Proceedings of the Pakistan Academy of Sciences:
A: Physical and Computational Sciences 57 (4): 13–22 (2020)

ISSN: 2518-4245 (print), 2518-4253 (online)

Pakistan Academy of Sciences

Research Article

Cloud Based Multi-Level Security, Event Based Surveillance and Real-time access in Smart Homes using Zigbee

Jawad Ali[1], Haseeb Zafar[2], Inamullah Johar[3], and Nasar Iqbal[4]

[1,2,4]Electrical Engineering Department, UET Peshawar, Pakistan
[3]Electrical Engineering Department, UET Peshawar (Mardan Campus), Pakistan,

Abstract: In recent years, smart home automation, real-time access to smart appliances, security & surveillance and inter-connected sensory node application are being the active topics for its considerable development. The work utilizes a smart home gateway that enables the bidirectional data streams to be converted between Wi-Fi protocol (IEEE 802.11b/g/n) and ZigBee protocol (IEEE 802.16.4, 6LoPAN). The paper describes the unified application of Infrared beam sensors & motion detectors (PIR BISS0001) and IP camera (ICamView IP-01b) in the smart home surveillance and reducing video data communication as well as needless storage of the video stream. The devices are remotely monitored using a server that can obtain a real-time connection upon the anomaly detection in the surveillance area. The ZigBee-WIFI gateway is solving the bottle-neck between the data rates of two different communication technologies, i.e., WIFI (VT6656) and ZigBee (JN5148). All the devices are remotely monitored by a centralized server that is making adequate decisions based on the data received from these IP based devices.

Keywords: Internet of Things (IoT), ZigBee, Remote Sensing, WSN

1. INTRODUCTION

Internet of Things (IoT) is the upgraded form of heterogeneous networking [1] with the introduction of IP for every connected node. IoT node, an individual productive element in the connected network of IoT, is possessing one or more of the features including recording, analyzing, feedback, actuating or supporting communication. The five features make the use of IoT widespread [2–5]. Health, security, industry, entertainment, communication [5] and every emerging and already advanced technology has some room to become more productive by embedding IoT. Control, information handling, security and decision making are the four-main stream uses of IoT. Further, each of these categories can be devised into two generic parts that are autonomous and man driven. The four said streams might be addressed differently when the amount of time for action is considered. These tasks can be performed either after a regular interval of time or it can be instantaneous, based on the type of application or need. IoT based technologies do not reside inside computers only. IoT transforms data driven devices (things) to make particular and exclusive decisions.

The ubiquitously communicating nodes [6, 7] can make concurrent decisions using feedback mechanism both from locally made decision making schemes and remote server based protocol utilization. IoT has defined both application level protocols and network level protocols for communicating nodes. The application level protocols include CoAP, IBMs MQTT, HTML 5s Web Socket, XMPP, RESTFUL Services and AMQP. Network level protocols include 6Lo, 6LoWPAN, LoBAC, Z-Wave, Thread, 6TiSCH, IPv6 over G.9959 and IPv6 over Bluetooth Low Energy. All these protocols enable the integrity of data, on-time delivery and availability of the information with minimal costs and expandable usage.

The Literature review section includes a brief literature of IoT enabled technologies and some

Received: July 2018; Accepted: December 2020
*Corresponding Author: Jawad Ali <jawad@uetmardan.edu.pk>

of its widespread applications. The devices that are used in developing the unified surveillance system are explained in the experimental setup. The methodology section gives an insight into the work and then results, application and future advancements are quoted in the ending sections.

2. LITERATURE REVIEW

2.1 Home Automation and Path to IoT

IoT applications were at first a Do It Yourself (DIY) based approach. These approaches were, in the majority, explored in small projects such as Wi-Fi based home automation using Arduino, PIC MCU and Atmel 89c51 and its derivatives. Web services and android based home automation and security protocols are operational using Raspberry Pi and tiny OS. Similarly, structured and semi structured data are delivered to cloud for machine learning and other formats of number crunching using Hadoop clustering techniques and Systems [8]. Email based notification systems are also developed using GPRS modules in connection with different processing equipment that include MCUs, MPUs and tiny OS. Email based notifications are not readily handy in controlling approaches. Thus, real-time applications of remotely controlling applications in home automation are done using DTMF receivers with both looped feedback and without feedback applications.

Many low powered, PCB mounted modules are directly connected to the communicating nodes for wireless sensors based mobile technologies in the literature. These approaches are in advanced forms using GSM with PIC MCU for application specific remotely controlling scenarios. Bluetooth based lower power and low range, scalable networking is also developed in the recent years due to its actively scalable nature and the introduction of Bluetooth in smartphones and hand-held devices. These applications were developed initially with the help of processing and communicating modules such as GSM (SIM-900) and Arduino UNO. In later years, Bluetooth enabled devices were directly manufactured with a custom firmware for adding up to local home network and thus active pairing to home automation and control.

2.2 Application of IoT in Updating Smart Homes

A smart home provides intelligent, autonomous and ease of control, management and monitoring of households. The connectivity is not limited to electronic appliances only but each appliance is enabled for connecting to the Internet, local moderator or coordinator to enhance its functionality. This enhanced functionality is obtained by introducing Machine to Machine (M2M) communication [9] between these smart devices. A typical IoT based smart home is depicted in Figure 1. M2M architecture is quite similar to that of IoT because most of the M2M communication based devices use network protocols that are the characteristics of IoT. Note that each connection is IoT needs smooth communication with its depending devices for adequate performance.

Individual Thing in M2M communication is referred to as a node (in this document, we will be using node(s) and" Thing(s)" interchangeably). The current M2M market is highly fragmented and it is least standardized. Moreover, growth in M2M due to small projects is adding more complexity in unifying home automation by including its different modular networks. For example, security and surveillance systems [10] are separately managed and billed whereas energy utilization, smart grid and control are dealt in another network. Thus, many companies of diverse applications need to collaborate on a unified platform to cope this issue of increasing networking complexity and diversification. IoT gives this solution because of its IPv6 based connectivity and identifying each and every device (Things) in a networks as a separate entity. These devices are then connected to one another based on the information and communication scheme that is the core functionality of the IoT based applications.

The end nodes, connecting nodes, processing (middleware) & decision-making nodes, each node has a key role in M2M communication. The connectivity, being the backbone of these nodes, is accomplished using variety of protocols. General purpose low data rate wireless protocols include BLE and ZigBee. Wi-Fi is used for relatively higher data rates and its energy consumption depends upon its usage frequency. Each device is connected to

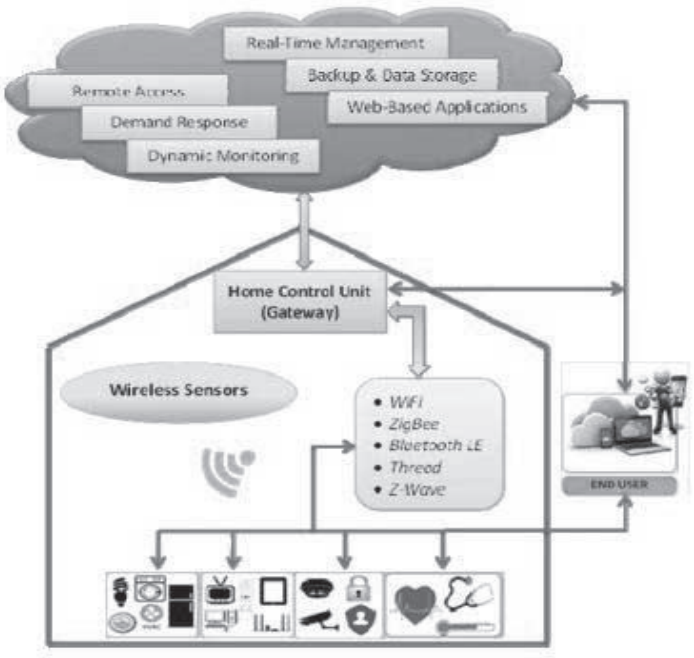

Fig. 1. Typical IoT based smart home

the central communicating node in its unique way. Depends on this connectivity based application control, Cloud based IoT connectivity solutions are employed [11]. The application includes time and event based appliance control, scheduling, information exchange and notifications, security and surveillance, logging and a big list of other useful and needful activities besides intelligent monitoring of self-health and automatic network healing.

2.3 Homes IoT Application in Smart Home Security and Surveillance

2.3.1 Security in Smart Environment:

Security is a vast field in information and communication technology. It ranges from access control in/to specific geographic or logical premises to information security and data communication [12]. The level of security is defined by the type of encapsulation required to grant access and strict permission from using information of assets of a specific individual or firm. Smart home security [13–15] is divided into two phases, the registration phase and the validation phase. First, user's registration is processed and a legit user is added to the system for control, maintenance and updates. The authentication phase uses the validation mechanism for allowing the legit user to use the system, in our case, home appliances.

Advance authentication systems use user name and create a hash using neural networks. The output hashes are then used to run the home appliances and also for a different level of access. Fingerprint, face recognition, IR face structure mapping, retina detection, code based techniques, RF ID based authentication systems are being employed for its range of application is smart homes [16]. The smart home environment is equipped with various kind of tracking, recording and sensing devices. These devices are usually provisions with various home appliances and are value added services. The concept of a smart home uses these handy sensors to give more comfort and security to the end-user and make the smart homes more personalized. Privacy aware infrastructures such as Sentry@ Home provides this information sharing with promising security.

2.3.2 Surveillance in Smart Environment:

The electronic guard in smart environment is active 24/7 and is thus more efficient and cost effective as compared to common watch man. But, this electronic watchman is prone to be deceived and may not be trained enough to consider a security

threat as a threat. Thus, close looped systems need to have efficient algorithms to assure security in smart environments, including domestic security and security of households.

At this point, we have understood that the scope of surveillance may include but is not limited to just visual intruder to access a system or an area. Tracking of the culprit, tracking of the information the culprit is using, communicating, exchanging and the areas being breached during security protocol tempering must be properly communicated in order to maximize the efficiency of a surveillance system. Off-course the activities that are to be monitored may include but not limited to the usage of cash dispensing machines, driving a car, using a library card, getting and sending emails and even using telephone. We can see a verying pattern in the said activities. That is, all these activities can be properly logged with time stamps as well. Such data can be also checked for links with other personnel's' information for the same tasks using databases. This gives us a broader sense of information based surveillance, all possible with the advancement in IoT.

2.4 ZigBee to Wi-Fi Connectivity

Connectivity in smart home networking face challenges like interoperability, self-network healing & management, proper signalling, bandwidth constraints and power restriction.
Table 1 compares the two standards based on scalability, power consumption, communication techniques and ranging. Based on these diverse properties, one can readily select ZigBee for short range, multipurpose communication for home based automation, control, security & surveillance systems, their interconnectivity and interoperability. ZigBee is new trend in IP based networking and uses 802.15.4 Physical layer. It supports IPv6 using 6LoWPAN. The discussion concludes that home automation is scalable if ZigBee and its predecessors are used. ZigBee makes automation plug'n'Play. Addition of new appliance or Thing to the existing infrastructure won't affect the performance of previously developed ZigBee based mesh network drastically. As this technology does not support relatively higher data rate applications so the home automation must be provided with a backbone networking for carrying large amount of collective and individual data.

2.5 Algorithms Applied for Security and Surveillance

Many algorithms have been developed for security and surveillance till data. These algorithms include logging data security and surveillance as well as video and audio based tracking and anomaly detection. Maximum average correlation Height (MACH) is a correlation based filtering approach for target detection as well as its classification. Automatic Target detection and Recognition algorithms (ATR/D) is used for multi view point object racking in its field of view (FOV). Real time communication protocols and messaging techniques such as COTS video cameras are used for continuous monitoring. The distributed approaches are used on Military operations in urban terrain (MOUT) scenarios which gathers information about various fields. Video surveillance and monitoring pro-gram (VSAM) was the first large funding based development program by U.S. government. This was the first program that inscribed the application of multi camera systems, auto calibration and tuning, still image detection and tracking objects if interest.

The next generation surveillance includes but is not limited to detection and tracking only. Automatic calibration system, event based recording, tracking object on multiple cameras and objects moving from one FOV to another is also addressed (Figure 2). Other challenges that are being addressed in the current research include face recognition at a certain distance and angle. Interpolation based image completion are also the focal point of the research and programmers and engineers are using advanced artificial intelligence approaches for identifying at any position, distance and angle.

The advanced tracking systems that are being developed by the U.S. department of states are collectively titled as Combat Zone That See (CZTC). Wireless Ad hoc routing schemes are used that are centrally connected and offers the facility of activity monitoring and long-term movement pattern analytics. Extraction of information from video and data feed has already gained much attention and thus many working schemes are developed. The next challenge is to concentrate

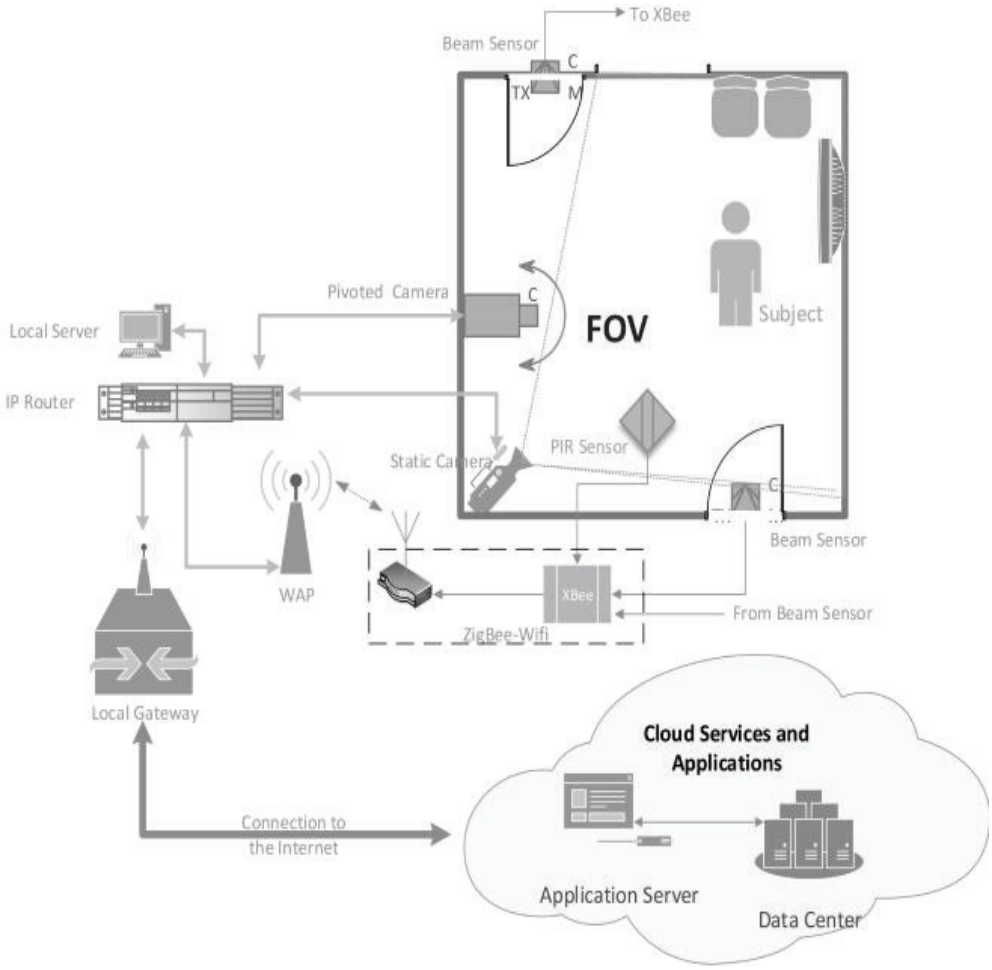

Fig. 2. Cloud based Multi-level security, event-based surveillance and real-time access in smart homes using ZigBee

Table 1. Comparison between WIFI and ZIGBEE based Networking

Characteristics	Wi-Fi	ZigBee
IEEE Standard	802.11	802.15.4
Frequency band	2.4GHz, 5GHz	2.4GHz
Nominal range	150m	100m
Peak current consumption	116mA	30mA
Power consumption per bit	0.00525W/bit	185.9mW/bit
Data Rate	1Gbps	250Kpbs
Network topology support	Star, Mesh	Star, Mesh & Cluster
Number of nodes per network	250/access point	65000

on unifying a large set of feeds and vast area deployment. These challenges include minimizing deployment costs, wiring and its complexity, low power hardware etc.

3. EXPERIMENTAL SETUP

Our design includes a static camera, Pan-Tilt-Zoom Camera, PIR sensors and its controlling circuitry. The monitoring space is covered by one or more cameras whereas the PIR sensors are used for triggering different controlling events for event based recording and notifications. The design covers a 4x4m room containing two inlets (doors). The devices that are used for security monitoring and surveillance include Pivoted camera that can rotate and track object inside the room, static camera that is used for recognition and still imaging as well as surveillance in its Field of View (FOV). The doors are given with IR beam sensors that can detect any object passing through the door.

3.1 Surveillance Field and PIR Sensor

The surveillance field resides inside the IR beam sensors. The field contains (not covered fully) a proximity sensor that timely sends notification to the remote server about the change in position of the subject. A passive infrared sensor (PIR) is an electronic device for measuring intensity of heat radiation of about 10 microns wavelength. The inlets to the surveillance area are covered with infrared beam sensors. These sensors have multiple beams that are received by its active RF receiver from the transmitter. This sensor enables the algorithm to work on height based scenarios as well. In case of a human, if walking normally, all the beams are interpreted. Thus basic level security check starts from this entry point. The data from this sensor is also managed using XBee.

3.2 Sensors to ZigBee Connectivity

The middle pin of this sensor sends data to XBee on Analog input pin 20. Its other two pins are connected to ground and +5V power source. The sensor pin will receive signal each time variation in temperature due to motion is detected. Similarly, the output from IR Beam sensor are fed into XBee Wi-Fi module. XBee Wi-Fi has a fully integrated support for cloud and remote connection and is readily applicable for both industrial and domestic use. It can support a theoretical data rate of 72Mbps which is sufficient in our case.

3.3 Feeding ZigBee Data to Server

As discussed in the previous section, XBee WIFI is a cloud connected product. It also has a local web UI and can be accessed using Putty from a socket based program running on the same network. The XBee module takes the data of motion, proximity and intrusion detection and places it on the local server that has the triggering mechanism for recording events. The work uses XCTU which is a free window, Linux and MacOS based platform for wireless configuration of these XBee modules.

3.4 Camera to Server Connectivity

IP camera in this scenario uses translated network addresses, (NAT). We are using static and rotating IP Cameras for multi-level security and intruder detection and surveillance. Both cameras are directly connected to the local router using RJ-45 cable. The router is accessed using its admin panel and the IP addresses of both the cameras are searched in the connected devices. The connected addresses are made static for device names corresponding to the IP cameras. The router also has a connection with the local server. The networked cameras are accessed from the server using the obtained IP addresses from router. Each camera can be configured using the built-in web UI of the IP cameras. It is mandatory to change the access authentication username and password for the camera because this camera will be available for every person connected to the router. The purpose of keeping this camera on NAT is to separate it from direct intercourse with the outside word.

3.5 Server to Cloud Connectivity

The cloud based application server is remotely accessing the information of the local server. The application installed and running on the cloud includes face and shape matching algorithms, anomaly detection and emergency signaling plus notifications for now. The connection between cloud application and local server is purely TCP/IP based. Thus, on time packet delivery and information security are performed by encapsulating the data

using some encoding techniques. The work uses blob XORing for encryption and decryption of secure information and signals.

4. METHODOLOGY

4.1 Algorithm of Operation

The algorithm of intruder detection, entering to the field of view, snapping sample for recognition and then object tracking is given in Figure 3. The process starts with the orders of remote server on which application for surveillance is installed. The remote server when activates orders to switch the security mode to ON status, the local server sends orders using LAN-Wi-Fi-ZigBee connection to turn on IR Beam Sensor. The sensor is installed on the inlet of the area under observation. Upon breaching this level, a simple SMTP/HTTP request acknowledges the local server and the server initiates second security check. Note that the second security check i.e., proximity sensor check is effective but not necessary for this system.

The PIR sensor, when detects some intrusion inside the area, Static Cam turns ON and samples of videos are sent to the local LAN connected server. This server runs basic algorithm after cropping still images and facial recognition is performed. The proposed system uses line edge map technique for fast processing. After the intruder is detected and recognized. The samples are sent to the cloud server and kept there. On the query of local application server, the tracking of the subject is started but the data is not shared unless the remote cloud server asks for it. The session starts in this algorithm because the cloud server has already initiated orders for recording the event. The event and hence session stops as the remote application is not in need of the position of the subject.

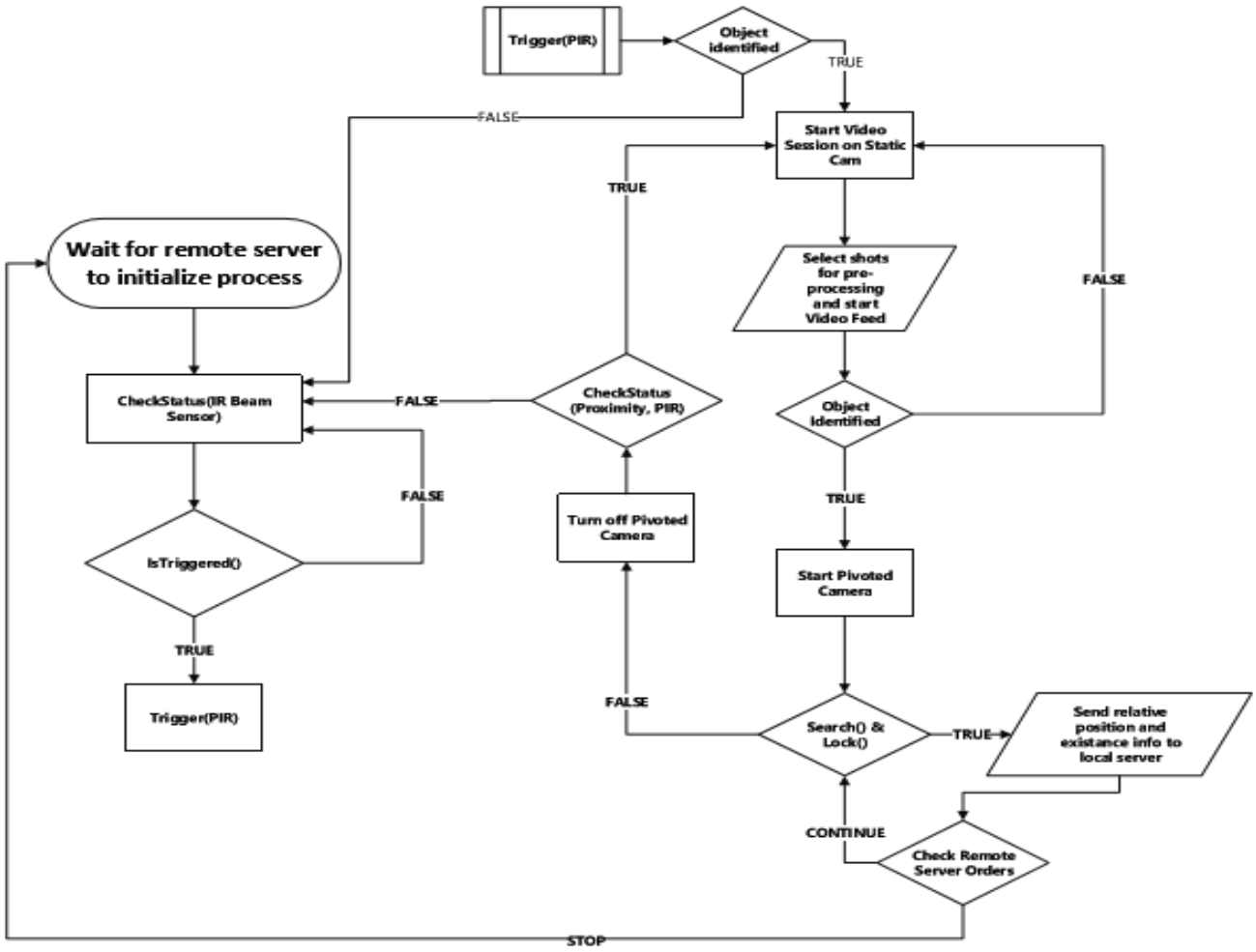

Fig. 3. Process flowchart interpreted in the coming sections.

4.2 Application Mechanism

The subject, when enters the room, the door IR beam sensors triggers the PIR sensor that are available for checking the proximity and hence the presence of the object inside the area (room). Both sets of these sensors are collectively, managed by XBee that sends the information via ZigBee-WIFI switch to the local server for processing. The local-server, on the other hand, send message to the IP based static camera to record the event and connects the video feed of the camera for local assessment. This whole process is monitored via an application server that is virtually installed on the cloud.

After the information of subject is pre-processed on the local server. This TCP/IP network links the application server with the pivoted camera controls. This camera doesn't send the video to the cloud and thus saves bandwidth. On the other hand, the subject is analyzed on the application server for further authentication and surveillance purpose. The said mechanism is plug and play and each IP based camera can be directly linked with the application server and the positioning of any type of object can be tracked without sending the data to the remote server.

4.3 Obtaining Data

1) Intruder only opens the door: In this scenario, only IR Beam triggers the PIR using XBee. PIR checks the proximity and sends the status using XBee to the local server for a fixed duration. After a fixed number of iterations of proximity check, the server resets both sensors.
2) Intruder is static inside the room: In this scenario, IR Beam sensor is triggered, the local server receives this information and turns up the PIR sensor. The PIR sensor sends the change in the IR characteristics and heat characteristics of the room. After that it sends message to turn on the static camera using the same local server. The static camera searches its FOV and sends it to the local server. The server runs face recognition and object detection algorithm and keeps it in the local server. As the object is identified so the pivoting camera searches for object/face. It locks the target but the static position of the object is detected by the local server and the remote server is only given with one position of the intruder.
3) Activity surveillance and anomaly detection: Though the second scenario is also an anomaly because both the security levels are breached. The intruder has successfully entered the area and the proximity and the static camera has confirmed the identity and existence of the subject. But due to the static behavior of the intruder, the algorithm is not able to perform the task for which the whole setup is created. When the intruder moves inside the area that is under surveillance, the pivoted camera captures every move of the intruder while the video is compared with the feed of static camera and hence the relative position is also noted. This algorithm thus gives maximum control over locking and updating the exact position of the intruder. Fig. 4 is the real-time log that is generated at the remote application side for surveillance.

5. DISCUSSION

The work presented in this document uses advanced IoT concepts such as ZigBee for inter-connectivity and immediate response. Thus, it is readily applicable in the development of smart homes. The whole system is cost efficient because the local server can be deployed on Raspberry pi and the Local routers can be omitted. A desktop computer is used as local server because it was convenient for modifications that were necessary for the efficient modelling and design of this smart security and surveillance system. The efficiency of the system is relatively higher than the traditional surveillance systems because in the traditional systems, continuous video feeds are used and the real-time face recognition and anomaly detection is a big challenge.

The mechanism reduces bandwidth utilization and improves the system efficiency because of its two major contributions and differences to the traditional surveillance. The first is, only the coordinates of the next point to which the object moves are sent to the server for updating the location information. Secondly, continuous feed of video is avoided and event based recording and triggering is employed by the algorithm which cuts-off storage costs as well as bandwidth utilization. Another facility that is offered by this technique

is that application server is deployed remotely on cloud. This is the most important benefit of this system if we consider remotely control and access as our focal point of research.

6. FUTURE WORK AND MODIFICATIONS

The future work can be based on three broader terms we found during this research. Firstly, the work has a great capacity in terms of its improvement both in its response time and increasing the productivity. Secondly, this work is not only limited to intruder surveillance inside a fixed area. The coordinate based object location and pivot camera tracking can be used to track the movement of an object under surveillance of many cameras. In that case, we will just have to put some effort into utilizing the already developed algorithms and made some modification to those algorithms so that it can be used for cloud based surveillance systems as well.

The future work may include, adding many cameras and moving object from the FOV of one camera to that of other. Action and event can also be recorded locally in much detailed manner on the introduction of extra sensors and cameras to the existing infrastructure. Addition of other devices is relatively easier because the infrastructure is using already developed technologies and hence productivity can be increased without much effort and expanding installation and maintenance costs. Multiple object detection is also added to the future extrapolation of the work presented in this document.

7. REFERENCES

1. K. Xu, Y. Qu, and K. Yang, "A tutorial on the internet of things: from a heterogeneous network integration perspective," IEEE Network, 30(2): 102–108 (2016).
2. M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," IEEE Transactions on Industrial Informatics, 9(1): 277–293 (2013).
3. H. Zhang and W. Ni, "Applications of iot technology to the constructions of hospital information systems,"in 2017 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 1405–1408 (2017).
4. Y. Wang, M. Zhang, and Y. Zuo, "Potential applications of iot-based product lifecycle energy management," in 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 1999–2002 (2016).
5. R. Porkodi and V. Bhuvaneswari, "The internet of things (iot) applications and communication enabling technology standards: An overview," in 2014 International Conference on Intelligent Computing Applications, 324–329 (2014).
6. M. Say, "Ubiquitous computing riding the next wave," ITNOW, 56(1): 22–23 (2014).
7. J. Y. C. Sun, "System scaling for intelligent ubiquitous computing,", IEEE International Electron Devices Meeting (IEDM), 131-137 (2017).
8. R. Sadikin, A. Arisal, R. Omar, and N. H. Mazni, "Processing next generation sequencing data in map-reduce framework using hadoop-bam in a computer cluster," 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 421–425 (2017).
9. E. Oyekanlu, C. Nelatury, A. O. Fatade, O. Alaba, and O. Abass, "Edge computing for industrial iot and the smart grid: Channel capacity for m2m communication over the power line," in 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), 1–11 (2017).
10. J. J. S. Haribaabu. V, "Intelligent surveillance system using internet of things," International Science Press, IJCTA, 37(9): 313–318 (2016).
11. A. Elsaeidy, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "A smart city cyber security platform for narrowband networks," in 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), 1-6 (2017).
12. W. Hu, T. Tan, L. Wang, and S. Maybank, "A survey on visual surveillance of object motion and behaviors," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 34(3): 334–352 (2004).
13. S. Srivastava, A. Bisht, and N. Narayan, "Safety and security in smart cities using artificial intelligence x2014; a review," 7th International Conference on Cloud Computing, Data Science Engineering Confluence, 130–133 (2017).
14. S. Datta and S. Sarkar, "Automation, security and surveillance for a smart city: Smart, digital city", *IEEE Calcutta Conference* (CALCON), 26–30 (2017).
15. V. Beltran, J. A. Martinez, and A. F. Skarmeta,

"User-centric access control for efficient security in smart cities," in 2017 Global Internet of Things Summit (GIoTS), 1-6 (2017).

16. H. Wei-Dong and Z. Bo-Xuan, "Smart home wireless system using zigbee and ieee802.15.4," in 2016 Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC), 858–863 (2016).
17. W. Bialek, and S. Setayeshgar. Cooperative sensitivity and noise in biochemical signaling. Physical Review Letters 100: 258–263 (2008).