International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Review of Home Automation Systems and Network Security using IoT

Otieno Godfrey Oduor

Department of Master of Computer Applications,
Jain (Deemed-to-be University) Knowledge Campus, Bengaluru, Karnataka, India

ABSTRACT

In the current tech world, there are multiple advancements being made in the field of Network Security, this is because devices are grouped into various networks and can be accessed remotely through the use of the internet. As a result, it is integral to ensure that only the authorized personnel are able to access and control the respective devices which are connected in the various networks. Mobile devices such as smart phones, laptops, tablets etc. have enabled users to access their information on the go at any time provided they have internet connectivity and are connected to the devices network.

KEYWORDS:

IoT – Internet of Things,
MQTT - Message Queuing Telemetry Transport,
ANN – Artificial Neural Networks,
DDoS – Distributed Denial of Service
PKI – Public Key Infrastructure

How to cite this paper: Otieno Godfrey Oduor "Review of Home Automation Systems and Network Security using IoT" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.805-808, URL: www.ijtsrd.com/papers/ijtsrd30687.pdf

IJTSRD30687

1. INTRODUCTION

Information technology has become the integral part of our life. To satisfy the need of the society, almost in each work, we use the technology. In current era computer science is major subject. It has many real life applications such as cloud computing (HYPERLINK \l "XU201275" *1*), artificial intelligence*2*), PowerShell (HYPERLINK \l "HMo20" *3*), Internet of things*4*,*5*,*6*,*7*,*8*,*9*,*10*,*11*), SPP (HYPERLINK \l "broumi2019shortest" *12*, HYPERLINK \l "kumar2019multi" *13*, HYPERLINK \l "Kumar2019l" *14*, HYPERLINK \l "kumar2019novel" *15*, HYPERLINK \l "kumar2019shortest" *16*, HYPERLINK \l "kumar2018neutrosophic" *17*, HYPERLINK \l "kumar2020different" *18*, HYPERLINK \l "kumar2017shortest" *19*), TP (HYPERLINK \l "kumar2019pythagorean" *20*, HYPERLINK \l "Kumar2019m" *21*, HYPERLINK \l "JPr" *22*), internet Security (HYPERLINK \l "SAKHNINI2019100111" *23*), uncertainty (HYPERLINK \l "gayenchap102019" *24*,*25*,*26*) and so on. Information Technology is the mode by which user can use computers and internet to store, fetch, communicate and utilize the information. So all the organizations, industries and also every individual are using computer systems to preserve and share the information. The internet security plays a major role in all computer related applications. The internet security appears in many real-life applications, e.g., home security, banking system, education sector, defense system, Railway, and so on. In this manuscript we discuss about the protection of authentication which is a part of internet security.

Home automation in layman's terms is the process of being able to monitor and operate household devices such as tv's, air conditioning systems, security appliances etc. without the need of having any physical interaction with the devices.

Fig 1.1 Home with an Automated System

The devices are all connected to the same network and through the use of a mobile device a user will be able to control the household devices remotely. The devices are equipped with sensors which will be used in sending and receiving signals, users will be able to input commands that

will execute the instructions and perform the various tasks and in turn generate outputs. The primary function of automating a household is to conserve energy (to ensure devices are in use only when needed) thus minimizing cost for energy consumption.

Components of Home Automation

- IoT sensors.
- IoT gateways.
- IoT firmware.
- IoT cloud & database.
- IoT middleware.

2. Literature Review

In (HYPERLINK \l "Sey" *27*), the authors have proposed the use of Blockchain and Ethereum for developing IoT systems. A blockchain is a growing list of records (blocks) linked using cryptography and each block has a cryptographic hash of the previous data, timestamp and transaction data.

Blockchains are resistant to modification of the data because if one block is modified then all previous blocks need to be modified as well otherwise the links between the original blocks are lost. Ethereum is a public blockchain based computing platform which allows developers to write and compile programs (smart contract) that can run on blockchain. Keys are managed using RSA public key cryptosystems whereby the private keys are stored on individual systems while public keys in Ethereum.

2.1. Blockchain and Ethereum system

Ethereum is a distributed computing platform thus all involved entities have parts of blockchain of Ethereum which constantly update and make transactions.

The smart contracts contain code which when certain criteria are met, they are executed. e.g a user can set the air conditioning system to be automatically switched on/off at a particular time of the day. The smart contracts are compiled in an Ethereum virtual machine and the Ethereum nodes execute the instructions in the code once the corresponding contract is verified to have come from a valid account.

In *28*), the authors have explained how the use of temperature sensors along with the ESP8266 as the gateway are used in implementing a home automation system. The protocol used to achieve the home automation process is the Message Queuing Telemetry Transport, it's a lightweight protocol which works on TCP while efficiently using the network bandwidth. It comprises of the following agents which enable the exchange of application messages; the MQTT client, MQTT broker and the MQTT server. The MQTT client can either publish or subscribe to application messages, MQTT server is the link between the MQTT clients and its purpose is to receive and send the application messages to the clients while the MQTT broker collects and organizes information from MQTT clients that intend to publish their data.

2.2. ESP8266 based MQTT system

Light Dependent Resistors are connected to the ESP8266 development board, the intensity from the sensors is processed and actuation is performed. ESP8266 is configured as an MQTT client publisher and its data is sent to the MQTT broker. It also subscribes to commands for controlling the actuation. Once the system is set up, a user can configure the amount of light that is required at any given time in a particular room, the LDR sensors connected to ESP8266 will detect the light in the room then send the information to it. Based on the predefined instructions set by the user, ESP8266 will regulate the light in the room by either turning on/off the lights.

In (HYPERLINK \l "Mil19" *29*), the authors have proposed the use of; i) Raspberry Pi which is a customizable and programmable small computer with support for a large number of peripherals and network communication, and ii) Oblo Living system that comprises of sensors, actuators, a central control unit and supervisory controls. Raspberry Pi is acts as a personal computer and has external connection ports such as USB and HDMI ports, which facilitate communication with external devices. The control unit in the Oblo Living system is the gateway and it connects all the devices.

2.3. Raspberry Pi & Oblo Living system

The gateway collects information from the sensors, it runs multiple calculation loops and controls the behavior of the actuators then stores the relevant information. The supervisory control provides an interface which is used to display the results from the gateway in a human readable format.

For exchange of information to occur in the network, the connected device must know the communication protocol (MQTT), and it's should be authorized by the gateway. Once verified, the user through the help of the supervisory control's interface will set the instructions which will be processed by the gateway and the lighting system of a room or the entire house will be switched on/off when a person enters the room. In *30*) the authors have implemented a system which is referred to as Beehouse, it comprises of the following components, an Arduino microcontroller board, Zigbee technology, Sensors and Actuators.

2.4. Bee house system

The components are put together as hardware nodes totaling to three nodes, whereby each will have an actuator and corresponding sensor. The Arduino board accepts input from its surrounding through sensors and actuators. The type of Arduino board used is the Duemilanove due to its accessibility to pins for interfacing external circuits, its built in RS-232 to USB controller which is used for programming the microcontroller and also enabling communication between the board and any software.

The Zigbee protocol is used as the communication medium and its modules dubbed XBee are integrated with Arduino using an add-on board known as the XBee shield. There are three sensors used, i) to measure the temperature 10k ohm thermistors are used, ii) for measuring the light, mini-photocell sensors are used which interpret the light available as high, medium or low, and lastly Passive Infrared sensors are used to detect motion in the rooms. The Actuators interact with the sensors by taking actions after receiving commands from the user or events from sensors. In (HYPERLINK \l "Eli16" *31*), the author have proposed counteracting the threats faced on IoT by using a supervised ANN which is then assessed on its ability to prevent DDoS attacks.

2.5. Artificial Neural Network Intrusion Detection system

The ANN is used as an offline Intrusion Detection System that collects and processes data from different locations on the IoT network then tries to detect whether a DDoS attack is ongoing on the network. The neural network is provided with labelled training set, it then gains knowledge by mapping from inputs *x* to outputs *y*, given a labelled set of inputs-output pairs;

$d = \{(x_i, y_i)\}^{N}_{i=1}$. d is the training set; N is the number of training examples.

3. Results and Discussion

In *27*), the advantages of using of blockchain and Ethereum to develop IoT systems include;

A. Ethereum allows developers to write smart contracts thus the code is considered to be Turing-Complete (runs on top of Ethereum). This enables the easy management and configuration of the IoT devices.
B. Blockchain also can't be modified without permission hence making it secure.
C. The use of blockchain also allows the synchronization of several linked devices to be done due to its distributed ledges.

In (HYPERLINK \l "SBa19" *28*), the authors have presented the advantages of using an ESP8266 based home system,

A. it provides a low-cost development board and enables the development of apps through Arduino IDE.
B. MQTT is a lightweight transport protocol that utilizes the network bandwidth. It also allows MQTT clients to subscribe to application messages that they need while ignoring the unnecessary ones.

The disadvantage of using ESP8266 for a Home Automation system is that it's only suited for IoT nodes which have few capabilities and resources; hence it can't be used on a large scaled environment.

The Raspberry Pi and Oblo Living system in *29*) has the following advantages;

A. Raspberry Pi is an affordable, customizable and configurable small computer that is able to support more peripherals and network communication devices.
B. the Oblo Living system simplifies the overall network architecture by providing a central based processing unit. It is connected to all sensors and actuators in the network and also to the internet. As a result, supervisory control units can connect to it remotely.
C. the system also uses MQTT protocol, which is a publish/subscribe based protocol thus eliminating unwanted messages.
D. security is also guaranteed in the network, because any connected device on the network must be authenticated by the gateway before being allowed access.

The Beehouse system in (HYPERLINK \l "Ali11" *30*) provides a slightly advanced module as compared to *28*), and (HYPERLINK \l "Mil19" *29*). It uses a Java based GUI and MySQL database. The GUI is split into two windows, the first showing the login page and the second highlighting the main systems interface. The intermediary for the connected devices is a breakout board known as the XBee Explorer USB and it links the Beehouse nodes to the Beehouse interface through the USB port.

4. Proposed Model

Of all the systems reviewed in this paper, the Ethereum and Blockchain based system in *27*) provides a more stable and efficient technique for implementing security on IoT based systems due to its advanced features and also its co-complementing aspects (drawbacks of using Ethereum alone are resolved by Blockchain and vice versa). However, the system can be made more secure by using a Hyperledger fabric together with Gemalto's Safe Net instead of combining Ethereum with Blockchain.

Hyperledger fabric is a private and 'permissioned' Blockchain network that requires its members to register through a Membership Service Provider (MSP). It also uses smart contracts and employs a distributed ledger system.

4.1. Implementation

The Hyperledger fabric network is made up of;

A. **peers –**
that execute chaincode, access ledger data, endorse transactions and interface with applications

B. **orderers –**
which ensure the consistency of the blockchain and deliver the endorsed transactions to the peers of the network

C. **users**
To guarantee secure authentication, the MSP's Fabric Certificate Authority uses the traditional PKI hierarchical model and generates a unique digital identity in the format of an X.509 digital certificate to every member in the network. These identities are used to determine the permissions and access levels of each member in the network.

By combining the Hyperledger fabric with Gemalto's Safe Net Hardware Security Modules the crypto key pairs for the identities of the members are generated and secured. Also, the crypto keys used in SSL and TLS network connections are generated and stored securely.

5. Conclusion

In the current tech world, Blockchain provides one of the most secure data protection mechanisms as it can't be altered retroactively, without the alteration of all subsequent blocks. Its implementation on IoT devices and networks would be a sensible strategy.

6. REFERENCES

[1] Xu, X. From cloud computing to cloud manufacturing. Robotics and Computer-Integrated Manufacturing 2012, 28, 75-86.

[2] Haenlein, M.; Kaplan, A. A brief history of artificial intelligence: on the past, present, and future of artificial intelligence. California Management Review 2019, 61, 5-14.

[3] Mohapatra, H.; Panda, S.; Rath, A. K.; Edalatpanah, S. A.; Kumar, R. A tutorial on powershell pipeline and its loopholes. International Journal of Emerging Trends in Engineering Research 2020, 8 (4).

[4] Mohapatra, H. HCR using neural network; Ph.D. dissertation; Biju Patnaik University of Technology, 2009.

[5] Mohapatra, H.; Rath, A. K. Detection and avoidance of water loss through municipality taps in india by using smart tap and ict. IET Wireless Sensor Systems 2019, 9 (6), 447-457.

[6] Mohapatra, H.; Rath, A. K. Fault tolerance in WSN through PE-LEACH protocol. IET Wireless Sensor Systems 2019, 9 (6), 358-365.

[7] Mohapatra, H.; Debnath, S.; Rath, A. K. Energy management in wireless sensor network through EB-LEACH. International Journal of Research and Analytical Reviews (IJRAR) 2019, 56-61.

[8] Nirgude, V.; Mahapatra, H.; Shivarkar, S. Face recognition system using principal component analysis & linear discriminant analysis method simultaneously with 3d morphable model and neural network BPNN method. Global Journal of Advanced Engineering Technologies and Sciences 2017, 4, 1.

[9] Panda, M.; Pradhan, P.; Mohapatra, H.; Barpanda, N. Fault tolerant routing in heterogeneous environment. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH 2019, 8, 1009-1013.

[10] Mohapatra, H.; Rath, A. K. Fault-tolerant mechanism for wireless sensor network. IET Wireless Sensor Systems 2020, 10 (1), 23-30.

[11] Swain, D.; Ramkrishna, G.; Mahapatra, H.; Patra, P.; Dhandrao, P. A novel sorting technique to sort elements in ascending order. International Journal of Engineering and Advanced Technology 2013, 3, 212-126.

[12] Broumi, S.; Dey, A.; Talea, M.; Bakali, A.; Smarandache, F.; Nagarajan, D.; Lathamaheswari, M.; Kumar, R. Shortest path problem using Bellman algorithm under neutrosophic environment. Complex & Intelligent Systems 2019, 5, 409--416.

[13] Kumar, R.; Edalatpanah, S. A.; Jha, S.; Broumi, S.; Singh, R.; Dey, A. A multi objective programming approach to solve integer valued neutrosophic shortest path problems. Neutrosophic Sets and Systems 2019, 24, 134-149.

[14] Kumar, R.; Dey, A.; Smarandache, F.; Broumi, S. A study of neutrosophic shortest path problem. In Neutrosophic Graph Theory and Algorithms; Smarandache, F., Broumi, S., Eds.; IGI-Global, 2019; Chapter 6, pp 144-175.

[15] Kumar, R.; Edalatpanah, S. A.; Jha, S.; Singh, R. A novel approach to solve gaussian valued neutrosophic shortest path problems. International Journal of Engineering and Advanced Technology 2019, 8, 347-353.

[16] Kumar, R.; Edalatpanah, S. A.; Jha, S.; Gayen, S.; Singh, R. Shortest path problems using fuzzy weighted arc length. International Journal of Innovative Technology and Exploring Engineering 2019, 8, 724-731.

[17] Kumar, R.; Edaltpanah, S. A.; Jha, S.; Broumi, S.; Dey, A. Neutrosophic shortest path problem. Neutrosophic Sets and Systems 2018, 23, 5-15.

[18] Kumar, R.; Jha, S.; Singh, R. A different approach for solving the shortest path problem under mixed fuzzy environment. International Journal of fuzzy system Applications 2020, 9 (2), 132-161.

[19] Kumar, R.; Jha, S.; Singh, R. Shortest path problem in network with type-2 triangular fuzzy arc length. Journal of Applied Research on Industrial Engineering 2017, 4, 1-7.

[20] Kumar, R.; Edalatpanah, S. A.; Jha, S.; Singh, R. A Pythagorean fuzzy approach to the transportation problem. Complex and Intelligent System 2019, 5, 255-263.

[21] Pratihar, J.; Kumar, R.; Dey, A.; Broumi, S. Transportation problem in neutrosophic environment. In Neutrosophic Graph Theory and Algorithms; Smarandache, F., Broumi, S., Eds.; IGI-Global, 2019; Chapter 7, pp 176-208.

[22] Pratihar, J.; R. Kumar, S. A. E.; Dey, A. Modified Vogel's Approximation Method algorithm for transportation problem under uncertain environment. Complex & Intelligent Systems (Communicated).

[23] Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R. M.; Srivastava, G. Security aspects of Internet of Things aided smart grids: A bibliometric survey. Internet of Things 2019, 100-111.

[24] Gayen, S.; Smarandache, F.; Jha, S.; Kumar, R. Interval-valued neutrosophic subgroup based on interval-valued triple t-norm. In Neutrosophic Sets in Decision Analysis and Operations Research; Abdel-Basset, M., Smarandache, F., Eds.; IGI-Global, 2019; Chapter 10, p 300.

[25] Gayen, S.; Smarandache, F.; Jha, S.; Singh, M. K.; Broumi, S.; Kumar, R. Introduction to plithogenic subgroup. In Neutrosophic Graph Theory and Algoritm; Smarandache, F., Broumi, S., Eds.; IGI-Global, 2020; Chapter 8, pp 209-233.

[26] Gayen, S.; Jha, S.; Singh, M.; Kumar, R. On a generalized notion of anti-fuzzy subgroup and some characterizations. International Journal of Engineering and Advanced Technology 2019, 8, 385-390.

[27] Seyoung Huh, S. C. S. K. Managing IoT Devices Using Blockchain 2017, 4.

[28] S. Balakrishnan, B. M. N. S. S. S. S. G. S. Home Automation System using ESP8266 based MQTT 2019, 4.

[29] Milosevic Milos, N. C. J. K. T. A. Lighting Control Using Raspberry Pi and Oblo Living Home Automation System 2019, 10.

[30] Ali Mohammed A, H. A.-K. D. C. O. S. A. A. V. P. User Friendly Smart Home Infrastructure: BeeHouse 2011, 6.

[31] Elike Hodo, X. B. A. H. P.-L. D. E. I. C. T. a. R. A. Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System 2016, 6.