International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 10, October-2023, http://ijmec.com/, ISSN: 2456-4265

IOT-BASED SECURITY APPLICATIONS FOR INDUSTRIAL AUTOMATION: ENHANCING SAFETY AND PROTECTION

Mr. Muzaffar Ali Mohammad [*1], Mr. Rajesh Reddy Gade [*2], Dr. Mohammed Iliyas[*3]

[*1] PG Student Dept. of ECE (Embedded Systems), Shadan College of Engineering and Technology

md_hamedali@yahoo.com

[*2] Assistant Professor, Dept. of ECE, Shadan College of Engineering and Technology

rajesh.gbjr@gmail.com

[*3] Professor & HOD, Dept. of ECE, Shadan College of Engineering and Technology

ilyas.ece@gmail.com

Abstract: The provided source highlights a practical application of IoT (Internet of Things) technology, specifically in the realm of financial transaction monitoring and management conducted over the internet. This advanced automation system incorporates a diverse range of sophisticated devices, all accessible through a user-friendly interface. These devices can establish connections with a high-level automation network through a web-based interface and are also compatible with low-power communication technologies such as Zigbee and remote systems. The primary goal of this initiative is to facilitate the control of commercial machinery by leveraging mobile devices connected to Wi-Fi networks. Customers are granted seamless interaction with these devices through a user-friendly web interface that is readily accessible via the internet. With this system, users can effortlessly manage various devices including lighting, fans, and door locks, all through a straightforward web page. Additionally, the system features a notification capability that enables the transmission of messages and images via remote control, enhancing communication between users and the system. Experts are available to collaborate with clients, working together to design customized device configurations tailored to their specific requirements. Clients have the flexibility to choose from a selection of available tools based on their interactions with these specialists. In situations where the online connection experiences disruptions or the specialist is unavailable, the system seamlessly transitions to onboard control, allowing the devices to function locally. This technology offers the potential to deliver a scalable and cost-effective business automation solution.

Keywords. Arduino, NodeMCU, LDR Sensor, Lm35.

1. INTRODUCTION

The implementation of Industry 4.0 involves the connectivity of a company's assets to the internet, allowing for the collection of vast amounts of data that can be used to develop new services and products aimed at enhancing business productivity and efficiency. This transformation relies on the integration of Cyber-Physical Systems (CPS), complemented by Internet of Things (IoT) technologies and artificial intelligence methods. IoT plays a crucial role in the digitization of products and resources by deploying small internet-connected sensors throughout the system. Controlled process systems (CPS) manage and oversee system control by seamlessly integrating both hardware and

International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 10, October-2023, http://ijmec.com/, ISSN: 2456-4265

software components within a collaborative networked environment. As organizations exchange substantial amounts of data across various locations, the importance of adhering to cybersecurity standards becomes paramount.

According to a report published by McKinsey, the expansion of the Internet of Things (IoT) also amplifies the risk of cyberattacks. Previously, cyber risks were confined to the realm of information technology (IT); however, they now pose a significant threat to production systems.

Nonetheless, Cisco's 2018 Annual Cybersecurity Report reveals that this investment may still be insufficient, with 83% of IoT devices remaining vulnerable to attacks. Alarmingly, 53% of reported incidents resulted in damages exceeding USD 500,000. The cornerstone of security lies in the CIA triad, encompassing Confidentiality, Integrity, and Availability. These three principles must always be addressed in discussions regarding security.

These three pillars provide a framework for designing the security infrastructure of an organization. It is imperative to safeguard data confidentiality by preventing unauthorized access, maintain data integrity by averting unauthorized alterations or deletions, and ensure data availability, providing timely access when needed.

Despite IoT's significant impact in these fields, security is often a secondary consideration during the deployment of such solutions. This paper aims to analyze vulnerabilities within a widely recognized security mechanisms. The study examines two unrelated case studies—one based on building automation and the other on factory automation. By identifying vulnerabilities and implementing straightforward protective measures, the paper enhances system security by safeguarding against common types of attacks.

The paper's structure consists of the following sections: Section II discusses the implications of IoT adoption for security. Sections III and IV present two case studies based on Internet of Things applications, including security risk analysis and recommended mitigation procedures. Section V explores the key findings and their applicability to other IoT-involved fields, accompanied by lessons learned. Finally, the study concludes in the last section, highlighting areas for further research.

2. SYSTEM HARDWARE

Objective

The primary goal of this project is to develop a system for controlling and monitoring office automation processes using Internet of Things (IoT) technology within a building and during business operations.

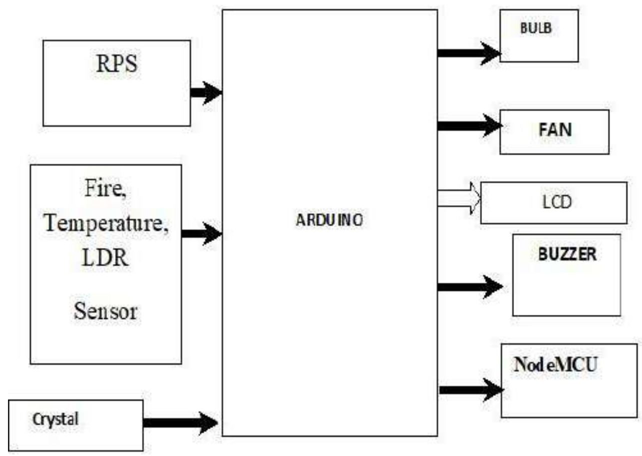
Implementation

This task can be accomplished using various hardware components such as Arduino Uno, NodeMcu, and locally available controllers designed for commercial applications.

Project Description

This project aims to establish a robust IoT-based solution for monitoring and managing financial operations by leveraging the extensive internet connectivity available in the field. The user interface of this automation system comprises fixed devices that can interface with the financial automation network via a web portal. Additionally, it utilizes low-power communication methods like Zigbee and wireless technology. Consequently, users have the ability to control business machinery through their mobile phones, utilizing wireless communication and NodeMcu as a communication hub. In this setup, stakeholders can interact with the system as a whole through a web-based interface.

BLOCK DIAGRAM



3. RELATED WORK

Several studies in the field concur that the existing Building Automation (BA) technologies are vulnerable to various forms of attacks. For instance, Gasser et al. conducted an analysis of BACnet, revealing that over 14,000 devices could potentially be exploited for amplification attacks, a type of Denial of Service (DoS) attack.

Another noteworthy contribution comes from Meyer et al., who investigated potential attack vectors within building automation. They explored the possibility of gaining access to local networks through online device service providers, infiltrating user devices, or compromising data stored with service providers. This research is particularly relevant in today's context with the introduction of new devices like wearables, smartwatches, fitness trackers, and mobile phones.

Ravi M. and their co-authors, in their 2015 research, highlight the growing interest in automation and the utilization of wireless communication systems, which have enhanced the sophistication and effectiveness of the systems. In their setup, when an anomaly is detected within a designated area, the local network dispatches an SMS to a pre-defined mobile recipient, extending the reach of the system. The use of a Raspberry Pi as a central station is considered standard practice, given its ARM eleven CPU and advanced connectivity features, including Ethernet. All system components are meticulously designed to seamlessly integrate with the Wireless Sensor Network (WSN), enabling the collection of data and transmission to a centralized master chamber while maintaining LAN connectivity for concealed operations. Sensor Nodes employing ZigBee within the wireless network emerge as crucial components in the future landscape of healthcare systems.

Their research introduces a smartphone-based physiological monitoring device capable of accurately displaying a patient's vital signs, including pulse and blood pressure, within a working environment. The entire system connects to a central location to gather the patient's physiological data comprehensively. An organizational network is employed to collect data transmitted from the gateway location, establishing a connection between the server and the organizational network point. This setup facilitates direct patient monitoring in their chamber, enabling medical professionals to make timely decisions regarding various medical conditions prevalent in the region.

In another study conducted by Keerthi VallapReddy and colleagues in 2014, they propose a comprehensive license plate recognition system with detailed design considerations. Their system is focused on consistently capturing license plate images from vehicles during authorization processes. These legitimate components are processed using the Raspberry Pi CPU for verification. The system goes beyond mere recognition as it detects unauthorized plate snapshots using a signal-generated device. When an authorized vehicle is identified, the system activates a DC motor to execute the associated task, typically involving access control.

The article emphasizes the significance of automation in the field of device research, highlighting the disruptive impact of automation on various aspects of the research domain. Their approach employs a preconfigured personal computer, often referred to as the Raspberry Pi processor, as the central focus of their system. Within this computer, users can efficiently interact with results and input modules that play a pivotal role throughout the research evaluation.

Fabio Leccese and his colleagues, in their 2014 article, have identified and examined a clever urban application. The paper delves into the controlled management of streetlights, introducing innovative advancements in the field. Their meticulously designed system utilizes a layered approach to efficiently oversee streetlights, combining local operations for immediate control and long-distance coordination.

In this system, each streetlight in close proximity is equipped with an electronic card for administrative purposes and a ZigBee connection. The network of these interconnected streetlights relays data to a central control unit, responsible for the holistic management of the urban lighting network. Impressively, the cost-effective central control unit is powered by a Raspberry Pi control card, offering substantial computing capabilities.

This concept aligns with the concept of a "smart city," reimagining traditional urban planning. It envisions the possibility of identifying and nurturing demand-driven systems that integrate surveillance and automation features, leveraging fast-evolving technologies and their interconnected components commonly employed in various applications.

Furthermore, this system considers the energy-efficient aspect of public lighting systems. By incorporating new lighting technologies, it seeks to create previously unimaginable energy savings and cost reductions. To facilitate remote control of this intelligent system, a WiMAX connection was evaluated and implemented, effectively eliminating the spatial limitations traditionally associated with buses in this context.

ISSN: 2456-4265

DOI: https://doi-ds.org/doilink/10.2023-93264496

Overall, this innovative urban system has undergone multiple evaluations and studies since its inception, highlighting its significance in the field of urban planning and infrastructure management.

In recent years, embedded systems have gained increasing importance, especially for handling specific tasks that may be overlooked by more complex solutions. One notable aspect of these systems is the incorporation of multimedia elements. In today's society, tasks like sending messages, managing various types of multimedia content, streaming multimedia, and interfacing with the physical environment have become quite common. This is particularly crucial when it comes to evaluating, managing, and monitoring targeted locations using multimedia devices, serving various purposes related to security and assurance.

This article introduces a method for capturing video and still images of moving objects, utilizing open-source development tools (specifically Raspbian, a Linux variant) and a programming language (Python). The device's effectiveness is enhanced by employing advanced sensors, allowing it to capture distinct real-world features from a specific location over a predefined period. The collected data is then uploaded to the internet and can be accessed through a dedicated webpage. Moreover, the camera can be controlled via a web-based interface, offering a wide range of control options thanks to its Python-based programming. All of these functionalities are inherent to the device itself.

In a study conducted by V. Ramanath and colleagues in 2015, the focus shifts from the conventional method of using keys to start a car to a novel approach centered on facial recognition technology. Facial recognition is an evolving and lucrative field, continually advancing in capabilities. The method, known as "face recognition," involves the verification of the identity of the car's legitimate users by searching an established database for their facial features. When a customer approaches the vehicle, their facial image is compared to those stored in the reference database. If a match is found, access to the car is granted; otherwise, individuals without a match in the database are given some time before being allowed access to the vehicle. This system employs Haar cascades for object detection and utilizes prominent feature analysis for facial recognition. Notably, this system was implemented using a cost-effective piece of hardware, the Raspberry Pi microcontroller, specifically equipped with the ARM1176JZF-S CPU. The primary objective of this Raspberry Pi-based system is to manage both still images and video, enabling swift facial recognition.

These IoT-based systems offer efficient solutions for monitoring and controlling environmental factors, providing advantages such as real-time data accessibility and public involvement in pollution management endeavors. They harness contemporary technology to develop cost-effective and reliable monitoring solutions.

The Automated Air & Sound Control device represents a significant advancement in addressing a critical threat to environmental well-being. It effectively tackles the challenges posed by highly polluted areas, offering support for modern technology and promoting a healthier lifestyle. Notably, this device allows individuals to monitor pollution levels via mobile applications on their smartphones. To implement this system, sensor devices must be strategically deployed within the environment to collect and analyze data. By deploying these sensor devices, real-world interaction with the environment becomes possible, allowing them to communicate with other devices through the network. Subsequently, the collected data and analysis results are made available to end-users through wireless means. This data plays a crucial role in addressing issues related to the impact of idling vehicles on air quality, such as anticipating air quality changes at traffic signals. Furthermore, it enables real-time monitoring of carbon monoxide (CO) concentration in specific areas, and this data can be accessed from various mobile communication devices, including PDAs, smartphones, and tablet computers, contributing to maintaining air quality under control.

This paper introduces a network designed for monitoring air quality, both indoors and outdoors. The sensors' responses are influenced by factors like temperature, humidity, and the cross-effects of other gases. Two data processing architectures have been implemented for calculating several air quality parameters, utilizing JavaScript and LabVIEW Web Publisher technology. A key innovation is the application of a neural network algorithm within an embedded server (web sensor), while the other architecture operates on a local computer. The latter architecture handles tasks such as data analysis from sensor nodes via TCP/IP remote control, detecting pollution events, estimating gas concentrations using neural network inverse models, and logging air quality data, which is then published on the web.

The proposed portable device incorporates embedded sensors installed on various subjects, such as vehicles, individuals, or animals. This device utilizes innovative polymer-modified tuning fork sensors for data collection and delivery. It includes sample conditioning with interference removal and air zeroing capabilities, rendering it a standalone and portable unit. Ambient air is drawn into the device through either particle filters (for detection mode) or zero filters (for calibration mode). The filtered air undergoes sample conditioning through interference removal before being delivered to the tuning fork sensors inside a sensor cartridge. The responses of these sensors are digitized and wirelessly transmitted to a user interface device, such as a mobile phone or a less portable device like a computer. Bluetooth technology is employed for wireless communication, offering flexibility in choosing the user interface.

In this research, a vehicular wireless sensor network (VSN) architecture is proposed for monitoring microclimates based on GSM short messages and vehicle location data. The prototype includes vehicles equipped with CO2 sensors, GPS receivers, and GSM modules, forming a ZigBee-based intra-vehicle wireless network. Each vehicle serves as a vehicular sensor, roaming within the area of interest and periodically reporting sensed data via GSM short messages. The collected data is then processed by a server that utilizes Google Maps to visualize the results.

The Wi-Fi Sensor Network Air Pollution Monitoring System (WAPMS) consists of sensor nodes and a communication device that facilitates data transmission to a server. Sensor nodes autonomously collect data, which is then transmitted to one or more base stations and subsequently forwarded to a sensor network server. The system also allows for remote commands to be sent to the nodes to fetch data, as well as autonomous data transmission. The development of this system aims to assist government authorities in establishing an air pollution indexing system.

The paper introduces MAQS (Mobile Air Quality Sensing), a personalized mobile sensing system designed for indoor air quality (IAQ) monitoring. MAQS estimates IAQ components based on human activity, such as CO2 and contagious viruses, using CO2 levels, and other factors like volatile organic compounds (VOCs) using air exchange

DOI: https://doi-ds.org/doilink/10.2023-93264496

rates. MAQS combines smartphones and portable sensing devices to deliver personalized and energy-efficient IAQ data.

In the proposed work, a MiCS-oz47 sensor is used to measure ozone concentration in the environment by analyzing the sensor's tin dioxide (SnO_2) layer's resistance. Digital communication is established through the board's RS232-TTL interface, directly connected to an HTC Hero smartphone with a USB Mini-B port. This research demonstrates the possibility of using gas sensors to create comprehensive high-resolution air pollution maps, a crucial aspect of participatory sensing devices.

One significant concern in such networks is ensuring strong performance, as gas sensors consume significant power, and sensor nodes must operate unattended for extended periods on battery power.

The system consists of multiple distributed monitoring stations communicating wirelessly with a backend server via machine-to-machine communication. Each station is equipped with gaseous and meteorological sensors, data logging capabilities, and Wi-Fi communication. The backend server collects real-time data from these stations and converts it into information accessible to users through web portals and mobile applications. Data collected over four months is analyzed and evaluated for performance.

Taewoon Kim and J. Morris Chang have explored power-saving mechanisms for 802.11 in large-scale sensor networks. They propose a method for selectively and dynamically changing node memberships and rearranging traffic to maximize sleeping intervals without causing data delivery delays. Their approach also involves utilizing unused Association Identifiers (AIDs) to reduce unnecessary wake-ups and conserve power in battery-operated sensor devices.

Hsueh-Chun Lin and colleagues Their WSN gateway design incorporates functions such as serial listening, transaction logging, and internet listening, enabling analog and digital signal conversion, data classification, threshold determination, database redundancy, and mobile communication.

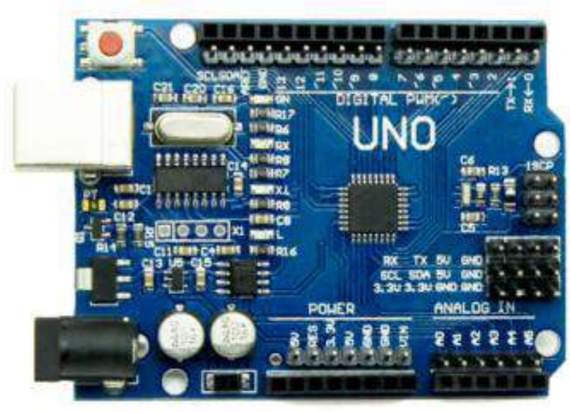
Sk Riyazhussain and team elucidate a Raspberry Pi-controlled Traffic Density Monitoring System. Raspberry Pi is employed for traffic surveillance, continuously monitoring and recording traffic conditions. It also detects traffic density and provides real-time traffic reports to travelers. Additionally, the system includes screens for public display, which can serve advertising purposes. Raspberry Pi facilitates managing advertising preferences and displaying traffic reports.

Shailendra Singh and colleagues They utilize the Yuktix IOT hardware platform, sensor nodes, and a Central Data Acquisition Unit (CDAU) to monitor greenhouse conditions locally or remotely. The system incorporates Yuktix cloud, web applications, Android applications, and controllers for environmental control.

Xuan-Thuan Nguyen and team address the reliability of sustained data delivery in Wireless Multimedia Sensor Networks (WMSNs), even in the presence of environmental noise. They introduce a reliable transport protocol (RTP) combining automatic repeat request error control with error correction mechanisms. Experimental results on Raspberry Pi compute modules and Atmel transceivers demonstrate RTP's ability to successfully transfer data over a wide range of transmission rates and distances.

International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 10, October-2023, http://ijmec.com/, ISSN: 2456-4265

4. ARDUINO



Overview:

The Arduino Uno is a microcontroller board subject to the ATmega328 (datasheet). It has 14 motorized data/yield pins (of which 6 can be utilized as PWM yields), 6 essential wellsprings of information, a 16 MHz artistic resonator, a USB alliance, a power jack, an ICSP header, and a reset catch. It contains everything expected to help the microcontroller; just interface it to a PC with a USB association or power it with an AC-to-DC connector or battery to begin.

The Uno contrasts from every first board in that it doesn't utilize the FTDI USB-to-back to back driver chip. Or on the other hand possibly, it joins the Atmega16U2 (Atmega8U2 up to change R2) adjusted as a USB-to-successive converter.

The Uno board has a resistor dismantling the 8U2 HWB line to ground, making it less mind boggling to put into DFU mode.

The board has the going with new highlights:

pinout: included SDA and SCL pins that are close to the AREF stick and two other new sticks set close to the RESET stick, the IOREF that engage the shields to adapt to the voltage gave from the board. In future, shields will be extraordinary with both the board that uses the AVR, which works with 5V and with the Arduino Due that works with 3.3V. The resulting one is a not related stick, that is set something aside for future purposes.

- Stronger RESET circuit.
- Atmega 16U2 uproot the 8U2.

"Uno" suggests one in Italian and is named to check the top tier section of Arduino 1.0. The Uno and structure 1.0 will be the reference changes of Arduino, pushing ahead. The Uno is the most recent in a development of USB Arduino sheets, and the reference model for the Arduino compose; for an examination with past structures, see the archive of Arduino sheets.

5 NODEMCU

WI-FI: The WI-FI module used in this project is ESP8266. It follows TCP/IP stack and is a microchip which is less

DOI: https://doi-ds.org/doilink/10.2023-93264496

in cost. This microchip allows microcontroller to connect to a WI-FI network, by using Hayes style command connections are done or made through TCP/IP connection. ESP8266 has 1MB of built in flash, single chip devices able to connect WI-FI. Espressif systems are the manufacturers of this module, it is a 32 bit microcontroller. There are 16 GPIO pins in this module. This module follows RISC processor. It has 10 bit DAC. Later Espressif systems released a software development kit(SDK) which is used to programme on the chip, so that another microcontroller is not used. Some of the SDK's are Node MCU, Arduino, Micro Python, Zerynth and Mongoose OS. SPI, I2C, I2S, UART are used for communicating between two sensors or modules.

Figure : Wi-Fi module

6. IoT Technology and Applications

IoT development speedily assist the IoT application that focused on the heap industry and specific users, while networks and devices allow connectivity of physical things. IoT application gives reliable vital device-to-human and device-to-device communication. IoT device applications need to ensure that information is received and properly acted according to a suitable specific way, a simple example is that of logistic application monitoring that has the transported status of goods such as organic products, fresh products, meat and dairy terms. Furthermore, during logistics, quality control of climate change, shock and humidity is regularly monitored and suitable movements are strategically and naturally made to preserve goods spoilage from a long distance when connection is out of courage. To claimed that "some examples of IoT applications in existence can be found in Smart Environment, Smart Greenhouse, Smart Cities, Smart Water, Smart Metering, Security and Emergency, Industrial Control, Home Automation and Electronic Health". 'IoT' is therefore stationed on devices that can examine sensed data and then transmit it to the user. K. IoT Challenges As stated in a previous study, there are some challenges that IoT design would face in the coming future generation. All the devices, nodes connected in associate in nursing IoT design needs to have terribly low latency over reliable links. Because of the vast variety of IoT devices and the use of various frequency bands, there would be a crisis in spectrum house. Although IoT devices are expanding on a daily basis that consumes terribly lesser power, still there'll be a big quantity of greenhouse gas emission because of all of these devices. Finally, IoT architecture not solely must be price effective however additionally they have to be capable of supporting heterogeneous applications and devices. As stated above on IoT challenges, IoT applications

International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 10, October-2023, http://ijmec.com/, ISSN: 2456-4265

will have some more basic needs to tackle, for example, Device addressing, Security, Scalability, Mobility, Anchor-less sending and so on. As mentioned, IoT applications contains numerous heterogeneous devices, and however, content security is a key concern that plays a great roles. A previous study has indicated the challenges of both IoT and ICN in their past study, this past study endeavours to combine them where IoT illustrate the different challenges and on the other hand, ICN illustrates the positive solutions. Nonetheless, their study explained initially how different ICN features can address IoT issues and after that, some use cases and contextual investigations are examined

7. LIMITATIONS

The system has following limitations:

1. **Compatibility**: As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.
2. **Complexity**: There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That leaves you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when it requires a single cartridge.
3. **Privacy/Security**: Privacy is a big issue with IoT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the work place or with your friends.
4. **Safety**: There is a chance that the software can be hacked and your personal information misused. The possibilities are endless. Your prescription being changed or your account details being hacked could put you at risk. Hence, all the safety risks become the consumer's responsibility.

8. CONCLUSION

In today's context, there is a pressing need for electronic solutions. We are proactively utilizing cameras to monitor various situations in advance. Within our organization, we have integrated the Internet of Things (IoT) to streamline operations and empower individuals to take timely and effective actions. This approach is aimed at reducing manual intervention. Sometimes, delays in responding to situations can lead to property damage and even endanger lives. Therefore, we are promoting the advancement of automation through the integration of the Internet of Things (IoT) and artificial intelligence (AI) to enable the system to make critical decisions.

9. Future Prospects

Looking ahead, our focus will be on developing more intricate attack scenarios by building upon the foundational ones currently under development. We will also consider implementing more sophisticated defense mechanisms. For instance, one avenue of exploration involves the use of machine learning algorithms to identify patterns in agent interactions and potential threats.

ISSN: 2456-4265

DOI: https://doi-ds.org/doilink/10.2023-93264496

REFERENCES

[1] Qingping chi, Hairongyan, chungzhang, zhibo pang, Li Da Xu Senior member,(2014) , “A reconfigurable smart sensor interface for industrial WSN in IOT environment”, IEEE transactions on industrial informatics, vol. 10, no. 2, 2014.

[2] MihaiT.Lazerescu,, “A design of WSN for long term environmental monitoring”, ”IEEE J.Emerg.Sel. Topics Circuits Syst., vol. 3, no. 1, pp. 45– 54, Mar. 2013.

[3] CharalamposDoukas and IliasMaglogiannis , “Bringing IoT and Cloud Computing towards Pervasive Healthcare”, Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012.

[4] Lihong Jiang, Li Da Xu, HongmingCai, Zuhai Jiang, Fenglin Bu , An IoT-Oriented Data Storage Framework in Cloud Computing Platform, IEEE Transactions On Industrial Informatics, vol. 10, no. 2, 2014.

[5] George Suciu, SimonaHalunga, AlexandruVulpe, Victor Suciu , “Generic Platform for IoT and Cloud Computing Interoperability Study”, IEEE Transactions On Industrial Informatics vol. 10, no. 1, 2013.

[6] Yuan Jie Fan, Yue Hong Yin , IEEE, Li Da Xu, Senior Member, IEEE, Yan Zeng, and Fan Wu “IoT-Based Smart Rehabilitation System”, IEEE Transactions On Industrial Informatics, vol. 10, no. 2, 2014.

[7] YingLeng and LingshuZhao, “Novel design of intelligent internet-ofvehicles management systems based on cloud- computing and internet-ofthings”, International Conference on Electronic & Mechanical Engineering and Information Technology, 2011.

[8] Chengen Wang Zhuming Bi Li Da Xu , “IoT and Cloud Computing in Automation of Assembly Modeling Systems” IEEE Transactions On Industrial Informatics, vol. 10, no. 2, 2014.

[9] Cui Wenshun, Yuan Lizhe, CuiShuo and Shang Jiancheng ,“Design and Implementation of Sunlight Greenhouse Service Platform Based on lOT and Cloud Computing” 2nd International Conference on Measurement, Information and Control, 2013.

[10] Lodhi, Amairullah Khan, M. S. S. Rukmini, Syed Abdulsattar, and Shaikh Zeba Tabassum. "Performance improvement in wireless sensor networks by removing the packet drop from the node buffer." Materials Today: Proceedings 26 (2020): 2226-2230.

[11] Lodhi, Amairullah Khan, and Syed Abdul Sattar. "Cluster head selection by the optimized ability to restrict packet drop in wireless sensor networks." In Soft Computing in Data Analytics, pp. 453-461. Springer, Singapore, 2019.

[12] Lodhi, Amairullah K., M. Santhi S. Rukmini, and Syed Abdulsattar. "Energy-efficient routing protocol for network life enhancement in wireless sensor networks." Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science) 14, no. 3 (2021): 864-873.

[13] Ketki Ram Bhakre, R. K. Krishna ”Distance Distribution Approach of Minimizing energy Consumption in Grid W3ireless sensor network" in the International Journal of Engineering and Advanced Technology (IJEAT), Volume1, Issue5, June 2011.

ISSN: 2456-4265

DOI: https://doi-ds.org/doilink/10.2023-93264496

[14] Lodhi, Amairullah Khan, M. S. S. Rukmini, and Syed Abdulsattar. "Energy-efficient routing protocol based on mobile sink node in wireless sensor networks." International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN (2019): 2278-3075.

[15] Lodhi, Amairullah Khan, M. S. S. Rukmini, and S. Abdulsattar. "Energy-efficient routing protocol for node lifetime enhancement in wireless sensor networks." Int J Adv Trends Comput Sci Eng 8, no. 1.3 (2019): 24-28.

AUTHOR PROFILE

Mr. Muzaffar Ali Mohammad, M.Tech student in ECE (Embedded Systems) from Shadan College of Engineering And Technology, Peerancheru, Telangana.

Dr. Rajesh Reddy Gade, Assistant Professor, Dept. of ECE from Shadan College of Engineering and Technology, Peerancheru, Telangana.

Dr. MOHAMMAD ILIYAS, HOD & PROFESSOR, Dept. of ECE from Shadan College of Engineering and Technology, Peerancheru, Telangana.