Securing IoT Communication between Controller and Application using AES-128

Er. Sharanjeet Kaur[1], Dr. Gurjit Singh Bhathal[2]

[12]*Department of Computer Science, Punjabi University, Patiala*

Abstract -Internet of Things of IoT is one of the emerging technologies in the contemporary world. The concept of IoT is outperforming by assimilating with cloud and automation sector. Thus, many people get lured to this concept and starting working on these technologies. Each day, plenty of objects or devices get connected with internet at burgeoning rate. However, the biggest challenge is the issue of providing security to IoT based devices, for which lightweight and robust cryptographic algorithms are being used in microcontroller. By doing this, the performance does not get affected by this, and it provides the efficient solution to security. AES algorithm is considered as best cryptography algorithm than any other counter algorithms. Nonetheless, such systems are not being used as it has very low processing capability and it is mostly 8 bits. Nowadays, Single Board Computers have been incorporated since they are capable of supporting full operating system having better processing power, more storage space, and sensors can be attached to it. In this paper, implementation of single board system has been discussed with DHT11 sensor that sends the data of temperature and humidity to thingspeak cloud API. Also, the AES 128-ECB encryption method has been used.

Keywords – IoT, Raspberry Pi, AES, Cryptography, DHT11, Thingspeak

1. INTRODUCTION

Since Internet of Things has a wider scope, myriad devices have been connected to it, and thus performing automation. There are mainly four different parts – Sense, Collect, Analyze, and React. The standalone unit capable of being controlled remotely can be referred to as Internet of Things. The US National Security and Telecommunications Advisory Committee (NSTAC) has proposed IoT based applications on three shared common principles as described in fig 1.1.

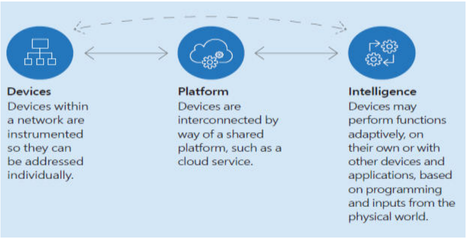
Devices
Devices within a network are instrumented so they can be addressed individually.
Platform
Devices are interconnected by way of a shared platform, such as a cloud service.
Intelligence
Devices may perform functions adaptively, on their own or with other devices and applications, based on programming and inputs from the physical world.

Figure 1.1 – Three Common principles of IoT [4]

The objects of IoT are combined with microcontrollers and sensors that enable communication with each other. We can consider objects, such as people, devices, animals, vehicles and so on. In other words, mobile to car, coffee making machine can be take into consideration as internet via free source IPV6 that flows the data without any intervention from a human or computer. IoT devices have the capability to gather, analyze and process the data for information parsing. IoT chiefly has three things, people, connectivity and processes. The popular applications of IoT include Smart cities and healthcare, smart home, digital farming and so on. It saves the crucial time resources along with the manpower. This means every individual identity and thing have their own space along with specific address over the internet. There are several factors which are required to manage the Internet of Things insight of certainty, and safety. Over the internet, users are constantly vulnerable to threats and ever-growing nature of internet disturb the functionality and its meaning that stress in exploiting the important foundational delicacy. Unfortunately, this is not true for IoT devices. The main purpose of this is to obstruct the development of such model and to minimize the effect. Therefore, better understanding of elements and advancement is paramount. Many Mobile-based application are pervasive in nature and alluring customers. Similarly, the sensory devices are in this race to facilitate multitude extent of information to enhance customer experience.

2. IoT Architecture Model

The term Internet of Things mainly revolves around two words, i.e. Internet and Things. Things can also be called as objects with a unique identity with the ability to perform remote sensing, actuating and also real time monitoring in different sorts of data. These objects can communicate with different objects and application and share data on certain parameters. The term “Internet” mainly defines a global communication network used to connect trillions of computing machines across the planet[8] that also helps in information sharing. IoT does not have a standard model yet, but its architecture fig1.2 revolves around below illustrated model specified with three major layers :

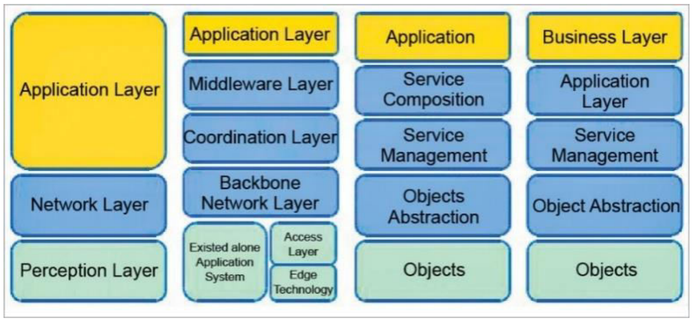

Figure 1.2 – IoT Architecture[14]

Perception Layer – It is the physical layer that includes sensors for sensing and gathering information. It identifies the smart objects on the basis of various parameters in the environment.

Network Layer – It connects the application layer with the perception layer. It connects with servers, network devices like routers and other smart things. It transmits and processes sensor data.

Application Layer – This layer provides application based services to the user. It provides the user interface that shows the details to the user like if he wants to switch on some device and he is sending some inputs or requests to the sensors to retrieve the data.

3. Security Issues with IoT

IoT is a revolution in almost any industry and is changing the way work is done with more and more emphasis on automation using Internet Connected Devices. But when internet is involved, one biggest concern becomes the security and privacy of the devices and data connected with Internet. Google and Amazon are two of the largest companies in IoT at the moment with the plethora of the devices they introduced in the last year including APIs[6] to make work simpler for the users. This IoT revolution will not be stopped soon, and here are some of the biggest security and privacy issues that a client and business have to consider before connecting their devices and data with the humongous Internet :

- **More devices, more problems:** Network Firewall is an important part of a client or company's network as all devices work behind a firewall and if the packets need to travel to the internet from internal network, they have to go through the firewall. Time is changing very rapidly, around ten years ago, we at homes were worried to protect and secure the computers, five years ago, we were worried to secure data on our smartphones too and now new devices connecting with internet like our home appliances, cars, our wearables, etc have added to our worry. Yes, Firewall is there as a security appliance to stop outside traffic originated from external network towards internal, but hackers still have ways to enter the network as there is no such thing as hundred percent security in the network. What IoT bring is that it provides hackers with a much bigger ground to play with lots more devices than before which they can hack. For example, if hackers hack our car and remotely control it and there is nothing that you can do. Hackers can also hack a patient's or baby's health monitoring band which can make good bit of damage. A figure 1.3 shows how a hacker can bring problems to you, if IoT is not secure :

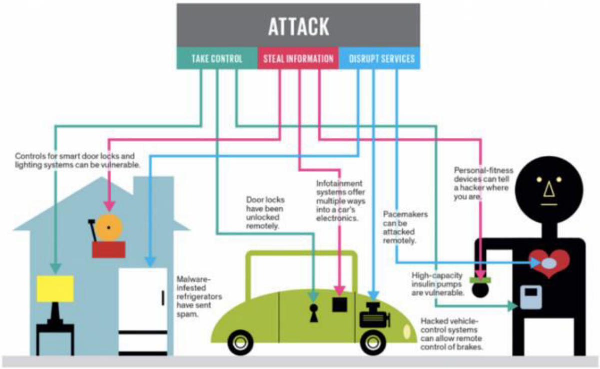
ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Pacemakers can be attacked remotely.
Personal-fitness devices can tell a hacker where you are.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

Illustration: J. D. King

Figure 1.3 – IoT Security Issues[15]

- **Lots and Lots of updates:** One thing that every network security professional will tell you is "Security policies have to be dynamic", yes, and it is true. When you buy any software like Microsoft Windows 10, Microsoft sold that to you by saying that it is secure, but with the time, hackers discover some vulnerabilities in the Windows 10, and when Microsoft comes to know about the vulnerability, they start to make security patches or security updates to their Windows 10 customers [6] so that hackers could not exploit the vulnerabilities. It is related with IoT products that you bought from companies like Amazon, Google etc. When you buy an IoT device, it is safe when you bought it, but hackers eventually discovered some vulnerabilities that makes the product unsafe. Therefore companies making IoT devices have to come up with lots and lots of updates as security patches to cover the vulnerabilities. So if you are not updating your device or have turned it off, like the people does when they installs pirated software, then security is compromised. Also when some software upgrade is end-of-life from the company and they do not provide any updates or patches and you are still using that software, then your software becomes a easy exploit for hackers. For example, there are still lots of companies or people using Microsoft XP while the support for Microsoft was ended in year 2014.

- **Lazy and unaware customers :**Automatic updates are used because humans are to perform basic steps to update the computer with latest updates and keep their computing machine safe[5] If they are not able to protect a single computing device by updating manually, how can one protect IoT devices. While companies making IoT products like Amazon, Google, Samsung etc are taking IoT security seriously, but in all the cases, the first line of defense is consumer itself. These IoT devices can be used against the consumer by the hackers if security is not applied on time. Select your IoT vendor carefully, as smaller vendors can offer you much cheaper price with some extra attractive features, but in case that small company folds, then there will be no one to patch the security vulnerabilities.

- **Data Protection from corporates :**Hackers are not the only ones, who you have to be scare of. Large corporates which distributes these IoT devices can also collect your personal[1-2] information and it becomes much more dangerous when they use it while you are doing money transactions. For example, there are companies which have distributed their employees wearable's like Fit bits, so that they can track their health and get lower health insurance premiums. Companies can also sell data to other companies which automatically violate individual privacy rights.

- **Data Encryption and Authentication :**IoT involves collection of data from sensors to the cloud or any application which is linked with IoT device. There are billions of devices [10] connected with Internet. Data processing is an important part between IoT device having sensors and the cloud running the application. Most of the data is personal which has to be secure using the strong encryption standards, otherwise Man-in-the-middle attacks or information leakage can become a big issue and will be a direct threat to consumer. There are two parts of security which has to be done in the securing the channel which can be securing the data and the network which most probably be wireless. Authentication is also very important part of the security, there has to be proper authentication in place between the IoT device and the application, otherwise open connectivity [11] can do a lot of damage. For example, if you have a temperature sensor at your smart home, which sends data to the application in encrypted form, but if there is no authentication, anyone can generate fake data and tells the application to instruct the AC to cool the room, even if it's cold already.

- **Side Channel Attacks:** Even if one can have encryption[1] and authentication in place, it will still leave a chance of side channel attacks. In this type of attacks, hacker is not focused on information, but on how information is presented. It can be information presentation like power consumption, timing information etc. The above discussed security issues along with the Proactive and Reactive approaches needed to be taken for countermeasure are listed in table 1.2.

Table 1.2 – IoT Security Issues

SNO	Security Issue	Proactive Approach	Reactive Approach
1.	Lots and Lots of updates	Auto-updates	Scan the application to find any vulnerability issue and apply updates forcefully, and then turn on auto-updates.
2.	Lazy and unaware customers	Give customers an easy to use interface and manuals.	Scan the application and contact technical support in case of any vulnerability
3.	Data Protection from corporates	Do not save your Debit/Credit Card information permanently on any application.	Block the cards/Change the pin in case of transaction issue.
4.	Data Encryption and Authentication	Use complex passwords and encryption standards.	Change Passwords immediately, and use some complex encryption standard.
5.	Side Channel Attacks	Use strong authentication and end-to-end encryption	Change encryption to end-to-end.

4. RESULTS

For the experiment purpose, we have setup the IoT environment with the help of Raspberry Controller and DHT11 sensor that sends the data to Things Speak server and perform IoT Analytics. Further, it stores the data that is transmitted by IoT sensor on internet. For this, we have Raspberrrry3b as shown:-

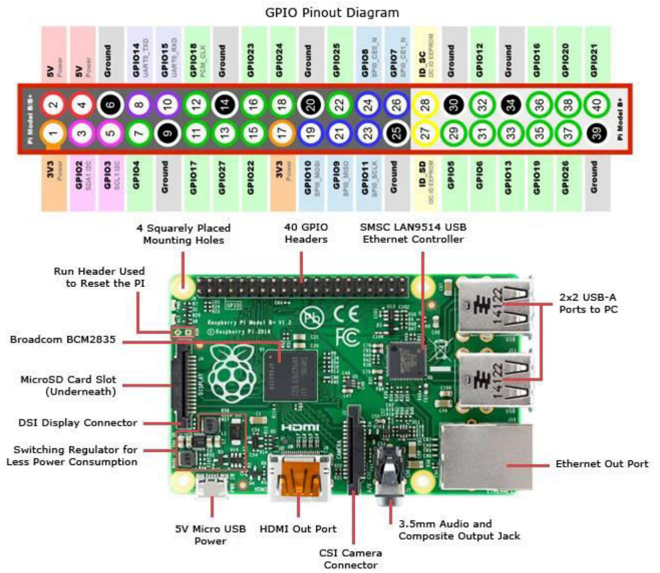

Figure 4.1 – Raspberry Pi 3b Pinout Diagram used in IoT work

Raspberry Pi 3 Model B is a microcontroller model of 3rd generation from Raspberry Pi. It is replaced by Raspberry Pi 2 in February 2016. It has the following specification:

- Quad Core 1.2GHZ Broadcom BCM2837 64-bit CPU
- 1GB RAM
- WLAN Card
- Bluetooth Low Energy Card
- 40-pin GPIO
- 4 USB Ports
- HDMI Port
- Camera Port to connect RPi Camera
- DSI Display port to connect RPi touchscreen display
- Micro SD Port
- Micro USB power source

As per the official website, Raspberry Pi 3 Model B will be used in production till January 2026. Apart from Raspberry Pi, we have used a HDMI to VGA converter to display the Raspberry Pi results as shown below:

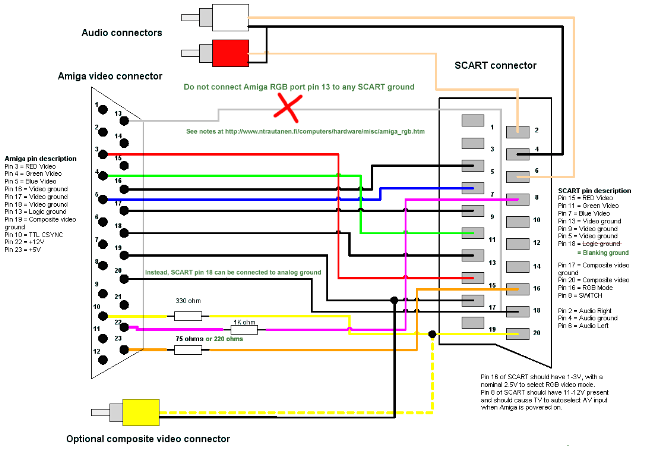

Figure 4.2 – HDMI to VGA Converter

DHT11 Sensor is used to monitor the temperature and humidity of the room. This sensor comes with 8-bit microcontroller. DHT11 has the technology that ensures the higher reliability and great scalability. This sensor has an element resistant and sensor which can be used for measuring wet temperature of devices. DHT11 offers several benefits like great quality, rapid response time and higher performance. The figure is showing of DHT11 Sensor:

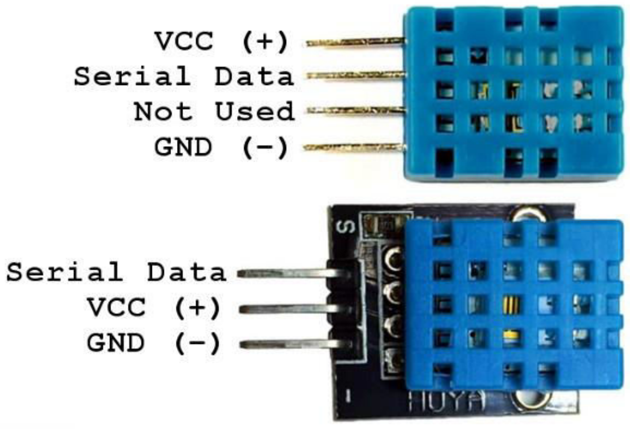

Figure 4.3 – DHT11 Sensor Pinout

After collecting all the hardware requirements, which includes a computer monitor or laptop, but we have shown the main connectivity of the experiment which is between raspberry pi, dht11 sensor and micro-USB cable. The Below figure shows the connectivity as we did in our work.

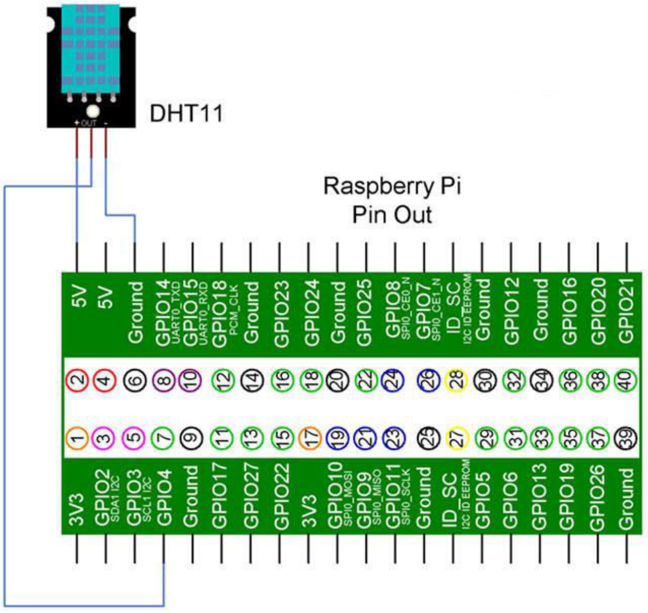

Figure 4.4 – Raspberry Pi and DHT11 sensor integrated

Another important prerequisite of this is Internet. It should be available during the whole process to process and execute the operations of IoT. The data of IoT gets stored using Things Speak API. Server holds the data in cloud and then visualize and perform streams. The data can be sent to Things Speak that visualize the real time data and can share the details of social platforms, such as Twilio and Twitter. MATLAB analytics and MATLAB code have been used by Things Speakfor preprocessing and analytics the data. After connecting all the modules to controller, we wrote the code to assimilate the temperature and humidity data and further send all the data to Thingspeak, the main code is written in python as shown below:

```
import sys
import urllib2
from time import sleep
import Adafruit_DHT as dht

from Crypto.Cipher import AES

key = 'abcdefghijklmnop'

# Enter Your API key here
myAPI = '3UQPIDWDLSTSN4DX'
# URL where we will send the data, Don't change it
baseURL = 'https://api.thingspeak.com/update?api_key=%s'
% myAPI
def DHT11_data():
    # Reading from DHT11 and storing the temperature and
humidity
    humi, temp = dht.read_retry(dht.DHT11, 23)
    return humi, temp
while True:
    try:
        humi, temp = DHT11_data()
        # If Reading is valid
        if isinstance(humi, float) and isinstance(temp,
float):
            # Formatting to two decimal places
            humi = '%.2f' % humi
            temp = '%.2f' % temp
            cipher = AES.new(key, AES.MODE_ECB)
            msg1 =cipher.encrypt('temp is tt='+temp)
            msg2 =cipher.encrypt('humi is tt='+humi)

            print(msg1.encode("hex"))

            print(msg2.encode("hex"))

            decipher = AES.new(key, AES.MODE_ECB)
            print(decipher.decrypt(msg1))
            print(decipher.decrypt(msg2))

            #print(humi)
            #print(temp)
            # Sending the data to thingspeak
            conn = urllib2.urlopen(baseURL +
'&field1=%s&field2=%s' % (temp, humi))
            print conn.read()
            # Closing the connection
            conn.close()
        else:
            print 'Error'
        # DHT22 requires 2 seconds to give a reading, so
make sure to add delay of above 2 seconds.
        sleep(15)
    except:
        break
```

The aforementioned code is used to fetch the data of temperature and humidity values from the DHT11 sensor and all the data is then sent using the encrypted techinique,for which the AES encryption methodhas been used to encrypt the data ebing transmitted over the internet. Whenever we send the data to the thingspeak, it tends to store the data and start analyzing the data while creating a real time graph as shown below belowin terms of humidity and temperature values. As shown below in figure 4.5, humidity graph has represented highest temperature as 32 degree Celsius and lowest as 23 degree celsius. The disparity can bee noted because of slight change in temperature after we turned the air conditioning system to verify the working of temperature sensor accurately.

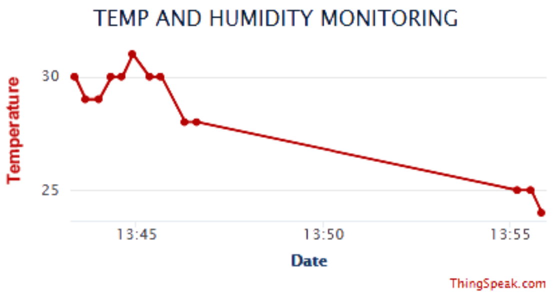

Figure 4.5 – Thingspeak temperature analytics graph from data collected from DHT11

Also, the Humidity values were calculated by DHT11 sensor and the thingspeak graph for humidity is shown down below in figure 4.6, where the highest value denoted is 74% and lowest is 59%.

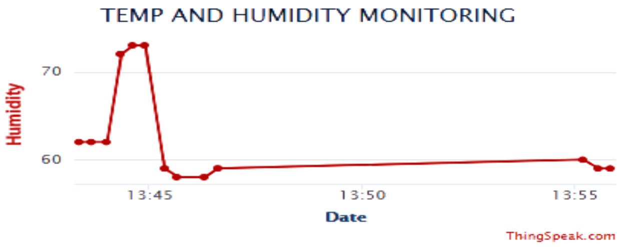

Figure 4.6 – Thingspeak humidity analytics graph from data collected from DHT11

The data of IoT is quite crucial which is send by default in plain text form, so it is highly vulnerable to MITM attacks i.e. Man-in-the-Middle attack. Therefore, attackers or hackers can breach the data and manipulate it over the internet without informing the receiver and sender. To solve this, encryption is essential which secures the IoT data. As shown in the code also, we have used the Advanced Encryption Standard with 128 bits in ECB mode. When data is being ready to transmitted from the raspberry pi towards the internet, data gets encrypted with AES symmetric encryption method under the ECB mode. Following output represents the data is being sent in encrypted form whenever python code file gets executed, it shows perpetual data delivery to the thingspeak server that is located on public internet.The value that is being sent is clearly in encrypted form as Temp is tt = 29.00 with ECB mode using AES-128 and secret key as abcdefghijklmnop is:

Encrypted Value– 22C2DBB7698D0BE69CC1B6131FB44E938E64CE873F174DBB2423FCD814580E15

Data is sent in encrypted form using AES encryption, we can verify it by decrypting it with AES decryption tool available online using any AES Decryption tool. Firstly we will see if it produces the same value that is shown in the output by entering the value related text, mode and key value in the requirement section and then when we press enter, it is clear that it is creating same value as created by our code.

Now if we do the decryption using the same tool this time for decryption, we will see that after entering encrypted value, mode, number of bits and key value, the encrypted value gets decrypted again to its real plain text form verifying that our code has worked properly.

Encrypted Value – 22C2DBB7698D0BE69CC1B6131FB44E938E64CE873F174DBB2423FCD814580E15
Key – abcdefghijklmnop
Plain Text – Temp is tt = 29.00

CONCLUSION

IoT is rising rapidly and almost all the businesses and industries are either using it or looking forward to integrate them with their work to increase security, business productivity, performance etc. Security is one of the biggest reason people are thinking on if they go with IoT solutions or not. Different IoT applications like Home Automation, Smart Cities, Smart Transport, Smart Industry, Smart Healthcare systems etc., use critical data which is needed to be make confidential while at transport from source to destination. By default, Plain-Text data is used between the communicating devices and large scale or processor intensive encryption algorithms cannot be used on lightweight micro controllers. Ligthweight Encryption Standards are not as secure as some of the encryption standards used at processor level like AES, 3DES etc. AES128 can be used on micro controllers like Intel Galileo, Raspberry Pi etc. against the Lightweight Encryption Standards. A Raspberry Pi with single GB Ram is connected with DHT11 sensor and it sends data to thingspeak server over the internet. We have encrypted the IoT data using AES-128 algorithm to bring confidentiality over the internet.

REFERENCES

[1] Kamble, A., & Bhutad, S., 2018. Survey on Internet of Things (IoT) security issues & solutions. International Conference on Inventive Systems and Control (ICISC).

[2] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu., 2018. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.IEEE Internet of Things Journal.

[3] Tuhin Borgohain, Uday Kumar, Sugata Sanyal., 2015. Survey of Security and Privacy Issues of Internet of Things. Int. J. Advanced Networking and Applications(IJANA).

[4] Mohamed Abomhara and Geir M. Koein., 2015. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security.

[5] J. Satish Kumar, Dhiren R. Patel., 2014. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications.

[6] Benedikt Abendroth, Aaron Kleiner, Paul Nicholas., 2017. Cybersecurity policy for the Internet of Things. Microsoft.

[7] Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed., 2017. Internet of Things Applications, Challenges

and Related Future Technologies. World Scientific News(WSN).

[8] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja., 2015. The Internet of Things (Iot): A Scalable Approach to Connecting Everything, The International Journal of Engineering and Science.

[9] Saranya C. M., Nitha K. P., 2015. Analysis of Security methods in Internet of Things. International Journal on Recent and Innovation Trends in Computing and Communication.

[10] Rizvi, S. S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018). Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018* (pp. 163-168). [8455902] Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

[11] S. Misra et al., 2016. Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering.

[12] Nandhini, R & Srilakshmi, P & Ramdoss, Aparna. (2018). Study on Security issues in Internet of Things.

[13] Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems.

[14] IoT Protocols.,2017. *https://opensourceforu.com/2017/07/internet-things-protocols-landscape/*.[Online]

[15] Joe Hanson.,2015. *https://www.pubnub.com/blog/10-challenges-securing-iot-communications-iot-security/*.[Online]

[16] D. Richards, A. Abdelgawad and K. Yelamarthi, "How Does Encryption Influence Timing in IoT?," *2018 IEEE Global Conference on Internet of Things (GCIoT)*, Alexandria, Egypt, 2018, pp. 1-5. doi: 10.1109/GCIoT.2018.8620133

[17] S. Maitra, D. Richards, A. Abdelgawad and K. Yelamarthi, "Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy," *2019 IEEE Sensors Applications Symposium (SAS)*, Sophia Antipolis, France, 2019, pp. 1-6. doi: 10.1109/SAS.2019.8706017

[18] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, Secure integration of IoT and Cloud Computing, Future Generation Computer Systems, Volume 78, Part 3, 2018, Pages 964-975, ISSN 0167739X, https://doi.org/10.1016/j.future.2016.11.03 (http://www.sciencedirect.com/science/article/pii/S0167739X1630694X)

[19] K. Yelamarthi, A. Abdelgawad, A. Khattab, "IoT-Based Health Monitoring System for Active and Assisted Living," *Smart Objects and Technologies for Social Good: Second International Conference,* pp.11-20, Dec 2016.

[20]. C. Coelho, D. Coelho, and M. Wolf, "An IoT smart home architecture for long-term care of people with special needs," *2015 IEEE 2nd World Forum on Internet of Things,* pp. 626-627, 2015.

[21]. M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495, Aug. 2018.

[22]. M. Botta, M. Simek, and N. Mitton, "Comparison of hardware and software-based encryption for secure communication in wireless sensor networks," *36th International Conference on Telecommunications and Signal Processing*, Rome, pp. 6-10. 2013.

[23]. Atreyi Kankanhalli, Yannis Charalabidis, Sehl Mellouli, IoT and AI for Smart Government: A Research Agenda, Government Information Quarterly, Volume 36, Issue 2, 2019, Pages 304-309, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2019.02.003.

[24]. S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne, and R. Tourki, "Performance evaluation and design considerations of lightweight block cipher for low-cost embedded devices," *IEEE/ACS 13th International Conference of Computer Systems and Applications*, pp. 1-7, 2016.

[25]. R. M. Needham and D. J. Wheeler. Tea extensions. Technical report, University of Cambridge, 1997.

[26]. J. Grossschadl, S. Tillich, C. Rechberger, M. Hofmann and M. Medwed, "Energy Evaluation of Software Implementations of Block Ciphers under Memory Constraints," *Design, Automation & Test in Europe Conference & Exhibition,* pp. 1-6, 2007.

[27]. F. Zhang, "On the Security and Energy Consumption Estimation of Wireless Sensor Network Protocols" (Doctoral dissertation), 2012.

[28]. Y. Xiao, H. Chen, B. Sun, R. Wang, S. Sethi, "MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks", *EURASIP Journal on*

Wireless Communications and Networking, Vol. 2006(2), Springer, April 2006, pp. 1-12.

[29]. O. Barahtian, M. Cuciuc, L. Petcana, C. Leordeanu, and V. Cristea,"Evaluation of Lightweight Block Ciphers for Embedded Systems,"*Innovative Security Solutions for Information Technology and Communications Lecture Notes in Computer Science*, pp. 49–58, 2015.

[30]. H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, "One round cipher algorithm for multimedia IoT devices," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18383–18413, 2018.

[31]. Alex Biryukov and Léo Perrin, ""State of the Art in Lightweight Symmetric Cryptography." [Online]. Available: https://eprint.iacr.org/2017/511.pdf.

[32]. D. Dinu, Y. L. Corre, D. Khovratovich, L. Perrin, J. G. schadl, A. Biryukov, "Triathlon of lightweight block ciphers for the internet of things", *Cryptology ePrint Archive Report 2015/209*, 2015, [online] Available: http://eprint.iacr.org/.

[33]. "PIC18F27K40," *PIC18F27K40 - Microcontrollers and Processors - Microcontrollers and Processors*. [Online]. Available: https://www.microchip.com/wwwproducts/en/PIC18F27K40. [Accessed: 20-Dec-2018].

[34]. "PIC18F24K42," *PIC18F24K42 - 8-bit Microcontrollers - Microcontrollers and Processors*. [Online]. Available:https://www.microchip.com/wwwproducts/en/PIC18F24K42.[Accessed: 20-Dec-2018].

[35]. Real-Time Current Monitor with USB," *ee-quipment.com*. [Online]. Available: https://www.ee-quipment.com/products/real-time-currentmonitor-with-usb. [Accessed: 20-Dec-2018].

[36] Z. Shu, J. Wan, D. Li, J. Lin, A. Vasilakos, M. Imran, "Security in software-defined networking: Threats and countermeasures," *Mobile Network Applications*, vol. 21, no. 5, pp. 764-776, 2016

[37]. Sombir; SOLANKI, Kamna. LITERATURE REVIEW ON SECURITY OF IOT. **International Journal of Advanced Research in Computer Science**, [S.l.], v. 9, n. 2, p. 131-134, apr. 2018. ISSN 0976-5697. Available at: <https://www.ijarcs.info/index.php/Ijarcs/article/view/5689>. Date accessed: 28 aug. 2019. doi:https://doi.org/10.26483/ijarcs.v9i2.5689.

[38]. I. Andrea, C. Chrysostomou, G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," Proc. IEEE Symp. Computer Commun. (ISCC), pp. 180-187, July 2015.

[39]. M. Levesque, D. Tipper, "A Survey of Clock Synchronization Over Packet-Switched Networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2926 – 2947, 2016.

[40]. B. J. Mohd, T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," *IEEE Access*, vol. 6, pp. 35966-35978, 2018.

[41]. C. Paar, J. Pelzi, "Understanding Cryptography: A Textbook for Students and Practitioners," *Springer,* 1st edition, July 2010.

[42]. O. Barahtian, et. al, "Evaluation of Lightweight Block Ciphers for Embedded Systems," *SECITC*, Springer, vol. 9522, 2015.

[43] Srinivasan, C. R., Rajesh, B., Saikalyan, P., Premsagar, K., & Yadav, E. S. (2019). A review on the different types of internet of things (IoT). *Journal of Advanced Research in Dynamical and Control Systems*, *11*(1), 154-158.

[44] Talal, M., Zaidan, A.A., Zaidan, B.B. et al. J Med Syst (2019) 43: 42. https://doi.org/10.1007/s10916-019-1158-z

[45] Ahmad M., Ishtiaq A., Habib M.A., Ahmed S.H. (2019) A Review of Internet of Things (IoT) Connectivity Techniques. In: Jan M., Khan F., Alam M. (eds) Recent Trends and Advances in Wireless and IoT-enabled Networks. EAI/Springer Innovations in Communication and Computing. Springer, Cham

[46] Sufian Hameed, Faraz Idris Khan, and Bilal Hameed, "Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review," Journal of Computer Networks and Communications, vol. 2019, Article ID 9629381, 14 pages, 2019. https://doi.org/10.1155/2019/9629381.

[47] Luigi Atzori , Antonio Iera , Giacomo Morabito, The Internet of Things: A survey, Computer Networks: The International Journal of Computer and Telecommunications Networking, v.54 n.15, p.2787-2805, October, 2010 [doi>10.1016/j.comnet.2010.05.010]

[48] Kumar A., Salau A.O., Gupta S., Paliwal K. (2019) Recent Trends in IoT and Its Requisition with IoT Built Engineering: A Review. In: Rawat B., Trivedi A., Manhas S., Karwal V. (eds) Advances in Signal Processing and Communication. Lecture Notes in Electrical Engineering, vol 526. Springer, Singapore

[49] Birkel, H. and Hartmann, E. (2019), "Impact of IoT challenges and risks for SCM", *Supply Chain Management*, Vol. 24 No. 1, pp. 39-61. https://doi.org/10.1108/SCM-03-2018-0142

[50] Vishal Kumar Verma. Blockchain Technology: Systematic Review of Security and Privacy Problems and Its Scope with Internet of Things (IoT). *Journal of Network Security*. 2019; 7(1): 24–28p.

[51] Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2019). A Review of Factors Influencing Customer Acceptance of Internet of Things Services. *International Journal of Information Systems in the Service Sector (IJISSS), 11*(1), 54-67. doi:10.4018/IJISSS.2019010104

[52] H. Shin, H. K. Lee, H. Cha, S. W. Heo and H. Kim, "IoT Security Issues and Light Weight Block Cipher," *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Okinawa, Japan, 2019, pp. 381-384. doi: 10.1109/ICAIIC.2019.8669029