Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 1): pp. 8138-8147
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.836

Design Of Encrypted Digitally For Fol & Eol Manufacturing Sectors

1 S.Rajendran , 2 K. Sudha , 3 M. Kumaran , 4. V.Seedha Devi , 5 D. Balasubramaian

1. Professor, Department of Mechanical Engineering, Jaya Engineering College Chennai 602024,INDIA.
2. Assistant Professor, Department of Computer Science and Engineering, Sriram Engineering College.
3. Assistant Professor, Department of Computer Science and Engineering, Jaya Engineering College.
4. Associate Professor Department of Computer Science Engineering, Jaya Engineering College
5. Assistant Professor, Department of Master of Computer Application, Jaya Engineering College.

Email: r9551329915@gmail.com

Abstract:
Augmented Reality and Virtual Reality market has a potential to reach 151 Billion USD with a paramount CAGR of 70.4% by 2022. It is true that the AR and VR technologies have driven the gaming and entertainment industry, but it also has a very good potential to transform the healthcare industry since it actually can change a lot of traditional healthcare operations and branches in a number of ways, including radiology, oncology, training, and more. Still being at a very early stage, digital reality AR/VR technologies are helping care delivery specialists to save life and take critical decisions. Considering this potential of VR/AR, healthcare may revolutionize the way diagnostic practice is carried out to view MRI and CT images. In addition our proposal must be integrated with the AR feature for an effective notch of system.

1. Introduction

The IoT is enabled by technologies such as cybersecurity, cloud computing, edge computing, mobile technologies, machine-to-machine, 3D printing, advanced robotics, big data, the internet of things, RFID technology, and cognitive computing. Five of the most important ones are described below.

Cyber-physical systems (CPS): the basic technology platform for IoT therefore the main enabler to connect physical machines that were previously disconnected. CPS integrates the dynamics of the physical process with those of software and communication, providing abstractions and modeling, design, and analysis techniques.

Cloud computing: With cloud computing IT services and resources can be uploaded to and retrieved from the Internet as opposed to direct connection to a server. Files can be kept on cloud-based storage systems rather than on local storage devices.

Edge computing: A distributed computing paradigm that brings computer data storage closer to the location where it is needed. In contrast to cloud computing, edge computing refers to decentralized data processing at the edge of the network. The industrial internet requires more of an edge-plus-cloud architecture rather than one based on the purely centralized cloud; in order to transform productivity, products, and services in the industrial world.

Artificial intelligence and machine learning: Artificial intelligence (AI) is a field within computer science in which intelligent machines have created that work and react like humans. Machine learning is a core part of AI, allowing software to more accurately predict outcomes without explicitly being programmed. It is also possible to combine artificial intelligence with edge computing in order to provide industrial edge intelligence solutions shows on figure 1.

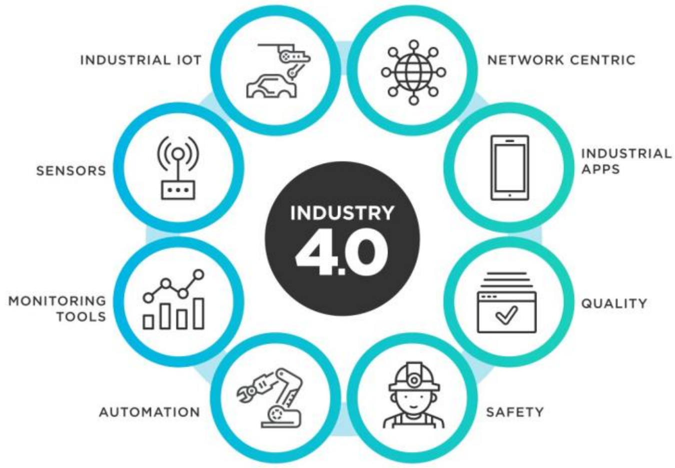

Figure 1 Industrial Internet of Things

1.2 ORGANIZATIONAL APPLICATIONS

The term Enterprise IoT refers to devices used in business and corporate settings. By Manuel Alonso-Rosa et al, it is estimated that the EIoT will account for 9.1 billion devices.

Medical and healthcare

The Internet of Medical Things is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring.The IoMT has been referenced as "Smart Healthcare", as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids.Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses.

Rosalino Rodriguez Calderon et al, Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost."Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used analysed health statistics."

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people to regain lost mobility via therapy as well.These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyse valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems.

IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behaviour. This can lead to more accurate underwriting and new pricing models.

The application of the IoT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and applying complex algorithms in health data analysis.

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication,smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance.

2. INDUSTRIAL APPLICATIONS

Also known as IIoT, industrial IoT devices acquire and analyse data from connected equipment, operational technology (OT), locations, and people. Combined with operational technology (OT) monitoring devices, IIoT helps regulate and monitor industrial systems. Also, the same implementation can be carried out for automated record updates of asset placement in industrial storage units as the size of the assets can vary from a small screw to the whole motor spare part, and misplacement of such assets can cause a percentile loss of manpower time and money.

Manufacturing

The IoT can connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control allow IoT to be used for industrial applications and smart manufacturing. IoT intelligent systems enable rapid manufacturing and optimization of new products, and rapid response to product demands.

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IIoT. IoT can also be applied to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability.Industrial management systems can be integrated with smart grids, enabling energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by networked sensors.

Agriculture

There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce the effort required to manage crops. For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs. The overall goal is that data from sensors, coupled with the farmer's knowledge and intuition about his or her farm, can help increase farm productivity, and also help reduce costs.

Subramani Roy Choudri et al,, Toyota Tsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyse the number of fish, and deduce the effectiveness of water flow from the data the fish provide. The Farm Beats projectfrom Microsoft Research that uses TV white space to connect farms is also a part of the Azure Marketplace now.

INFRASTRUCTURE APPLICATIONS

Monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks and on- and offshore wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. The IoT can benefit the construction industry by cost-saving, time reduction, better quality workday, paperless workflow and increase in productivity. It can help in taking faster decisions and save money with Real-Time Data Analytics. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

Energy management

Significant numbers of energy-consuming devices (e.g. lamps, household appliances, motors, pumps, etc.) already integrate Internet connectivity, which can allow them to communicate with utilities not only to balance power generation but also helps optimize the energy consumption as a whole.

The smart grid is a utility-side IoT application; systems gather and act on energy and power-related information to improve the efficiency of the production and distribution of electricity.Using advanced metering infrastructure (AMI) Internet-connected devices, electric utilities not only collect data from end-users, but also manage distribution automation devices like transformers.

Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions,and can even include areas like monitoring the movements of wildlife and their habitats.

Development of resource-constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile.It has been argued that the standardization that IoT brings to wireless sensing will revolutionize this area.

3. MILITARY APPLICATIONS

The Internet of Military Things (IoMT) is the application of IoT technologies in the military domain for the purposes of reconnaissance, surveillance, and other combat-related objectives. It is heavily influenced by the future prospects of warfare in an urban environment and involves the use of sensors, munitions, vehicles, robots, human-wearable biometrics, and other smart technology that is relevant on the battlefield.

Internet of Battlefield Things

The Internet of Battlefield Things is a project initiated and executed by the U.S. Army Research Laboratory (ARL) that focuses on the basic science related to the IoT that enhance the capabilities of Army soldiers. Avni Sharma et al, ARL launched the Internet of Battlefield Things Collaborative Research Alliance , establishing a working collaboration between industry, university, and Army researchers to advance the theoretical foundations of IoT technologies and their applications to Army operations.

Ocean of Things

The **Ocean of Things** project is a DARPA-led program designed to establish an Internet of things across large ocean areas for the purposes of collecting, monitoring, and analysing environmental and vessel activity data. The project entails the deployment of about 50,000 floats that house a passive sensor suite that autonomously detect and track military and commercial vessels as part of a cloud-based network.

4. PRODUCT DIGITALIZATION

There are several applications of smart or active packaging in which a QR code or NFC tag is affixed on a product or its packaging. The tag itself is passive, however, it contains a unique identifier which enables a user to access digital content about the product via a smartphone. Strictly speaking, such passive items are not part of the Internet of things, but they can be seen as enablers of digital interactions.

Network architecture

The Internet of things requires huge scalability in the network space to handle the surge of devices. With billions of devices being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport.

Decentralized IoT

Decentralized Internet of things, or decentralized IoT, is a modified IoT. It utilizes Fog Computing to handle and balance requests of connected IoT devices in order to reduce loading on the cloud servers, and improve responsiveness for latency-sensitive IoT applications like vital signs monitoring of patients, vehicle-to-vehicle communication of autonomous driving, and critical failure detection of industrial devices.

Size considerations

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects. Jonathan J Hull et al, there were already 83 million smart devices in people's homes. This number is expected to grow to 193 million devices by 2020.The figure of online capable devices grew 31% from 2016 to 2017 to reach 8.4 billion.

Space considerations

In the Internet of things, the precise geographic location of a thing and also the precise geographic dimensions of a thing will be critical.Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information or decide to not take the action.

Social Internet of things

Social Internet of things (SIoT) is a new kind of IoT that focuses the importance of social interaction and relationship between IoT devices.SIoT is a pattern of how cross-domain IoT devices enabling application to application communication and collaboration without human intervention in order to serve their owners with autonomous services,and this only can be realized when gained low-level architecture support from both IoT software and hardware engineering.

Social Network for IoT Devices

IoT defines a device with an identity like a citizen in a community, and connect them to the internet to provide services to its users. SIoT defines a social network for IoT devices only to interact with each other for different goals that to serve human.

Social IoT Challenges

Internet of things is multifaceted and complicated.One of the main factors that hindering people from adopting and use Internet of things (IoT) based products and services is its complexity.Installation and setup is a challenge to people, therefore, there is a need for IoT devices to mix match and configure themselves automatically to provide different services at different situation.

R. Silva et al, System security always a concern for any technology and it is more crucial for SIoT as not only security of oneself needs to be considered but also the mutual trust mechanism between collaborative IoT devices from time to time, from place to place. Another critical challenge for SIoT is the accuracy and reliability of the sensors. At most of the circumstances, IoT sensors would need to respond in nanoseconds to avoid accidents, injury, and loss of life.

Data storage

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks.These networks share data among sensor nodes that are sent to a distributed system for the analytics of the sensory data.

Another challenge is the storage of this bulk data. Depending on the application, there could be high data acquisition requirements, which in turn lead to high storage requirements. Currently the Internet is already responsible for 5% of the total energy generated, and a "daunting challenge to power" IoT device to collect and even store data still remains.

Security

Security is the biggest concern in adopting Internet of things technology,with concerns that rapid development is happening without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary.

The Mirai Botnet had singled out specific IoT devices that consisted of DVRs, IP cameras, routers and printers.Top vendors that contained the most infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik**.** Pranav Bedekar et al, a Computer Scientist at Cloud flare noted that native DDoS vulnerabilities exist in IoT devices due to a poor implementation of the Publish–subscribe pattern.These sorts of attacks have caused security experts to view IoT as a real threat to Internet services.

Seonghun Park et al, the Washington Post wrote an article regarding the security and ethical challenges that can occur with IoT doorbells and cameras: "Last month, Ring got caught allowing its team in Ukraine to view and annotate certain user videos; the company says it only looks at publicly shared videos and those from Ring owners who provide consent. Just last week, a California family's Nest camera let a hacker take over and broadcast fake audio warnings about a missile attack, not to mention peer in on them, when they used a weak password"

IOT ADOPTION BARRIERS

Despite a shared belief in the potential of the IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Mike Farley argued in Forbes that while IoT solutions appeal to early adopters, they either lack interoperability or a clear use case for end-users.

A study by Ericsson regarding the adoption of IoT among Danish companies suggests that many struggle "to pinpoint exactly where the value of IoT lies for them".

5. RESULTS AND DISCUSSION

To begin with, testing of the model from the IoT part, we have used BLYNK IoT platform. In which, we just made a simple BLYNK project of adding a button in the dashboard which will send data 0 & 1 to virtual pin V1

After that, we have made a code in which, if we receive the data 1 from pin V1, we just send the signal high to digital pin of ESP8266 from Expressif flavor NodeMCU IoT development board which ultimately turns on Relay. And as soon as we receive 0 the relay gets turned off shows on the figure 2.

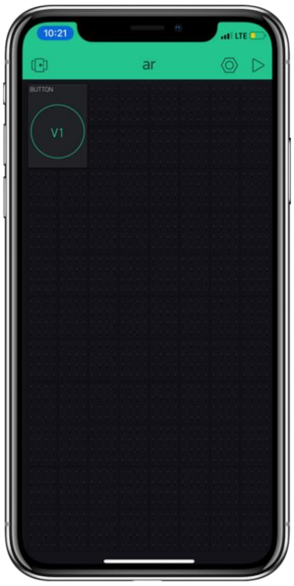

Figure 2 Mobile Blynk User Interface

AR PART OF PROJECT

For AR, we will be using Unity Hub software on our computer, There are lot of steps involved in setting up our Unity Hub software. The primary step is attach Vuforia Engine with our project. It act as a Virtual camera with 3D visual effects. And a C# script is required to handle the environment which is used to get interfaced with the outside world from computing platform of Blynk IoT.

Finally we need to make the GUI perpendicular to the screen for creating a virtual environment and the last step is to get the license from the Vuforia cloud server to access the real world with virtual environment

CONCLUSION

This project provided as brief proposal on the upgrading the system of EOL and FOL process of the industrial assembly sectors with proper usage of manpower resource algorithm and trading algorithm with advanced data science integration from ML and DL. It in turn can reduce the workmanship of industries by precise data collection and effective use of material resource. The AI integrated digital scaling system provided a proper prediction of share values investments of the company. We have suggested lot of advanced concepts behind augmented reality and artificial intelligence to make the process unique and systemized. This system can be applicable to all production and assembly sectors of industries for effective use of resource in turn help the massive growth of company in "E Tendering" Process.

REFERENCE:

1. Manuel Alonso-Rosa, Aurora Gil-de-Castro, Antonio Moreno-Munoz, Joaquin Garrido-Zafra, Elena Gutierrez-Ballesteros and Eduardo Canete-Carmona IEEE "An IoT Based Mobile Augmented Reality Application for Energy Visualization in Buildings Environments" [Vol: 0008 – 37231 © 2019]
2. Rosalino Rodriguez Calderon, Rafael Santillana Arbesu, IEEE "Augmented Reality in Automation", [Vol: 0002 – 30561 © 2015]
3. Mikko Kyto, Barrett Ens, Thammathip Piumsomboon, Gun A. Lee, Mark Billinghurst, IEEE "Pinpointing: Precise Head-and Eye-Based Target Selection for Augmented Reality", [Vol: 0001 – 4530620 © 2018]
4. Avni Sharma, Rinkesh Patel, IEEE "Home Automation Using Augmented Reality", [Vol: 0002 – 32031 © 2017]
5. R. Silva, J. C. Oliveria, G. A. Giraldi , IEEE "Introduction to Augmented Reality", [Vol: 0004 – 132341 © 2009]
6. Pranav Bedekar, Snehal Nargundi, IEEE "A Review on Home Automation using Augmented Reality",[Vol: 0012 – 105861 © 2016]
7. Seonghun Park, Enok Weshnly, Badin Rikhav, Morey Sushwat IEEE, "Development of an Online Home Appliance Control System Using Augmented Reality and an SSVEP-Based Brain–Computer Interface, Creative Commons Attribution", [Vol: 0009 – 202531 © 2019]
8. Jonathan J Hull, Berna Erol, Jamey Graham, Qifa Ke, Hidenobu Kishi, Jorge Moraleda, Daniel G Van Olst, IEEE "Paper–Based Augmented Reality"[Vol: 0009 – 3056 © 2007]
9. Subramani Roy Choudri, A. Divija , N Vijayalakshmi , P. Vamsi, IEEE "Touchless Home Automation Using Augmented Reality", [Vol: 0003 – 34620 © 2021]