Internet of Things based Gateways: Applications and Challenges

Balamurugan MS, Manojkumar R,

Abstract—Billions of data is getting connected to Internet of Things server but many a times the data is from different systems, especially in Industries a lot of data comes to same server through different gateways. Some typical applications like Healthcare, Transportation, and Smart City are looking to connect to the Internet of Things server but through a gateway of its own, which increases the complexity in system architecture. Traditional Internet of Things Gateways is used to collect the data from downstream devices connected to sensors and send it to the respective server for further processing. But however there is a need for typical heterogeneous gateways which can minimize the traffic and with presence Machine learning technologies, so the intelligence can be brought into the gateway itself for further prediction and processing. It is predicted that by 2022 the need of Internet of Thing gateways is not only to process the data stream but also apply some intelligence and if possible predict the outcomes based on the requirement, which means the Internet of Things gateway Architectures are going to be quite different from the traditional gateway architectures. Also it is important in cases like Smart Cities where there is a need of reading data from different heterogeneous devices which relies on its own architectures and network protocols like WiFi, ZigBee, LoRaWAN, Sigfox it is understood that if in case of these scenarios if there can be a single gateway which can read data from heterogeneous devices and process the data stream for further processing there can be much better understanding of data processing. This can also minimize network traffic, radiation hazards. The following work emphasizes on the need of Multi-standard gateway and relevant case studies focus on implementation of machine learning algorithm in predicting an appropriate result.

Index Terms: IoT, Gateway, MQTT, WiFi, Zigbee, Ethernet, Zephyr RTOS

I. INTRODUCTOIN

Considered to be the new buzz word in the business world but though the technology is available right from 1990's, Internet of Things(IoT) has resulted in many new business developments and new business models. This new ecosystem has given rise to a lot of M2M based communication and services. There arises a need of a standard IoT architecture reference model. There are various radio communication technologies like WiFi, Zigbee, Sigfox, LoRaWAN etc., that has been established as most preferred way of taking data from nodes to endpoints and then to an IoT server for building an Intelligence from the data[10]. But though M2M based communications are still not recognized as there is no defined standard yet that is standardized. There are lot other factors which impact the architecture design like battery power; security of IoT devices has been one of the most discussed/researched factors in IoT.

A review of the research articles indicates that a common implementation and standard is yet to be arrived on M2M implementation. This work focuses on designing an IoT based gateway and its implementation, based on survey from various models of M2M implementation. Article [1] discusses on implementation of MQTT based IoT implementation specifically focusing on ETSI standards. This work discusses on new MQTT based implementation as MQTT proxy, broker and client, which is also widely implemented in Texas Instruments CC2650 BLE and Zigbee based SoC. The work has proposed a new M2M architecture for M2M implementation in for MQTT resources and which also proposes new IoT based gateway for implementation. ETSI a standardization committee has created several working groups focusing on standardizing M2M based implementation like eHealth, transportation, smart city. With clusters of working group working on different standards to be adopted and converged to single gateway however will be the focus of this standard to be implemented.

Article [2] has proposed a new 6LoWPAN based IoT architecture that can be connected to existing IoT gateway. In this work the author has proposed to connect the data from sensor hub to through border routers to 6LoWPAN gateway which is running in a contiki based server. The contiki server is converting the 6LoWPAN data to the IPv6 data. Also in addition the WSNs are also connected to IoT Gateway.

In Article [3] the author has discussed on various aspects of security implications on the IoT architecture. The author has distinguished the security in bootstrapping phase and operation phase and the protocols that has to be considered in implementing the security. Based on the Resource constrained and heterogeneous communication the article discusses on implementing the DTLS and DoS measures in bootstrapping phase. In Operational phase the article discusses on End – End security and DTLS implementation and challenges for the same.

In article [4] authors proposes and discusses on contemporary issues of Interoperability of the IoT devices. Here basically the MQTT, CoAP and XMPP are considered to be the defacto standard by various organization in Interoperability.

A. Architectural framework of IoT

P2413 an active working group of IEEE has been working on to form a Unified architecture framework for IoT where verticals like

Revised Manuscript Received on April 18, 2019.

Balamurugan MS, School of Electronics Engineering, Vellore Institute of Technology, Chennai, India.

Manojkumar R, School of Electronics Engineering, Vellore Institute of Technology, Chennai, India.

healthcare, transportation can form a reference model for data abstraction and the quality. Also this framework has taken into consideration that includes protection, security, privacy and safety of the data. This reference model provides a generic architecture that can be integrated into multi-tired systems.

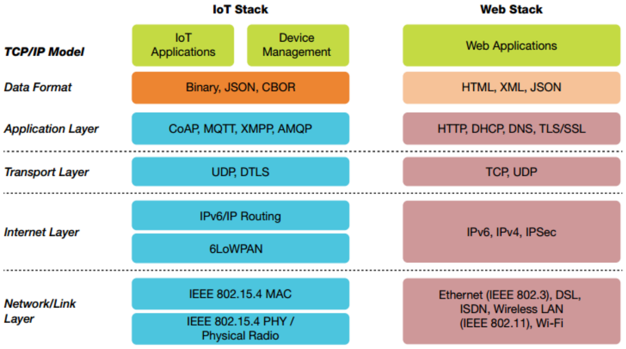
B. Security for IoT Architecture

To address the security measure MQTT's modified version has been proposed in the article [5], where a slightly modified version of MQTT suiting to MQTT-SN. Here the author has modified the existing MQTT protocol by augmenting Key/Cipher text Policy/Attribute based Encryption (KP/CP-ABE) using lightweight Elliptic Curve cryptography. In further enhancing the security article [6] proposes to enhance the communication using MQTT using a hardware that processes the transport layer security (TLS).

II. IoT Architecture

Using IoT Technologies it is quite possible to build devices which become smarter day by day, where intelligence can be brought to the nodes rather at the server end. Building IoT based architecture will involve hybrid collection physical and virtual entities. Physical things are basically collection of sensors, Microcontrollers, actuators, radio communication devices and Computer servers. Virtual Entities are that software which indulges in developing Artificial Intelligence into the data brought forward by the physical entities.

The literature work by PP Ray[11] describes in detail about IoT architecture and its various entities. In general to summarize an IoT architecture with interoperability will look out for the following characteristics: (a) Standard Interface and Protocol, (b) Public and operating (c) Open, Scalable and Flexible. The open architecture will have to take into consideration these functional layers (a) Sensing or Physical layer, (b) IoT access gateway, (c) Network and service layer. (d) Application layer



	IoT Stack	Web Stack
TCP/IP Model	IoT Applications Device Management	Web Applications
Data Format	Binary, JSON, CBOR	HTML, XML, JSON
Application Layer	CoAP, MQTT, XMPP, AMQP	HTTP, DHCP, DNS, TLS/SSL
Transport Layer	UDP, DTLS	TCP, UDP
Internet Layer	IPv6/IP Routing 6LoWPAN	IPv6, IPv4, IPSec
Network/Link Layer	IEEE 802.15.4 MAC IEEE 802.15.4 PHY / Physical Radio	Ethernet (IEEE 802.3), DSL, ISDN, Wireless LAN (IEEE 802.11), Wi-Fi

Fig. 1 Generic IoT Architecture Reference Model Reference:MaximeLefranÃ§ois, Introduction to Internet of Things[12]

III. IoT Case Studies

The following chapter discusses about various case studies executed to validate the IoT Architecture in picture and evaluate the results for reviewing the architecture and to create a reference model for building a secured Multistandard IoT Gateway.

A. CASE STUDY 1: IoT architecture for Smart Home

With reference to the Fig.1 the generic architecture that is been widely discussed and used in the commercial world and research. The data is transmitted from sensing (physical layer) to the Application layer by an Intel IoT gateway running on Intel Quark architecture and the network and transport layer takes care of modifying and packing the data. The IoT architecture in discussion here is sensing the physical appliances like Light and Fan. The parameters like amount consumed by the appliance and state of appliance (on and off condition) is transmitted through the Intel IoT gateway.

The Intel IoT Gateway is running on a Linux based OS and is capable of receiving the BLE signals by default since of the BLE module built in the SoC. The system is also interfaced with a Zigbee module and the architecture is configured to receive the zigbee and BLE data. The Intel Edison based IoT gateway is configured with MQTT agent to transmit the physical of the appliances under test.

Meanwhile using the open API's available in the Data analytics server running on the cloud collects these data for further analysis and decision.

B. CASE STUDY2: IoT Architecture for e-Health

Case Study 2 discusses on the data gathering from different health monitoring activities and focuses on transmitting the data to the IoT server for further data analytics. In this case the parameters are from Body Area Network based activity. The readings from temperature sensor, Heart beat are gathered through again an Intel Quark based IoT gateway running on an Intel Edison and stored on an Intel analytics dashboard from Intel. From the Intel IoT analytics dashboard the data are further analyzed for identifying case to case decisions.

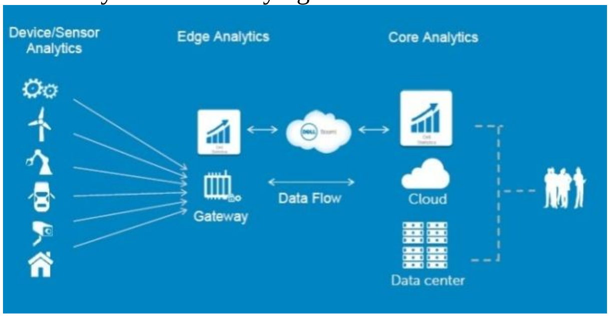


Fig. 2 (a) Intel IoT as Gateway with Edge Analytics based Architecture[13]

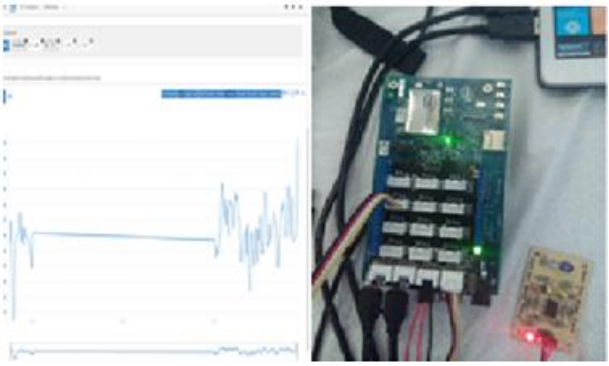
In case study 2 however the architecture is like simplex communication as only monitoring is the concern unlike case study 1 where monitoring and control is carried out.

C. CASE STUDY 3: Smart City Implementation

In this case the implementation is carried out using a nodes running on a TI CC3200 SoC gathering data's from: (1) garbage collection and scheduling, (2) street light control and monitoring (3) public and urban transportation system. However to implement a gateway in this design is a little challenging task as the data comes several nodes and connects to IoT server. All the data's are recorded on an IBM Bluemix server.

Fig.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



2

(b) Hearbeat rate monitoring on Intel IoT Dashboard

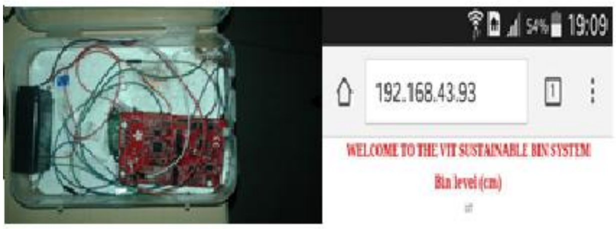


Fig. 3a IoT based Garbage collection system using CC320

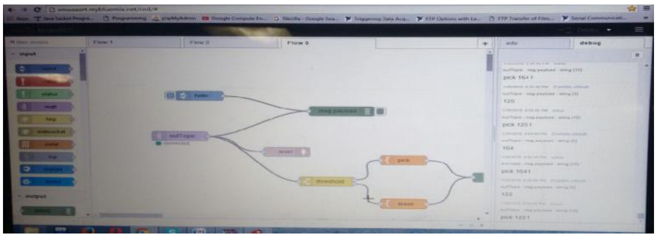


Fig. 3b Data gathered in IBM Bluemix.

D. CASE STUDY 4: WEATHER FORECASTNG SYSTEM

This work is done to forecast weather by deploying zephyr RTOS on ARM based SoC. The process involves collection and analysis of data to predict the weather conditions. It is implemented on an Zephyr based environment to validate an IoT system running on a Real Time environment. The Zephyr RTOS which runs on a small foot-print kernel deployed for resource constrained applications/embedded from small LED or senor to sophisticated smart watch and IoT. The parameters evaluated here is Temperature and Pressure. The data received from the sensor will in standard units. Considering all the BME280 is built with standard units.

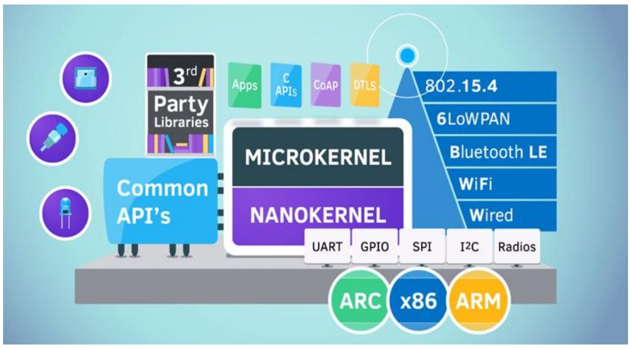


Fig 4a. Architecture for Arduino based services based on Zephyr RTOS[15]

Based on these case studies it has been observed that M2M architecture and design works according to the implementation under consideration. In traditional gateways using the built-in functions for interfacing multi-protocols and converting and communicating was made easier using special functions designed for them. Further the challenge was to rework on the packet to be formatted as per the standards and protocols under design. The only complexity inferred here is that for every implementation there is a need separate architecture reference model and there is no standard architecture where all can be integrated into a single entity. Also there is need for Interoperability, because each of the IoT implementation talks to its peers in its own protocol. If we consider the example of Smart City implementation where usually there is a need of multiple cases of implementation.

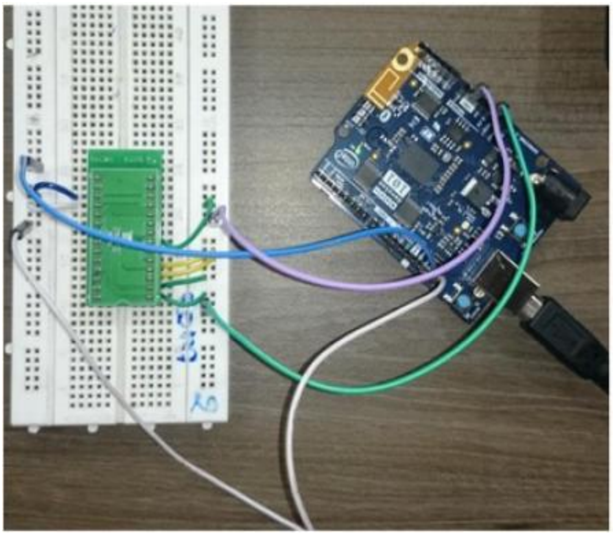
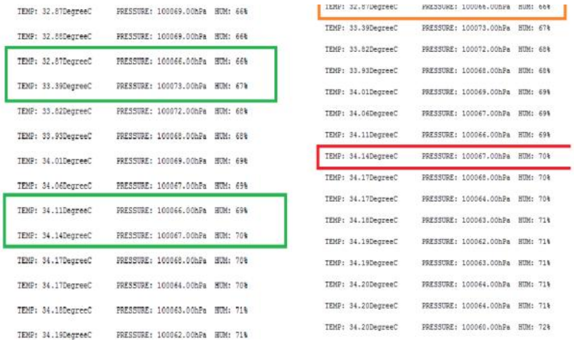


Fig 4b. Hardware Implementation of BME280 sensor Interface with Arduino 101 running Zephyr RTOS



```
TEMP: 32.87DegreeC    PRESSURE: 100069.00hPa  HUM: 66%
TEMP: 32.88DegreeC    PRESSURE: 100069.00hPa  HUM: 66%
TEMP: 32.87DegreeC    PRESSURE: 100066.00hPa  HUM: 66%
TEMP: 33.39DegreeC    PRESSURE: 100073.00hPa  HUM: 67%
TEMP: 33.82DegreeC    PRESSURE: 100072.00hPa  HUM: 68%
TEMP: 33.93DegreeC    PRESSURE: 100068.00hPa  HUM: 68%
TEMP: 34.01DegreeC    PRESSURE: 100069.00hPa  HUM: 69%
TEMP: 34.06DegreeC    PRESSURE: 100067.00hPa  HUM: 69%
TEMP: 34.11DegreeC    PRESSURE: 100066.00hPa  HUM: 69%
TEMP: 34.14DegreeC    PRESSURE: 100067.00hPa  HUM: 70%
TEMP: 34.17DegreeC    PRESSURE: 100068.00hPa  HUM: 70%
TEMP: 34.17DegreeC    PRESSURE: 100064.00hPa  HUM: 70%
TEMP: 34.18DegreeC    PRESSURE: 100063.00hPa  HUM: 71%
TEMP: 34.19DegreeC    PRESSURE: 100062.00hPa  HUM: 71%
```

```
TEMP: 32.87DegreeC    PRESSURE: 100066.00hPa  HUM: 66%
TEMP: 33.39DegreeC    PRESSURE: 100073.00hPa  HUM: 67%
TEMP: 33.82DegreeC    PRESSURE: 100072.00hPa  HUM: 68%
TEMP: 33.93DegreeC    PRESSURE: 100068.00hPa  HUM: 68%
TEMP: 34.01DegreeC    PRESSURE: 100069.00hPa  HUM: 69%
TEMP: 34.06DegreeC    PRESSURE: 100067.00hPa  HUM: 69%
TEMP: 34.11DegreeC    PRESSURE: 100066.00hPa  HUM: 69%
TEMP: 34.14DegreeC    PRESSURE: 100067.00hPa  HUM: 70%
TEMP: 34.17DegreeC    PRESSURE: 100068.00hPa  HUM: 70%
TEMP: 34.17DegreeC    PRESSURE: 100064.00hPa  HUM: 70%
TEMP: 34.18DegreeC    PRESSURE: 100063.00hPa  HUM: 71%
TEMP: 34.19DegreeC    PRESSURE: 100062.00hPa  HUM: 71%
TEMP: 34.19DegreeC    PRESSURE: 100063.00hPa  HUM: 71%
TEMP: 34.20DegreeC    PRESSURE: 100064.00hPa  HUM: 71%
TEMP: 34.20DegreeC    PRESSURE: 100064.00hPa  HUM: 71%
TEMP: 34.20DegreeC    PRESSURE: 100060.00hPa  HUM: 72%
```

Fig. 4c. Temperature and pressure recorded from serial window.

IV. SECURITY LAYER in IoT

Based on the above case studies the inference which whole IoT world is focusing is security in communicating entities. On several scenarios under consideration the IoT gateway is the typical responsible device which setsup the end to end security. A survey on the attack on Industrial IoT shows cyberphyscial systems inability to prone to attacks. Right from Eavesdropping, runtime attacks and malwares all targeted by powerful advisories as per article [7]. The author reviews the system is prone to attack

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

either the hardware through physical attacks, reverse engineering attacks and software basically by Trojan. Even Communication systems are hacked by DoS – Denial of Service.

As a clear indication that security architectures for IoT has been a major research. Major semiconductor manufacturers has focused on developing trusted computing based on secure hardware, Intel Software guard extension by Intel and ARM trustzone by ARM has been widely deployed in hardware level security. But since of strict real time requirements and complexity in the design makes it still not adaptable in the IoT. To build a secure IIoT(Industrial IoT), holistic approach is required to build a unified IoT gateway that can be adapted by any systems under implementation.

Security in IIoT is a major concern and in this implementation it is proposed to implement the MQTT in Network, Transport and Application layer and TLS in hardware abstraction layer. Using MQTT as a security measure will take into consideration of simple but still efficient security architecture for IoT. In the Network layer, especially when deploying aIoT based gateway considering a physically secure network or VPN would avoid any attacks in this layer. In transport TLS/SSL can be preferred for encryption. In application layer MQTT protocol uses client identifier with a username and password credentials.

V. CONCLUSION AND FUTURE CHALLENGES

Interoperability and building a multi standard gateway has always been of major concern which can be widely adapted in the IoT. But still the design is in a pedagogue stage and is yet to take shape and has to be tested for versatile usage as tested in 3 cases as discussed above. The case studies discussed here has been executed on versatile hardware like Intel, ARM, Arduino and mbed platforms.And in each of these cases the nodes are connected to IoT gateways through their respective network protocol. This kind of architecture will not fit for Edge Analytics to be carried out at the node. And also there is a need for Multi standard based gateways which can actually read data from heterogeneous nodes and carry out Edge Analytics. However the security measures has been increased in usage of this architecture in different layers by usage of MQTT and TLS and with Intel's own Intel's Gateway software solution stack providing levels of security at various levels. This certainly will open new doors in IoT Gateway which can be used multiprotocol implementation. Hence this work envisages the need of gateways which can not only collect data heterogeneous devices but also focus on building intelligence through edge analytics.

REFERENCES

1. Hsiang Wen Chen; Lin, F.J., "Converging MQTT Resources in ETSI Standards Based M2M Platform," in Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing(CPSCom), IEEE , vol., no., pp.292-295, 1-3 Sept. 2014
2. Ran Xua&Shuang-Hua Yanga, Ping Li, Jiangtao Cao, "IoT Architecture design for 6LoWPAN enabled Federated Sensor Network", Proceeding of the 11th congress on Intelligent Control and automation Shenyang, china, pp2997-3002, June 29 – July 2, 2014.
3. Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S. Kumar, KlausWehrle, "Security Challenges in the IP based Internet of Things", Wireless PersCommun (2011) 61:527–542, Sep 2011.
4. Pratikkumar Desai, Amit Sheth ,PramodAnantharam, "Semantic Gateway as a Service architecture for IoT Interoperability", IEEE International Conference on Mobile Services, pp 313 – 319, IEEE 2015.
5. Singh, M.; Rajan, M.A.; Shivraj, V.L.; Balamuralidhar, P., "Secure MQTT for Internet of Things (IoT)," in Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on , vol., no., pp.746-751, 4-6 April 2015
6. Lesjak, C.; Hein, D.; Hofmann, M.; Maritsch, M.; Aldrian, A.; Priller, P.; Ebner, T.; Ruprechter, T.; Pregartner, G., "Securing smart maintenance services: Hardware-security and TLS for MQTT," in Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on , vol., no., pp.1243-1250, 22-24 July 2015
7. Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 4, AUGUST 2014 pp 349 – 359.
8. Wang Quan 1, 2, Chen Xuhui1, Wang Ping1, Liu Chao, "Design and Implementation for the Industrial Wireless Gateway of Smart Tunneling", International Conference on Measuring Technology and Mechatronics Automation, 2010
9. Christian Lesjak, Daniel Hein and Johannes Winner –" Hardware-Security Technologies for Industrial IoT: TrustZone and Security Controller, IECON2015-Yokohama
10. Manfred Sneps-Sneppe and Dmitry Namiot, About M2M standards M2M standards and Open API, ICDT 2012 : The Seventh International Conference on Digital Telecommunications, 2012
11. PP Ray, "A survey on Internet of Things architectures",Journal of King Saud University – Computer and Information Sciences (2018) 30, 291–319
12. https://www.intel.com/content/www/us/en/internet-of-things/gateway-solutions.html
13. http://ci.emse.fr/teaching/maj-info/iot/2017/1/#title-slide
14. https://thehackernews.com/2016/02/zephyr-internet-of-things-os.html

AUTHORS PROFILE

Balamurugan MS, is working as Assistant Professor in Vellore Institute of Technology, Chennai and has over 10+ years of experience in Industry, Research and Academic. He has published over 10+ papers and has been actively working in the area of Internet of Things.

ManojkumarR, is working as Associate Professor in Vellore Institute of Technology, Chennai and has over 10+ years of experience in Research and Academic. He completed his PhD from TELECOM SudParis, France in 2012 and has been serving in Vellore Institute of Technology, Chennai since then. He has been working as Research Assistant in IIT Kanpur. He has published various research papers in the area of Humar Computer Interaction and Computer Vision.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication