Volume: 10, Issue: 1
Page: 91-96
2022

International Journal of Science and Business

Journal homepage: ijsab.com/ijsb

Implementation of a smart home prototype with security considerations

Walat Ali & Saleh Yousefi

Abstract

This study presents a project to implement an advanced and primary smart-home program that works with IoT. Generally speaking, this kind of projects has attracted the attention of many modern scholars lately. Advanced researches and projects are conducted worldwide to expand the advancement of the current technology, reduce the electricity usage, facilitating daily tasks, and providing control over everyday devices and gadgets. Advanced programs provide security and protection. These programs can be implemented to any modern electronic device that can be used in a smart-home through the help of Advanced Encryption Standard (AES) and special algorithms. The outcomes of this study reveal that using this project minimizes commuting and organizes daily tasks. Therefore, people need to use this program to save time. Economically, this program is affordable. The study concludes the main points of the research and projects.

IJSB
Accepted 13 March 2022
Published 15 March 2022
DOI: 10.5281/zenodo.6355100

Keywords: *Smart home, AES, Arduino, PHP, MySQL.*

About Author (s)

Walat ali, Information Technology, Duhok Polytechnic University (DPU), Duhok, Iraq.
Professor Saleh Yousefi, Engineering Technology, University of International Urmia (UIU), Urmia, Iran.

1.Introduction

The IoT future is going to revolutionize the Internet, to create networks of many of wireless identifiable objects and devices, communicating with each other at anytime, anywhere, with anything and anyone using any kind of services. It is predicted that in the near future, everything from people, groups, objects, products, data and services will be connected and affected by the IoT pattern(Chatzigiannakis et al., 2016). Increasingly rapid development of applications and innovative services that may change the way people live, work and communicate is expected(Price et al., 2005).

Transferred data may contain sensitive information about privacy, habits, activities and relationships of users. The security of these communication systems considered as one of the important issues in communication networks (Azahari Mohd Yusof et al., 2018). Therefore, it is very important that IoT systems ensure the confidentiality and integrity of information and the privacy and anonymity of users. The transfer of readable data is compromised by changes in the workflow. Implementing cryptography in data security is needed to increase confidentiality. All data are sent to a specific place where they can be encrypted in text mode(Ieee & Ieee, n.d.)(Shah & Bhat, 2020). Home automation systems help to save energy and manage internal energy demand, as well as control and monitor home electronic devices and increase home security, and it is known as one of the applications of IoT.

2. Literature Review

The experiment of securing data communications on IoT devices is highly limited and the available resources to support security technologies are limited as well. The amount of resources available in a device also depends on the purpose of the device, performance and resources remaining after the implementation of this feature. To be categorized as a device Class 0 The source must be below the source threshold described by Borman et al. With ROM less than 100 KB or RAM less than 10 KB. An example of a Class 0 device is the Arduino Uno an 8-bit microcontroller with a 16 MHz processor, both of them are Ram.

RAM is the processing memory of a program running on a device while ROM is the size of the program code. In the case of the Uno, the device has enough RAM to do significant work but lacks the ROM (code space) required for security mechanisms. The purpose of this literature review is to determine whether there is a gap in research into securing data communications from very limited devices and the Internet. The purpose of this literature review is to find the newest and most relevant solutions to solve data security problems from very limited devices to the Internet. There will be different solutions The problem is solved based on the need of resources and the ability to solve all or part of it(King, n.d.). Explore and address the threats which can leads to exploit the IoT. And also introduce two emerging security challenges that can be exploited by the attacker are Exponential increase in the number of weak links and Unexpected uses of data(Mosenia & Jha, 2017). Security protocols such as TLS or DTLS are effective on the Internet, but this does not mean that the same level of security can be achieved with low Internet connection network and loss. E2E IoT security Not insignificant, because of the many imaginable usage situations such as: CoAP / CoAP, DTLS / DTLS and HTTP / CoAP, TLS / DTLS are interceded by 6LBR which are varied requirements and Limitations They also acknowledge that having E2E is safe The connection between the two ends is maintained by only one protected correspondence channel, the LLN Even now it can be vulnerable to asset use, flooding, redistribution and reinforcement Attacks, since 6LBR normally does not do any verification(Mosenia & Jha, 2017).

They summarize the uses and the low ground Secure communications that record the convention stack design. Also, suggest a 8 Lightweight technique for building a secure end-to-end channel, which is negligible The inclusion of limited IoT tools, while keeping all convention operations unchanged Inside the UCN, this is achieved by changing some of the devices Integrated with the channel base to a valid gateway(Bui et al., 2012). Wireless body sensor network depends on three different levels of security Location of sensors on the wearable system. Patients use a wearable device that measures Body activities and conversion of body signals to values for understanding by a Man. Such information is reflected in the classification matrix. Information that is Classified as restricted, it can apply a moderate level of security such as reciprocity Authentication and exact location of patients.

Authentication section can be obtained Using PIN code with biometric password. Successful authentication, Role-based access control (RBAC) can be considered in which permissions are combined with roles and Users create specific members for patient data records(Alkeem et al., n.d.). In this article, Lamina, the diverse framework that has been launched, is shown Protection and security for the cooperation of client tools in the IoT space in broad daylight. It Includes an off-band, cloud-based registration framework where the main material is available Trades between client tools and your favorite IoT outdoor. Press the key once Materials are traded, Crypto CoP-based encryption and MAC address cycling are used Customer tools to secure outsiders cannot receive private data about the customer To the Internet of Things Lamina In addition, the public space of the Internet of Things can gather Adequate knowledge of the data in relation to customers who have traveled in this space to provide targeted data And offices while still providing customer identity (Harris III et al., n.d.).

There are a lot of security measures. Therefore, the proposed SGA can provide a common approval component and maintain a strategic one Distance from key speculation attack, online intangible key speculation Attack, information security and manual attack. SGA is suggested in this article Meets the security requirements of the car-to-car service layer center. To Ensures any nimble tools can talk to each other safely, security passage This software includes light symmetric key cryptography claims Functional, secure, secure end-to-end and machine-to-machine key exchange(Chen et al., 2016). The proposed architectural design tries to complete the existing experiment Enables steps and developers to have a better blueprint than what they do Calculate in several types of steps, with the aim that they can make changes to it In accordance with the highest level of security that the algorithm can achieve Guarantee. In addition, an attempt has been made to allow the testing of a synchronized algorithm Simple in hardware, while the possibility of parallel testing on Stay basic architecture(Arseni et al., 2016).

3. Experimental design and output of the DHT22 sensor

That gives data about the temperature. This sensor works with an advanced tool called Arduino esp32 which works on 5 volts. The sensor gets connected to port (4) of Arduino esp32. This method is applied through a specified algorithm that is called AES. The algorithm that has been used is called AES-ECB-128. Therefore, the esp32 tool with the aid of DHT22 reads the data and it will be secured with a 32 letters key. Then, the data will be saved to be later sent to the server. The server is consisted of sending and receiving data, and on the outside, it is connected with the sensor.

The server which is also called host + domain contains a lot of folders and files. These files and folders take different extensions such as PHP, CSS, HTML, +script, ...etc. After receiving, encrypting, and securing the data with a special key, the data will be saved in the server. After this process, and for further security, the data will be changed according to some algorithms.

Later, the data will be encrypted by AES encrypt operation in Cipher Block Chaining (CBC) Mode using a secret key. The data are received from esp32 tool which will be saved in the server. After that, the smart phone system such as Android and with the aid of API in the server will read the data. The data will be transformed successfully from the sensor to the mobile application or to any device with browsing feature.

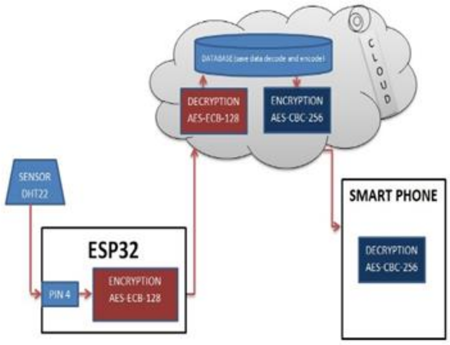

Figure 1. Using AES encryption/decryption for securing communications between user/server and server/sensor in the smat home ecosystem

4. Security of turning on and off the lights

This process gives the ability to change and give orders to your smart house such as turning on and off the lights, turning the TV on, or applying orders to any other device in your house. The entrance door can also be controlled by using Switch Relay. Similarly, the garage door or any other house machine can be controlled by using the smart card. There are a number of buttons to press to give these orders, the shape of these buttons is designed by using some programs and some different codes such as HTML; it is well-described and explained the codes that are used in chapter four. Whenever an order is given to turn on a light, the port becomes 1 and when it is turned off, the port becomes 0.

Thus, any device that can be turned on and off by giving these orders, 0,1 are given to the port. When the device is on 1, it means that it is on in the server and it will be saved by using an algorithm (AES-CBC-256). It will also be given a special key to save in the server after encrypting it. Later, the server will send the data to ESP32 tool through specific protocols. "After receiving the encrypted data, the ESP32 uses its secret key and AES decryption operation in Electronic Code Book (ECB) mode to decrypt the data. Then it sends an appropriate command to the related port." Therefore, when the port becomes 1, everything that is related to the port will be turned on. While when giving orders to turn them off, the port will become 0 in the server and saved in the server with algorithm AES-CBC–256 with a special key. It will again be sent to ESP32. ESP32 tool will receive it and decrypt it by using some special codes and algorithm (AES-ECB-128). In the final step, the ESP32 tool will give orders to the port to become 0 which means the light will be turned off.

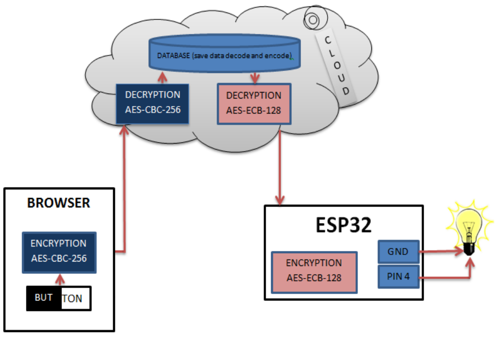

Figure 2. Using AES encryption/decryption for securing communications between user/server and server/light in the smart home ecosystem
and server/sensor in the smart home ecosystem".

5. Conclusion

In this research, we have implemented a custom algorithm for the smart home system studied, that uses Arduino ESP32 and php server as communication protocol. We have presented the main objectives of this research work first by identifying the vulnerability of our system, studying the more cryptographic algorithms in references that could suit the system and choose one of them. Finally, we have made a choice and implement the system where it causes to send all the commands encrypted for no intruder to understand or use against the owner of the system. Given that there are new systems and protocols every day and new ways to break all of the existing ones, we need to keep track them by eye on these changes so we can apply them to our present secured system. At the end We can conclude that we have present a methodology to increase the security to a IoT based smart home system while preserving an acceptable performance and keeping the whole costs low for the manufacturer of the smart home systems.

References

Alkeem, E. AL, Yeob Yeun, C., & Jamal Zemerly, M. (n.d.). *Security and Privacy Framework for Ubiquitous Healthcare IoT Devices*.

Arseni, Ş.-C., Miţoi, M., & Vulpe, A. (2016). Pass-IoT: A platform for studying security, privacy and trust in IoT. *2016 International Conference on Communications (COMM)*, 261–266.

Azahari Mohd Yusof, M., Hani Mohd Ali, F., & Yusof Darus, M. (2018). Detection and Defense Algorithms of Different Types of DDoS Attacks. *International Journal of Engineering and Technology*, *9*(5), 410–444. https://doi.org/10.7763/IJET.2017.V9.1008

Bui, N., Olivereau, A., Rossi, M., Bonetto, R., Lakkundi, V., & Serbanati, A. (2012). *Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples*. https://www.researchgate.net/publication/260540457

Chatzigiannakis, I., Vitaletti, A., & Pyrgelis, A. (2016). A privacy-preserving smart parking system using an IoT elliptic curve based security platform. *Computer Communications*, *89–90*, 165–177. https://doi.org/10.1016/j.comcom.2016.03.014

Chen, H. C., You, I., Weng, C. E., Cheng, C. H., & Huang, Y. F. (2016). A security gateway application for End-to-End M2M communications. *Computer Standards and Interfaces*, *44*, 85–93. https://doi.org/10.1016/j.csi.2015.09.001

Harris III, A. F., Sundaram, H., & Kravets, R. (n.d.). *Security and Privacy in Public IoT Spaces*.

Ieee, & Ieee. (n.d.). *2012 Second International Conference on Digital Information and Communication Technology and it's Applications*.

King, J. (n.d.). *MASTER'S THESIS A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet*.

Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE*

Transactions on Emerging Topics in Computing, *5*(4), 586–602. https://doi.org/10.1109/TETC.2016.2606384

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human Computer Studies*, *63*(1–2), 228–253. https://doi.org/10.1016/j.ijhcs.2005.04.008

Shah, J. L., & Bhat, H. F. (2020). Towards a Secure IPv6 Autoconfiguration. *Information Security Journal*, *29*(1), 14–29. https://doi.org/10.1080/19393555.2020.1716117

Cite this article:

Walat Ali & Saleh Yousefi (2022). Implementation of a smart home prototype with security considerations. *International Journal of Science and Business, 10*(1), 91-96. doi: https://doi.org/10.5281/zenodo.6355100

Retrieved from http://ijsab.com/wp-content/uploads/908.pdf

Published by

IJSAB International