn on and off the machinery.
- This method is clearly extremely time consuming and difficult to implement on a regular basis.
- Apart from that, it is ineffective since the person in charge of the responsibility may fail to do it at the appropriate time, resulting in physical harm.

4.2.1. Disadvantages

- Cyber physical management is carried out via a dominant server programme on one end and a machine on the other.
- We'd like an external analytical process system that calculated the chances of misunderstanding and information theft by gaining access to the server.
- The remote server is in charge of controlling the time and other settings.

5. Modules

5.1. Sensor Interface

The sensory component is important. Data is sent between machines, user terminals, and good sensors through interfaces, which are a set of principles. A device that produces infrared light in order to detect particular elements of the environment is known as an infrared sensor. An infrared sensor can detect motion as well as determine how warm an item is. A passive infrared sensor is one that measures rather than emits infrared radiation. All items within the spectrum emit some type of heat radiation on occasion. These sorts of

radiations are invisible to the naked eye, but they may be detected using an infrared detector. Within a 10-meter radius of the detecting device, a PIR sensor detects movement. This is usually average worth, which consists of a pyroelectric sensor that measures infrared emission levels. They feature a large workforce, a flat management structure, and require little effort.

5.2. Machine-To-Machine data posting

Within the method, Data publishing Sharing data that is received as input from one or more sources. Because the sensors that detect the individual near the devices rather than previous communications, information is posted from machine to machine. We commonly combine GSM with GPRS, which allows them to address and send queries from sensors to machines via information packets. (M2M) technology enables businesses to collect data from the back end of their operations and apply it in ways that have a significant influence on the bottom line. Data exchange between machines that takes place across one or more communication networks between the central system (server) and a wide range of equipment.

5.3. Data getting and Analysis

Analyzing data should be done with care.When testing numerous models fast, there's a good chance you'll discover at least one of them to be significant, but this might lead to an error. It's always required to adjust the importance level when evaluating multiple models because they provide different analytic techniques.

Statistical fluctuations present within the data that arrives at the machine via address, and then making a decision whether to stop completely or take other actions, and then they'll reply back to the machine that sent the address in between the cloud storage are in hot water in the long run responses

5.4. Appliance Control and response

In the home, all of those machines are intelligent, and we first provide management to the people who have to turn on and off the overall work, and then we connect the cloud storage, which stores the communications and how they respond, as well as the message that is sent to manage people if there is any motion near the machines. We also have interfaces if we want to add new machines. If necessary, it will notify the user by sending a message to remote devices such as the emergency department.

6. Conclusion

The primary goal of our projects is to Electronic risks are particularly deadly for children and people with disabilities. This proposed project would assist in the monitoring of children and disabled people in order to avoid external threats through the use of machine-to-machine communication, which will be executed through a cyber-physical system.

References

[1] TullioFacchinetti and Marco L. Della Vedova ,“Real-Time Modeling for Direct LoadControl 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 ofIEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTU), June2008, pp. 1-9.

[3] Shushan Zhao, AkshaiAggarwal, Richard Frost, XiaoleBai, “A Survey of Applications of Identity-BasedCryptography in Mobile Ad-Hoc Network,” IEEE Communications Surveys & Tutorials, Vol. 14, No. 2,SecondQuarter2012,pp.380-400.

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

[5] Geng Wu, ShilpaTalwar, Kerstin Johnsson, NageenHimayat, and Kevin D. Johnson, “M2M: From Mobile to Embedded Internet(2011),”IEEECommunicationsMagazine,April2011,pp. 36-43.

[6] Yan Zhang, Rong Yu, ShengliXie, Wenqing Yao and Yang Xiao, “Home M2M Networks: Architectures, Standards,and QoS Improvement,”IEEECommunicationsMagazine, April2011,pp.44-52.

[7] JorgSwetina,GuangLu,PhilipJacobs,FrancoisEnnesser,andJaeseungSong“TowardAStandardizedCommon M2M Service Layer Platform: Introduction To OneM2M ,” IEEE Wireless Communications , June2014, pp.20-26.

[8] Michael Haus, Muhammad Waqas, AaronYi Ding, Yong Li, SasuTarkoma, and JörgOtt, “Security andPrivacy in Device-to-Device (D2D) Communication: A Review,” IEEE Communications Surveys & Tutorials,Vol.19,No. 2,SecondQuarter2017,pp.1054-1079.

[9] Shuyi Chen, Ruofei Ma,Hsiao-Hwa Chen, Hong Zhang, WeixiaoMeng, and Jiamin Liu, “Machine-to-MachineCommunications in Ultra-Dense Networks—A Survey,” IEEE Communications Surveys & Tutorials, Vol. 19,No.3, ThirdQuarter2017, pp.1478-1503.

[10] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo, “AttackDetection and Identification in Cyber-Physical Systems” IEEETransactions On Automatic Control, Vol. 58, No. 11, November2013, pp.2715 -2729