
Ministry of Higher Education

and Scientific Research

University of Diyala

Department of Computer

# Secure Data Retrieval from a Remote Server

By
Nibras Raad Abdallah
Supervised
By
Asst. Prof. Dr. Taha Mohammed Hassan
Co-supervised
By
Asst. Prof. Dr. Ahmed Chalak Shakir

A thesis submitted to the University of Diyala
College of Science in a partial fulfillment of the
requirements of the degree of Master in the
Computer Science.

April 7, 2019

# Certificate of The Supervisors

We certify that read this thesis entitled **"Secure Data Retrieval from a Remote Server"** that was made under our guidance and supervision for the award of Degree of Master of Department of Computer Science of Diyala University. In addition, as an examing committee, examined the contents and in what is related for the student **" Nibras Raad Abdallah"**, and that in our opinion it meets the standard of a **thesis** for the degree of master of sciences in Computer Science.

*Signature :

Supervised By

Asst.Prof.Dr.Taha Mohammed Hassan

April 7, 2019

*Signature :

Co-supervised By

Asst.Prof.Dr.Ahmed Chalak Shakir

April 7, 2019

# Certificate of The Linguistic

This is to certify that this **thesis** entitled **"Secure Data Retrieval from a Remote Server"** by **"Nibras Raad Abdallah"** was prepared under supervisors from a linguistic point of view. Its language is amended to meet the style of the standard English language.

*Signature :

Name :

April 7, 2019

# Examination Committee Certification

We certify that thesis entitled **"Secure Data Retrieval from a Remote Server "** and as an examining committee, examined the student **"Nibras Raad Abdallah"** in its contents, and that in our opinion it meets the standard of a **thesis** for the degree of master of sciences in Computer Science.

(Chairman)
Signature :
Name : Prof.Dr.Qasim M.Hussein
April 7, 2019

(Member)
Signature :
Name : Asst.Prof. Naji M.Sahib
April 7, 2019

(Member)
Signature :
Name : L. Jumana W.Salih
April 7, 2019

(Member/Supervisor)
Signature :
Name : Asst.Prof.Dr.Taha M. Hassan
April 7, 2019

(Member/Supervisor)
Signature :
Name : Asst.Prof.Dr.Ahmed Ch. Shakir
April 7, 2019

Approved by University of a Diyala Faculty of Science Department of Computer Science.

(The Dean)
Signature :
Name : Prof.Dr.Tahseen Hussein Mubarak
April 7, 2019

# Declarations

I acknowledge that I have also been advised by academic staff about standards for good academic conduct and how to avoid plagiarism and other assessment irregularities.
I acknowledge that plagiarism is the unacknowledged use of another person's ideas, words or work either verbatim or in substance without specific and appropriate acknowledgment.
I acknowledge that the inclusion of a footnote or a source in a bibliography is insufficient for attribution of another's work.
I hereby certify that the research work in this thesis is my original work and it does not include any copied parts without the appropriate citation.
I acknowledge that any work that I submit for assessment at Department of Computer Science , College of Science , University of Diyala , Iraq:

- Must be all my own work.
- Must not have been prepared with the assistance of any other person, except those permitted within University guidelines or the specific assessment guidelines for the piece of work.
- Has not previously been submitted for assessment at this University or elsewhere.

I acknowledge that I must take reasonable steps to ensure that my assessments – and related preparatory work for submissions – are kept secure so that I do not enable another person to copy my work.
I accept that the College may check the originality of my work using a range of techniques, including computer based plagiarism detection software.
I accept that any suspected irregularity in my work will be dealt with under the University's Assessment Irregularities Procedure.

Kirkuk, Iraq
Nibras Raad
April 7, 2019

# Acknowledgements

*Thanks God for his generosity in the primarily and the lastly*

At the end of this thesis, I would like to take some time to thank all the people without whom this project would never have been possible. Although it is just my name on the cover, many people have contributed to the research in their own particular way and for that, I want to give them special thanks.

First, my supervisors,Assist.Prof.Dr.Taha Mohammed Hassan, you have created an invaluable space for me to do this research and develop myself as a researcher in the best possible way. I greatly appreciate the freedom you have given me to find my own path and the guidance and support you offered when needed. He is someone you will instantly love and never forget once you meet him. He's the funniest advisor and one of the smartest people I know. I hope that I could be as lively, enthusiastic, and energetic as him.

Assist.Prof.Dr.Ahmed Chalak Shakir, you have always been there for me, kept me in check and over the days have become a friend as well. I truly hope that we will be given the opportunity to work even closer together in the future. He has been supportive and has given me the freedom to pursue various projects without objection and he has also provided insightful discussions about the research. He is my primary resource for getting my science questions answered and was instrumental in helping me crank out this thesis. You was and remains my best role model for a scientist, mentor, and teacher. I will forever be thankful for you.

Next, I would like to thank the administration of The College of Sciences for the University of Diyala for their efforts to provide a distinctive model research university.

I also want to take a moment to thank my other committee members, to Prof.Dr. Qasim M.Hussein,Asst.Prof. Naji M.Sahib, and L. Jumana W.Salih. Thank you for investing time and providing interesting and valuable feedback. I feel proud and honored that you have accepted to be on my committee.

Last but not least, some people of outstanding importance for my research, I would like to show my sincere appreciation and gratitude to my wife. Thanks, to my beloved family, dad, mum and sibling for their self-sacrifice, consistent love, support, understanding and encouragement.

Nibras Raad AL_Bayaty

# Abstract

Internet of Things (IoT) applications nowadays have a wide impact on people's daily life while the size of IoT has been increasing rapidly. Millions of devices, a huge amount of data ,and different kinds of new protocols can bring many security issues. In addition, the malicious activities have increased with more sophisticated attacks, that will result in higher risks. Therefore, the security aspect is becoming increasingly important year-after-year.

LoRaWAN is a MAC layer protocol for long-range low-power communication dedicated to the IoT. It can be used to transmit messages between IoT end devices and gateways. However, since the development of LoRaWAN is still at an early stage, the security level of the protocol is not well developed, and the need for analyzing and developing the security level of LoRaWAN is necessary and urgent.

In order to be benefited from this modern protocol, it will be applied in a practical manner in the Ministry of Interior/Civil Status Directorate, Passports and Residence in Kirkuk Governorate/National Card(ID). This section is connected with the sub-districts in the same geographical area for exchanging data as an alternative to the Internet service due to the problems and its interruptions .

This thesis summarizes the secure features of LoRaWAN in the aspects of activation methods, key management, cryptography. Then, vulnerabilities of LoRaWAN are found, can be exploited by an attack. Attacks based on these vulnerabilities are designed and described. These attacks are replay attack, eavesdropping, bit flipping, and ACK spoofing.

As a proof-of-concept, the bit flipping attack is implemented and executed in a LoRaWAN environment. Afterward, mitigation and secure solution against this attack are given to protect the security of LoRaWAN networks by adding an encryption layer and digital signature by an adaptive method of elliptic curve cryptography to transfer data.

The result of the proposed system can be used in developing the security level of LoRaWAN protocol.

# Contents

# List of Abbreviations

| | |
|---|---|
| *ABP* | Activation By Personalization. |
| *ADR* | Adaptive Data Rate. |
| *AES* | Advanced Encryption Standard. |
| *ALOHA* | Advocates of Linux Open-source Hawaii Association. |
| *ANSI* | American National Standards Institute. |
| *AppEUI* | Application Unique Identifier. |
| *AppSKey* | Application Session Key. |
| *BLE* | Bluetooth Low Energy. |
| *CSS* | Chirp Spread Spectrum. |
| *DevAddr* | Device Address. |
| *DevEUI* | Device Unique Identifier. |
| *DH* | Diffie-Hellman. |
| *ECC* | Elliptic Curve Cryptography. |
| *ECCDH* | Elliptic Curve Cryptography Diffie-Hellman. |
| *ECDLP* | Discrete Logarithm Problem. |
| *FIPS* | Federal Information Processing Standards. |
| *FSK* | Frequency-Shift Keying. |
| *GPIO* | General-purpose input/output. |
| *GUI* | Graphic User Interface. |
| *Gbit/s* | Gigabit per second. |

| | |
|---|---|
| $HAL$ | Hardware Abstraction Layer. |
| $IANA$ | Internet Assigned Numbers Authority. |
| $ICV$ | Integrity Check Value. |
| $ID$ | National Unified Card Section. |
| $IEEE$ | Institute of Electrical and Electronics Engineers. |
| $IETF$ | Internet Engineering Task Force. |
| $IHS$ | Information Handling Services. |
| $Iot$ | Internet of Things . |
| $IP$ | Internet Protocol. |
| $ISM$ | Industrial, Scientific and Medical band. |
| $ISM$ | Industrial, Scientific and Medical. |
| $IT$ | Information Technology. |
| $LNA$ | Low Noise Amplifier. |
| $LoRa$ | Long Range . |
| $LoRaWAN$ | Long Range Wide Area Network . |
| $LPWAN$ | Low Power Wide Area Network. |
| $M2M$ | Machine to Machine. |
| $MAC$ | Medium Access Control. |
| $MHDR$ | MAC Header. |
| $MIC$ | Message Integrity Code. |
| $MQTT$ | Message Queuing Telemetry Transport. |

| | |
|---|---|
| $NIST$ | National Institute of Standards and Technology. |
| $NwkSKey$ | Network Session Key. |
| $NFC$ | Near field communication. |
| $OMA$ | Open Mobile Alliance. |
| $OTAA$ | Over The Air Activation. |
| $OFDM$ | Orthogonal Frequency Division Multiplexing. |
| $PKC$ | Public Key cryptography. |
| $RF$ | Radio Frequency. |
| $RSA$ | Strive, Shamir, Adleman. |
| $RSSI$ | Received Signal Strength Indicator. |
| $SPI$ | Serial Peripheral Interface. |
| $SKC$ | Secret Key Cryptography. |
| $TM$ | Trademark. |
| $UART$ | Universal Asynchronous Receiver/Transmitter. |
| $UL$ | Uplink. |
| $WPAN$ | Wireless Personal Area Network. |
| $WSNs$ | Wireless Sensor Networks. |

. . . . . .

# List of Figures

# List of Tables

# 1 Introduction

## 1.1 Introduction

Recently, the Internet has spread to every part of the world and has a direct impact on human life. As we entered the era of the most widespread digital communication, many of the devices will be connected to the Internet, that is, we have entered an era Internet of Things(IoT)[1].

Let us highlight the most popular definitions in the world of IoT first of Vermesan et al. in [2] which they defined IoT as an interaction between the digital world and the physical world where the two worlds interact via the use of many actuators in machines and embedded sensors.

In [3] Pena-Lopez et al. define IoT as a model, network capabilities and computing can be embedded in it of an object, these capabilities are used to inquire about the state of the object and change state if possible. We can use them collaboratively to achieve complex tasks that require a high degree of intelligence[1].

The fact, radio waves are easily available and inexpensive. Perhaps the most prominent requirements of IoT area are low bandwidth communications over a long range with low power and cost.

Popped up Several wireless communication standards such as Wi-Fi and Bluetooth, which are characterized by their speed in transmitting data over short distances, therefore it is not to be suitable for long range. Therefore many companies and researchers went to the development of modern technologies to transmit data over long distances at a lower cost with low energy. That was the reason for the emergence of Low Power Wide Area Networks (LPWANs)[4].

LPWAN technologies (NB-IoT, LoRa, SigFox,... etc) successfully offer wide area connectivity from a few kilometers to tens of kilometers with low power, low data rate, and low throughput applications. Their market is expected to be huge, where is about a quarter of overall thirty billion IoT/M2M devices are assumed to be connected through the Internet using LPWAN[5].

Formation of LPWAN networks by using several technologies such as (IEEE 802.11ah, IEEE 802.15.4g, and LoRaWAN), where are into one wide area network[6].

The proposed system of this thesis will discuss the possibility working a private network with distances of up to more than one kilometer in an urban environment scenario and data interchangeability for one important of the prominent LPWAN technologies, LoRaWAN™[7] without the need service of Internet and provide sufficient information to deal with this technology and the LoRaWAN networks, which allows the user to build his network easily without the need to take approvals and licenses by companies or institutions, and an important benefit of the proposed system is to serve the public interest into the provision of money and the cost of equipment.

LoRaWAN has able to the deployment of private and public networks. The work of this net similar to cellular ones.

LoRAWAN (Long Range Network Protocol) [5], mainly developed in January 2015 by the LoRa Alliance to facilitate IoT applications[8][9][10]. That guarantees the full compatibility between the objects of IoT, without need to the complex local applications[11].

## 1.2 Motivation

The motivation behind the proposed system is that many international companies have shared in this new technology, especially Semtech and its LoRa products, and it is expected that in the next few years a market will be flooded with the products associated with this technology. And the problems with the Internet service and the continuous interruption of service. Therefore, this study will be using the LoRaWAN technology was chosen as an ideal alternative to the INTERNET to transfer data, but recently, many studies have reported a security vulnerability that can develop into

an attack in the LoRaWAN technique called "bit-flipping attack"[12]. This attack changes specific fields in a cryptographical text without decryption [13].

## 1.3 The Aim of The Thesis

- Establish a large-scale low-cost network in urban areas to exchange data in high confidentiality without the need to use the Internet.
- Connect to a remote database for the purpose of dealing with the stored data.
- Adding an extra layer of security to increase the integrity(reliability) of data sent within this network using an adaptive method of the elliptic curve cryptography without affecting the efficiency of the network and the speed of data transfer.
- Using a modern technology, which has become a top technology of digital communication for the Internet of things, and how to adapted it with the proposed system to exchange data.
- The proposed system prevent dealing with the data that has been manipulated by the bit-flipping attack.

## 1.4 Literature Review

A little research and literature have been published on LoRa platform and the LoRaWAN stack. This section will be focused on the study of literature and backgrounds to understand the LoRa platform and its applications.

- In [14] Magrin et al. give a detailed overview of the LoRa platform and the IEEE 802.15.4 standard, it is the LoRa base which is used in the IoT environment, by using the star topology in the unlicensed Sub GHz spectrum.
- In [15] Gheorghiu et al. give an initial assessment of LoRa's standard and give an overview of the understanding of the protocol itself. In addition, it provides the differences between LoRa and other radio standards.

- In [16] Lee et al. give a way to protect the message from the risk of bit-flipping attack. By shuffling the location of all octets in the frame payload.

- Ramachandran et al. in [17] by using the LoRa protocol and one among its maximum important capabilities, the potential to limit deployment complexity via wherein gadgets and nodes automatically hook up with the network and transmit obtained data, that is reduced the electricity consumption. Also, it explains the importance of chirp spread spectrum (CSS)[18][19] and its impact on the scalability of the LoRa network, providing multiple data rates over frequency ranges. A Table comparing the data rate, spreading factor [20] and the radio bit rate can be seen in (Table 2.1). That paper also highlights testing techniques for range which are incorporated in this thesis.

- As an application, there are little papers that relied on this technology. In [21]and [5] the covering of LoRa technology was evaluated for outdoor cases.

- Authors in[22] made the attempt to apply LoRa technology for health and wellness monitoring.