Paper No CBGMW – 2019 – 019

A REVIEW ON THE DEVELOPMENT OF A SECURED INFORMATION SYSTEM FOR IOT BASED LIGHTING SYSTEM

Victoria Olasumbo[1], Olatunji Eniola Ifeoluwa[2], Oluwaremilekun Jacobs Adeopatoye[1], Abiodun Musa Aibinu[2], Sodiq Olanrewaju Akanmu[2], Taliha Abiodun Folorunso[2]

[1]Department of Cybersecurity Science Federal University of Technology Minna, Niger State

[2]Department of Mechatronics Engineering Federal University of Technology Minna, Nigeria.

victoria.olasumbo@st.futminna.edu.ng
eniolam1000752@gmail.com
remilekun.adeopatoye@st.futminna.edu.ng
maibinu@gmail.com
sodiq.akanmu001@gmail.com
funso.taliha@futminna.edu.ng

Abstract

Internet of Things is increasingly becoming a disruptive technology with various standards emerging primarily for wireless communication between devices and gadgets in the everyday life of a human. - The Internet of Things ' primary goal is to connect most too frequently used objects which has access to the internet and the ability to sense its environment, with or without the involvement of humans. The comprehensive use of the paradigm itself leads the current networking technologies to face conventional safety problems. Therefore, development of software or hardware for IoT devices requires some security measures such as cryptographic techniques. This paper presents reviews of various works that developed both software and hardware systems for IoT, it discusses the methodology and the significant result obtained from various project works.

***Keywords**: Cryptography, Information System, IoT, Lighting system.*

1. Introduction

Information System consists of hardware, software, database, network and individuals organized as a set of components for data collection, storage, processing and providing information. The interrelated processes among these components of information systems allow for the exchange of data that are generated daily by these processes and the generated data must be processed into meaningful information. The Internet of Things (IoT) is altering the information system's nature and scope. The IoT idea enables these devices to interconnect into our everyday objects, enabling humans to regulate and handle the activities and data of objects operating under their environment's distinct information systems using evolving communication technologies.

In recent times, IoT has enabled everything and anything to be connected to the internet across the distinct domains of life. Many sectors have been converted and even smarter than ever, ranging from healthcare to production, services, transport and housing as its effects have made an incredible impact as a universal solution media. IoT can minimize human efforts, the fusion of IoT into home automation is creating a buzz in the IT industry. It analyzes the sensor information and conducts suitable operations to save human time. IoT analyses the information recovered from the sensors and performs fitting exercises along these lines saving human time. The affirmation to individuals about their home exercises and protections prompted the advancement of the Home Automation

System. Using IoT, Light bulbs, coolers, drones, pet feeders, sensors, intelligent TVs, digital set-top boxes, security cameras, wearables, automotive and medical devices can now be connected to the Internet. IoT is described as a smart and interoperability node interconnected in a vibrant worldwide network of infrastructure, which also seeks to enforce the notion of connectivity from anywhere at any time. As IoT connected systems continue to develop rapidly, security is one of the greatest and most complicated problems facing IoT devices since the devices are connected to the internet hence making it vulnerable to significant attack.

The Security needs to manage the accompanying issues: avoiding information breaks (ensuring that unauthorized entities can't get to the data), authorization (characterizing entities that have access to the data) and guaranteeing the protection of the user. (Kamel & Hegazi, 2018) Different techniques have been used to develop systems for IoT, such as ZigBee wireless sensor network (Amare, Sengupta, & Research Scholar, 2017) and frugal labs IoT platform (flip) (Malche & Maheshwary, 2017). However, IoT integrated with PC vision, IoT mix with PC vision web services and cross-platform mobile services, Wi-Fi, Raspberry Pi, and connectivity are incorporated to better design IoT systems (Moubarak, 2016), (Rodge, Prajapati, Salve, & Sangle, 2017), (Pirbhulal et al., 2017). Encryption and authorization schemes such as AES, RSA, HMAC, and cryptographic algorithms are used to protect the stored data (Salim & Harba, 2017).

2. *RELATED WORKS*

The development of an IoT based home automation system that utilizes personal computers or mobile phones to manage essential home capacities automatically was reported by (Nandha, Kumar, Asst., & Asst., 2017). Android application which consists of main operations like light controlling, entryway controlling, smoke location and Temperature detecting was developed. Once the app starts, the user is initially attested, if the user is permitted, he is navigated to the main screen. The main screen contains a list of all operations among which the user can select any one function that he/she wishes to regulate. Once chosen, he would be able to see a current device to attach to the microcontroller. The Android Development Kits (ADK) board provides input and output pins that are just implemented through the utilization of attachments which is referred to as "shields." With an Android device and the Mega ADK, the user will be able to use all the sensors and actuators you need to form accessories. This might embody a Light Emitting Diode (LED) outputs, and temperature and light sensors, if the user desires, he will change or impair the implied gadget. The system is savvy enough to initiate caution once smoke is identified or to consequently on/off lights all through night hours. If the temperature goes awfully high or low, it will naturally Adjust the fan/AC according to the temperature. The system doesn't exclusively screen the detecting component data, similar to temperature, gas, light, movement sensors, however, it actuates a method per the need. It moreover stores the detecting component parameters inside the cloud (Gmail) in a very timely manner but the weakness in the system is that an attacker can hack the android application that controls the appliances and alter the application. Hence, there is a need for authentication before authorization. The method allows the system to additionally store the detecting component parameters inside the cloud (Gmail) in a convenient way which may encourage the user to examine the state of condition inside the home anytime and appliances were efficiently remotely controlled over the internet.

(B. Prakash, 2018) Reported on, the implementation of IoT to monitor and control home appliances through World Wide Web (WWW) HTTP / HTTPS protocols. The front end is designed with the use of HTML and CSS, with a database developed using MySQL. The development was implemented on an eclipse IDE whose programming language is Java and an Arduino IDE which uses the C++ programming language. Android smartphone is used to control the hardware. This technique makes it possible for the embedded system to handle and operate the devices at home even if the internet membership is down or the server is not up. But authentication is the limiting factor in the system, the technique is not using an authentication scheme. Communication with the server allows the user to select the appropriate device and communicate with the server so that the method is efficient. A system that controls home devices via smartphones was accomplished.

(Rodge et al., 2017) reported the development of a system that controls all electrical devices in an office. A Raspberry pi was used which required the installation of an operating system with other setup configuration After loading OS, Unlike the default user password, language, username, command line, etc., different settings settings were made. Connecting electrical equipment to the circuit is linked to Raspberry pi via Raspberry pi's general-purpose input / output (GPIO) pins. Azure cloud services for cloud connection are linked to Raspberry pi and mobile apps. The programming on the server side is performed in .NET framework and XMLThe Raspberry pi's activities were controlled by programming languages used to create a mobile application. The scheme enables customers to communicate without stretching to the gate with the tourists. One of the biggest faults in this scheme is that of data integrity. The method makes it easy and comfortable to access various appliances in the office which is controlled through mobile.

Accessing the web through smartphones allows home automation to be handy, (S. Singh, H. Matharu, 2017) developed an IoT based system that controls multiple devices with a mobile device. An ESP module was integrated to offer an inbuilt strong range of Wi-fi connectivity. Data is sent to the server that is stored in a buffer memory that is then transmitted via Wi-Fi to the cloud and the activities are conducted on information. The key processing of Raspberry Pi is used. The fixed regulator is configured to allow a certain amount of current while a range of current can be passed by the variable regulator. Different electrical and electronic parts, modules, blocks & connecting cables are used to connect home automation using IoT circuit. The technique enables the gate opening system to be based on a digital lock that compares a piece of encrypted code sent by the user but does not encrypt the signal sent to the server on the client side, thus opening it up to the man-in - the-middle attack. The method ensures that even when the cloud or the database is compromised the security code is not understandable by the hacker and a low-cost system that allows a user to access multiple appliances over the internet conveniently was achieved.

(B. Bakare, F. Odeyemi, 2015) Developed a system that allows the user to control a lighting system remotely using the Global System for Mobile communication (GSM). The GSM modem gets and sends the signal to the microcontroller when the GSM phone transmits the signal through Short Message Service (SMS). The microcontroller will access the SMS and alter the device status if the signal is a suitable code. Then the microcontroller sends a signal to the GSM modem to send a response via SMS to the GSM phone. The switches are the alternative way to modify the equipment status if the homeowner is close to the end of the transmission, the switch buttons can be used to modify the equipment status. When a state change happens, the buzzer will notify. The switches are the alternative way to modify the equipment status if the homeowner is close to the end of the transmission, the switch buttons can be used to modify the equipment status. When a state change happens, the buzzer will notify. Hence, the user is aware of activities carried with the appliances but security is not put consideration. Since the message is sent in plain text via SMS, anyone gets access to how the security light and other appliances are controlled. Hence, there is a need for an encryption algorithm to better secure the appliances.

A secure file transfer-based system designed with encryption and authorization scheme using Advance Encryption Standard (AES), Rivest Shamir Aldeman (RSA) and Hashbased Message Authentication Code (HMAC) were reported [8]. Receiver uses the RSA algorithm to produce important pairs (public and private keys) and provides the public key value to the sender. The sender utilizes 256-bit cipher keys to use the AES algorithm to encrypt data. The significant asymmetric algorithm (RSA algorithm) is used to encrypt the symmetric key with the public key of the recipient. For calculating the MAC with a combination of a hash function and a secret key, a HMAC SHA256 is used. The plaintext encryption ciphertext is then appended to MAC from the encrypted plain text. The receiver decrypts the AES key by using the stored key (private key) and then decrypts information using the AES key. To create a strong security system, the three kinds of encryption are combined to exploit the benefits of each. The technique utilizes three (3) hybrid features that result in powerful system safety being coupled with each other. The outcome indicates that the text size rose from 144 pieces to 784 and the time for encryption is less than 1 second.

Encryption of generated data will protect the data from unauthorized access enhancing the security of the IoT system, (Bokefode, Bhise, Satarkar, & Modani, 2016) developed a secured cloud system with a cryptographic algorithm to store IoT data IoT systems are positioned to retrieve information if phones are unable to connect to the Internet and are unable to transfer information, then gateways are used to provide the necessary connectivity as an intermediate between stuff and the cloud. The administrator defines the roles according to the organization's work functionality, and then adds the system user who wants to access the cloud storage data stored according to their needs. The administrator also generates one role manager to handle the user's roles and gives access rights. The role manager assigns the user the specific tasks and has the power to remove the user's allocated position. After that, the administrator encrypts and stores the collected machine data for a particular location in the cloud storage so that only consumers with appropriate roles can decrypt and display this data. The system allows a public cloud organization to securely upload IoT data. It provides great message encryption and decryption effectiveness. In addition, data collected from IoT devices is stored in an encrypted format so the cloud provider is unable to view or read the information. The method is useful in various company organizations where data is collected from IoT devices and job features are divided according to user-played roles in organizations. The information gathered from IoT devices are safely uploaded to cloud storage by implementing cryptographic methods for AES and RSA.

(Liu, Ying, Fan, Tsunoo, & Goto, 2011) design and implemented a secure system for AES core on Side-channel Attack Standard Evaluation Board. A set of data registers was introduced to save the intermediate value and ciphertext / plain text individually. The two sets of data registers will be placed in a separate location. A random number generator is used to select randomly which set to save the intermediate value and to make sure that the text / plaintext is saved in the other set. If Differential Power Analysis (DPA)attack chooses the intermediate to determine the position of the two register sets, a nonlinear operation is needed. And the only nonlinear procedure in AES is Sub-Bytes if the two sets of registers are on the same side of Sub-Bytes that the attacker can analyze in the first or last round of AES. The random number generator uses a one-bit register. In the first round, after exclusive plaintext OR and original key, we pick a binary number generated in the first round. We select one binary number from the consequence of the former round in the other rounds. The technique used for each AES round selects a set of registers, so attackers are unable to understand the information of each AES round. This method ensures the attackers are unable to attack AES efficiently and the system is therefore secure. Implementation of a low-cost AES core with low-cost countermeasure and highly secure apps like smart cards and embedded systems.

Increasing security in the implementation of AES, (Zodpe & Sapkal, 2018) reported on the use of Field Programmable Gate Array (FPGA). The key required for encryption / decryption is generated using the PN sequence generator. Using the 8bit PN sequence generator, the key block generates the initial key required for the encryption / decryption process. The 8bit PN sequence generator generates 255 8bit values each which can be concatenated to form the initial 128bit key. The key generation block selects internally the concatenation bytes and forms the 128-bit key. The output state of the PN Sequence Generator (each 8-bit) is stored in the Lookup Table (LUT) and provided as a multiplexer input of 256:1. An 8bit counter generates the 8bit row selection value of the multiplexer. The important comprises of 16 separate bytes and is acquired by altering the counter's original value for select lines by a big number of separate keys. These keys can then be dynamically implemented from the entire document to be encrypted to distinct 128-bit plain text blocks. One of the strengths was that the traditional AES algorithm fitted with the modified S-box method of the project and enhanced key generation method provides a 60 percent avalanche effect making it invulnerable to attack. This technique enables the design to synthesize and compare different FPGA equipment with current models that make the system effective. When synthesized on XC6VIX240T device with a maximum frequency of 463.42 MHz and 30.39 Gbps, the project achieves a 59.3Gbps throughput when implemented with a maximum frequency of 237.45 MHz on XC6SLX150.

To enhance the level of security of the existing AES algorithm, (Al- Mamun, S. M. Rahman, Ahmed Shaon, & Hossain, 2017) reported an inclusive analysis related existing works. The key size is 8 bits to boost the time of the brute force attack. This means expanding the present key size from 128 to 136, from 192 to 200, and from 256 to 264. This extra 8 bits is produced for encryption by a user-defined function called "getRandKey)" (and is secretly stored for further decryption use. The 8bit key is used when executing "getSBoxValue)." During the key expansion and the execution of SubBytes step for each round, the 8bit random key is Xor'ed the replaced s-box value in getSBoxValue. The main extension time improves considerably, making it more time-consuming for the brute force attack. The current key is expanded from 128 to 136, from 192 to 200, from 256 to 264 making it almost impossible to attack brute force. Modification of the current AES algorithm by XORing an extra s-box-value byte effectively improved the Time Security and Strict Avalanche Criterion, thus making the technique effective. The proposed plan's time safety increases 256 times compared to the existing system and the proposed system's strict avalanche effect is greater than that of the existing system for all key sizes 128, 192 and 256.

(Pirbhulal et al., 2017) worked on the use of C language to develop an IoT-based System to connect items of everyday life to the internet. The TMP36 temperature sensors used to capture the temperature of the environment that serves as the dataset. Both the temperature sensor and the Wi-Fi module were incorporated into a microcontroller board based on Intel Galileo. The Galileo board includes a 32-bit Intel Pentium-class system mounted on a chip comprising an Arduino Software Development Environment (IDE) in combination with an Intel fast data processing processor. This board is used to build a intelligent wireless sensor node, and the Wi-Fi module is mounted alongside the temperature sensor on the board to generate a sensor node. Sensor nodes are designed to use Wi-Fi as a wireless medium to collect data and then store the sensed data on the server. A Thing Speak server will be used to store the recorded data after appropriate authentication and the stored data will be transmitted to the destination node. The source node uses an encryption algorithm to generate data that is encrypted. The advanced IoT-based system meets all the required safety criteria, this model's architecture consumes less energy as it utilizes TBSA thus making the model more power-efficient. A security-based algorithm (TBSA) is a key generation process that is easy and effective.

(Surayati, Usop, Abidin, Wahab, & Kamaruddin, 2017) developed a secured system that transfers a file peer-to-peer from one computer to another computer using a JAVA application on the same Local Area Network (LAN). For the development of a file transfer scheme, Encryption Standard, 3DES, RSA and Blowfish were used. Symmetric keys provide the mechanism of communication between two encryption and encryption of Asymmetric keys. Before transmission is formed between the couple of sockets, a link is created for the key over the TCP protocol to distribute important first. Sockets listen to a link request (server) for the Asymmetric key encryption or public key, two keys are used (personal and public keys). The method provides the necessary authentication for the transfer of files in the network transmission, but the encryption scheme requires the party encrypting the data to know the secret key and the party decrypting the data, thus exposing files to hacker interception. Applying AES to file transfer systems can prevent hackers from attempting to steal any data during file transfers, making the technique effective. The scheme enables a file to be transferred safely over the internet.

(Marwaha & Bedi, 2013) Analyzes the feasibility of using a data security and privacy encryption algorithm in cloud storage. A scheme has been created that offers safety and privacy for cloud storage to create an encryption-based scheme to protect cloud-based sensitive data and structure how owner and storage service provider work on encrypted data Create a scheme where the cloud data is stored by the consumer. The data is transmitted and stored in encrypted form on the cloud, a retrieval system in which the user retrieves data in an encrypted form and is decrypted by the user at their site using an asymmetric key algorithm (public and private), both keys working at the user level. This method hides the meaning of data such that no unauthorized persons get to know the plain text. It uses an encryption algorithm hence prevent data from been altered even if access is gained by an unauthorized person. The system protects the message by an encryption algorithm.

Security and privacy issues can be overcome by employing encryption, security hardware, and security applications. Hardware is important in the architectural development of IoT, (Moosavi et al., 2015) reported Using intelligent gateways to implement a secure IoT-based healthcare system. A platform has been set up that includes medical sensor nodes, UT-GATE intelligent e-health gateway, remote server, and end-users. The UT-GATE offers end-user medical data from medical sensor nodes. UT-GATE is built from a Pandaboard21 mixture and Texas Instruments (TI) SmartRF06 board is embedded with CC2538 module22. The Pandaboard is a low-power, low-cost single-board computer development platform based on OMAP architecture based on TIOMAP4430 System-on-Chip (SoC) and manufactured using 45 nm technology. The OMAP4430 method consists of the sub-system Cortex-A9 microprocessor unit (MPU) including dual-core ARM cores with symmetric multiprocessing up to 1.2GHz each. 8 GB of internal memory is added to the Pandaboard and driven by Ubuntu OS controlling equipment and services such as notification. The technique decreases the medical sensor overhead without compromising the safety. The technique was based on the DTLS handshake protocol based on certificates, which is IoT's primary Internet Protocol (IP) safety solution. Communication overhead is decreased by 26 percent at the end of the project and communication latency is decreased by 16 percent from the intelligent portal to the end user.

Sensors allow physical data to be detected from the real world, (Amare et al., 2017) implemented a smart campus for the internet of things based on ZigBee wireless sensor network. IoT gateway connects the device and translates the protocol. ZigBee communication protocol sensors communicate with each other to exchange information ZigBee provides the packet-based radio protocol with routing and multi-hop features that use digital radios to allow devices to communicate with each other. A network manager creates the network and manages node data and transmitted / received data within the network. A server is linked to the internet to collect and store data from the wireless sensor network via their IoT gateway. The server's IoT gateway uses a website to access and regulate sensors. Therefore, this scheme encourages all aspects of the campus and produces an efficient IoT platform. Ultimately, the level of development that sees down-to-earth recognition of

IoT contracts and administrations has been achieved, beginning with field trials that ideally help clear the vulnerability that maintains a enormous spectrum of the IoT worldview.

(Ensor, 2015) used a motion system to develop an automated and secure system that controls lighting. The Passive Infrared Sensor (PIR) detects motion and the output is pin HIGH. To amplify the PIR signal, an op-amp is used. When the microcontroller's input unit gets a signal, the amplified signal input for the microcontroller and the output pin energizes the relay to turn the light on. Optocoupler is used to join two different power sources with a 12V relay been used to switch the lights ON and OFF. For op-amp, the microcontroller gets a fair amount of signal which gives the pulse to work as the programming is done. The method used motion sensors hence effectively save power. It is difficult to make the system operated only by the movement of humans because the system cannot differentiate between different objects of the same temperature range. Thieves may also discover it simple to fool the detection variety of PIR as they have a slotted detection area and not one like a microwave sensor continuously. The PIR sensor provides the microcontroller with a strong signal. The method is therefore effective. An efficient and time-consuming project with the use of PIR sensors.

(Kamel & Hegazi, 2018) worked on a secured management system as regards to IoT security. A security management system was developed for the IoT network to decrease time and power consumption and provide suitable security mechanisms for the IoT security layers. The system selects and manages the appropriate security mechanisms to achieve low consumption power and time. The method used enables the system to select suitable IoT security layers, processes, and protocols. It also enhances IoT network performance by choosing the appropriate security mechanisms to reduce energy and time consumption for IoT layers. The system provides security requirements to secure multiple application.

3. CONCLUSION

The Increasing use of IoT for home automation creates the need for proper implementation of security features across every technology implemented. Security is of great importance in the technology world, generally, a smart home is vulnerable to an internal attack when the cybercriminal is close to the house and an external attack where the Internet connectivity is used to commit a crime. The attacker intends to compromise the infrastructure of the smart home or acquire access to data stored via cloud services. Papers of various work that developed both software and hardware systems for IoT without putting security into consideration are reviewed in this study. To overcome this problem of security, a secure information system for IoT based security lighting system using some cryptographic algorithms such as AES, DES, RSA to protect data before transmitting over the internet can be developed. Username and password are required for authorization in the system, as the password will be encrypted using a selected cryptographic scheme.

REFERENCES

Al- Mamun, A., S. M. Rahman, S., Ahmed Shaon, T., & Hossain, M. (2017). Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte. *International Journal of Computer Networks & Communications*, 9(2), 69–88. https://doi.org/10.5121/ijcnc.2017.9206

Amare, B., Sengupta, J., & Research Scholar,]. (2017). Internet of Things (IoT) Driven Design and Implementation of Smart Campus. *International Journal of Computer Science Trends and Technology (IJCST)*, 5(4), 32–38.

B. Bakare, F. Odeyemi, F. (2015). Switching Of Security Lighting System Using Gsm. *American Journal of Engineering Research*, 4(1), 126–137.

B. Prakash, el al. (2018). IoT based Monitoring and Control System for Home Automation using

Prediction Algorithms. *International Journal of Research*, *5*(12), 4120–4124. https://doi.org/10.17148/ijarcce.2017.6614

Bokefode, J. D., Bhise, A. S., Satarkar, P. A., & Modani, D. G. (2016). Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption. *Procedia Computer Science*, *89*, 43–50. https://doi.org/10.1016/j.procs.2016.06.007

Ensor, M. O. S. (2015). Automatic Lighting and Security System Design Using Pir Motion Sensor. *Journal Institute of Information Technology*, *14*(8), 1–5.

Kamel, S. O. M., & Hegazi, N. H. (2018). A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security. *International Journal of Scientific and Engineering Research*, *9*(9), 1227–1244.

Liu, H., Ying, Z., Fan, Y., Tsunoo, Y., & Goto, S. (2011). Information hiding for AES core based on randomness. *Procedia Engineering*, *15*, 2113–2117. https://doi.org/10.1016/j.proeng.2011.08.395

Malche, T., & Maheshwary, P. (2017). Internet of Things (IoT) for building smart home system. *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, 65–70. https://doi.org/10.1109/I-SMAC.2017.8058258

Marwaha, M., & Bedi, R. (2013). Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing. *International Journal of Computer Science Issues (IJCSI)*, *10*(1), 367–370. https://doi.org/10.1007/978-981-287-990-5

Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, *52*(1), 452–459. https://doi.org/10.1016/j.procs.2015.05.013

Moubarak, M. H. (2016). Internet of Things for Home Automation. *Researchgate.Net*, 1–25.

Nandha, D. S. M., Kumar, K. G. A., Asst., P. M. R., & Asst., S. (2017). IOT Based Home Automation and Security System. *INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN BASIC ENGINEERING SCIENCES AND TECHNOLOGY*, *3*(24), 639–644.

Pirbhulal, S., Zhang, H., Alahi, M. E. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y. T., & Wu, W. (2017). A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors (Switzerland)*, *17*(1), 1–19. https://doi.org/10.3390/s17010069

Rodge, P., Prajapati, J., Salve, A., & Sangle, P. (2017). IoT Based Smart Interactive Office Automation | Internet Of Things | Cloud Computing. *International Research Journal of Engineering and Technology*, *4*(4), 982–986.

S. Singh, H. Matharu, S. M. (2017). International journal of engineering sciences & research technology internet of things (iot) based home automation system. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES $ RESEARCH TECHNOLOGY*, *6*(11), 239–244.

Salim, E., & Harba, I. (2017). www.etasr.com Harba: Secure Data Encryption Through a Combination of AES. *Technology & Applied Science Research*, *7*(4), 1781–1785.

Surayati, N., Usop, M., Abidin, A. F., Wahab, F. A., & Kamaruddin, N. U. (2017). Securing File Transferring System by Implementing AES Algorithm. *World Applied Sciences*, *35*, 122–132. https://doi.org/10.5829/idosi/wasj.2017.122.132

Zodpe, H., & Sapkal, A. (2018). An efficient AES implementation using FPGA with enhanced security features. *Journal of King Saud University - Engineering Sciences*, 1–8. https://doi.org/10.1016/j.jksues.2018.07.002