CSE 4000: Thesis/Project

A New Lightweight Chaos Based Cryptosystem For IoT Devices

By

Partho Choudhury Shoumya

Roll: 1807021

Department of Computer Science and Engineering

Khulna University of Engineering & Technology

Khulna 9203, Bangladesh

August,2023

A New Lightweight Chaos Based Cryptosystem for IoT devices

By

Partho Choudhury Shoumya

Roll: 1807021

A report submitted in partial fulfillment of the requirements for the degree of "Bachelor of Science in Computer Science & Engineering"

Supervisor:

Prof. Dr. Kazi Md. Rokibul Alam
Professor
Department of Computer Science & Engineering
Khulna University of Engineering & Technology (KUET)

Signature

Department of Computer Science and Engineering

Khulna University of Engineering & Technology

Khulna 9203, Bangladesh

August,2023

Acknowledgement

I would like to express my sincere gratitude to almighty who blessed me dearly to complete this report. I am indebted to the researchers and authors of scientific papers of this field for their meticulous work regarding innovative utilization of chaos theory in cryptography. Spending time on gaining knowledge of this filed of research has not only expanded my understanding of the intricate interplay between chaos theory and cryptography but has also served as a catalyst for deeper exploration within the realm of cybersecurity. Furthermore, I extend my appreciation to my thesis supervisor who have provided invaluable guidance throughout the process of preparing this report. His expertise and encouragement have been essential in developing a comprehensive understanding of the topic and refining the insights presented herein.

Author

Abstract

There are various uses for the Internet of Things (IoT), including intelligent industries, healthcare systems, and smart urban transportation. To avoid unauthorized access and potential harm to vital information in these situations, protecting transferred data is essential. At the moment, well-known IoT solutions rely on traditional encryption techniques like DES, RSA, and AES. But some of these algorithms are losing their dependability, and others require a lot of energy, memory, and processing power. This is a challenge for IoT devices with constrained resources. This work looks for a new, lightweight, and effective cryptosystem for protecting IoT communications to address these issues. This solution has components of diffusion, confusion, and a chaos-driven random generator. In contrast to current approaches, this research offers an improved lightweight cryptosystem with improved confusion-diffusion techniques that may be applied to hardware platforms with limited resources. Notably, the suggested method maintains flexibility in terms of the types of data used in IoT networks, supporting a range of formats including sensor data, text, voice, and image. These characteristics support the cryptosystem's possible use in a variety of real-world situations.

Contents

List of Figures

Chapter I

Introduction

1.1 Background

In the last decade, a large portion of the world's population has been living in cities. This portion is expected to increase to 70% by 2050 [1]. With the growth of cities, many problems appear such as pollution, traffic congestion and waste management. Thus, monitoring and controlling these systems becomes increasingly difficult as their size, complexity and interactions continue to grow. In addition, they are susceptible to frequent failures such as equipment failure, human error, and software error. In response to the urgency of addressing these issues, many initiatives are launched worldwide from city councils to companies and research laboratories. Actors of various disciplines propose to connect these systems to the Internet to manage them in an efficient way, which led to the concept of the Internet of Things.

1.2 Problem Statement

In IoT systems, it is becoming more and more obvious that transmitted data in such networks (Internet) are quite sensitive and have been susceptible to several attacks [2]. Recently, they have revealed a number of vulnerabilities, especially in smart transportation systems, smart grids, smart health systems etc.

Smart transportation system has been found to be vulnerable. It allows remote control of the vehicle, as well as impersonation and sending false information to neighboring vehicles. Smart grid integrates different micro-grids via two-way communications between energy providers and consumers, depending heavily on reliable measuring data. Nevertheless, these systems have shown vulnerabilities to disruption of state estimation by data integrity attacks, erroneous data injection attacks, data deletion attacks, and data erasure attacks. Smart health systems incorporate a number of sensors assessing the health status of patients and must conform to strict data privacy monitoring and regulatory requirements. However, a number of health systems have been subverted, including viruses such as WannaCry, Medjack, and SamSam that have impacted hospitals.

1.3 Objectives

As discussed the emerging threats in the previous section, the security of systems and their vulnerability to various attacks affect all sectors and aspects. Such risks require fast and efficient security algorithms. Indeed, existing IoT solutions come with security mechanisms at the transport and application layers. These mechanisms deploy conventional symmetric and asymmetric cryptography techniques such as AES, RSA, DES, and RC4. These algorithms are based on a permutation diffusion network. However, some of them have been broken and are no longer trusted. Others (such as AES) require considerable resources for IoT nodes that may have limited resources in terms of energy, memory, and computational power. So it was aimed in this work to overcome these difficulties and design a suitable cryptosystem for targeted devices.

1.4 Project planning

To develop such a cryptosystem in limited time frame, the overall work was divided into smaller parts and these smaller targets were tried to get done within deadlines. Previous and future work plans are shown using a gantt chart in Fit 1.1 below:

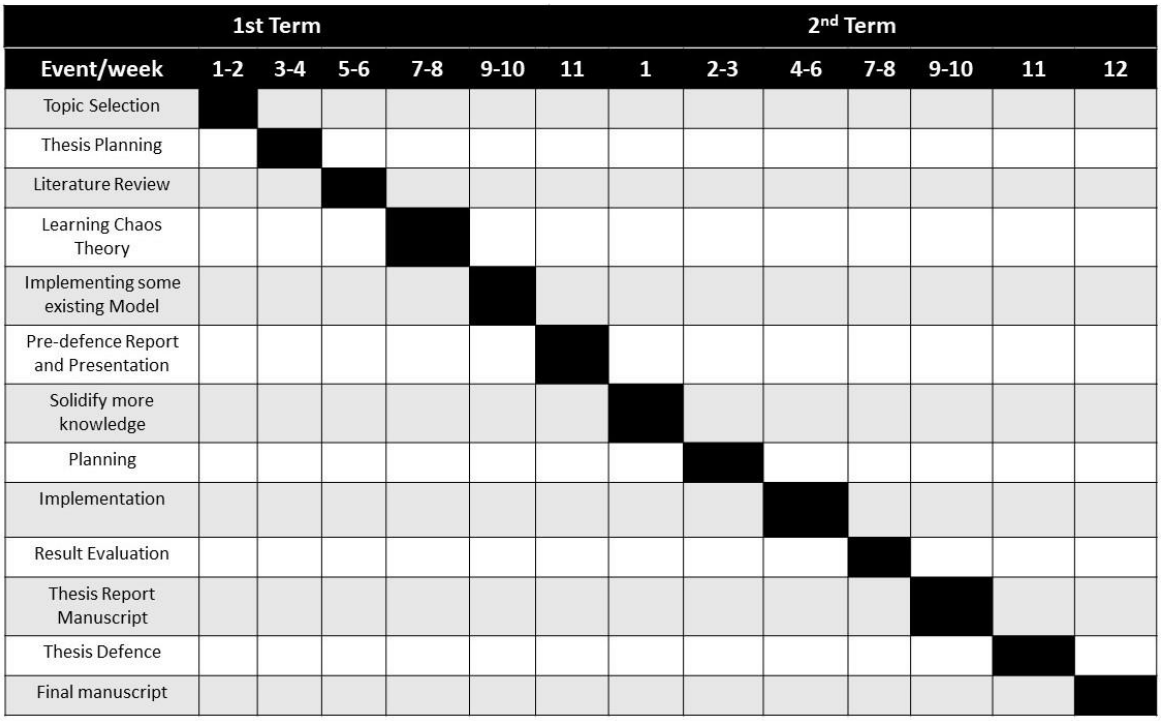

Fig 1.1: Gantt Chart for Project Planning

1.5 Contribution

This work was aimed to address some existing problems and find a better solutions to them. At the end of this work we are hoping to get done the following objectives:

- New chaos-based cryptosystem to secure IoT communications has been developed
- High-performance chaotic generator is designed using a discretized version of the Lorenz system. It can generate random keys that greatly improve the quality and security of the proposed cryptosystem
- New chaotic permutations at the bit level are achieved as proposed to improve the security of the cryptosystem.

1.6 Organization

The rest of the report is organized as follows. Chapter 2 discusses the related works previously done in this sector. All the required tools to design the proposed cryptosystem is designed in chapter 3. The methodology of the proposed cryptosystem is described in chapter 4. Chapter 5 validates the proposed cryptosystem with result analysis. Finally, chapter 6 concludes the report by discussing future scope of work to expand the research further.

Chapter II

Literature Review

For the last decade, several lightweight algorithms for security were presented with different security levels to protect data through the communication channels between IoT nodes. In order to obtain a relevant coverage of existing works related to lightweight cryptosystem, queries were performed. Going through the results of these queries, we only considered works dealing with IoT and lightweight cryptosystem concepts. In those works, the authors attempt to propose a “small” cryptographic algorithm, to face the very low battery load, the small size of ROM and RAM, and low CPU frequency. Some algorithms took advantage of the merits of the AES algorithm and attempted to adapt it to this constrained IoT node to ensure better security performances. Lee et al. implemented the AES encryption algorithm on an 8-bit microcontroller as an example of a hardware device. They evaluate the performance of their implementation as a function of plaintext size and the cost of the operation per hop in a network. The encryption and decryption time are measured related to the data sizes of 16, 32, 64, 128, 256, and 512 Bytes. For a data size of 16 bytes, the measured encryption time is 449 ms, resulting in an encryption speed of 0.29 kbit/s. This value is not enough for some applications that require a high encryption speed. Omrani et al. proposed a lightweight image cryptosystem for IoT devices called LICID. They implemented their solution in RaspberryPi. However, this board has significant resources, so it cannot be considered a constrained node. Abu Al-Haija et al. designed a microcontroller-based RSA. They used the Arduino Mega2560R3 microcontroller to implement the proposed RSA coprocessor with a small key of 32 bits. Some works have proposed cryptosystems using VHDL and targeting FPGA boards. Aishwarya and Sreerangaraju proposed a secure and lightweight compressive sensing of stream cipher . The proposed system is implemented using VHDL and simulated using the Modelsim tool. However, they did not give the resource consumption related to this implementation. Pasupuleti and Varma proposed a lightweight scheme with a Walsh–Hadamard transform access structure for providing data privacy in IoT. Their concern is more about access polity and they did not implement their solution in constrained IoT nodes.

Recently, other works considered chaotic systems for building cryptosystems thanks to the good cryptographic properties of chaotic systems. Indeed, chaotic systems have good cryptography features such as unpredictability, nonlinearity, aperiodicity, and high sensitivity to control parameters. In addition, their implementations require fewer resources in terms of processing, storage, and communication footprint compared to conventional approaches. Thus, they are lightweight in software development. These features made chaotic systems attractive for providing strong, lightweight, and efficient cryptography for resource constrained IoT nodes.

In contrast to those presented above, this work proposes a complete lightweight, and efficient cryptosystem with new confusion–diffusion layers. These operations are optimized to be implemented in different hardware boards with limited resources such as microcontrollers. In addition, the proposed solution makes no assumptions about data types. It is generic and open to any type of data (sensing value, text, voice, image, etc.). Moreover, the proposed solution shall go through a complete security analysis (randomness, entropy, histogram, etc.) which will validate the strength of the adopted method.

Chapter III

Required Tools

In the realm of securing Internet of Things (IoT) communications, conventional cryptographic techniques such as AES, RSA, and DES have been the prevailing tools employed. These methods, while effective, often demand substantial computational resources, making them unsuitable for IoT nodes with limited capabilities. However, in this work, a significant advancement has been introduced by devising a new lightweight and efficient cryptosystem tailored specifically for IoT applications. Lorenz system is being used to introduce chaotic behavior. This innovative solution encompasses a chaos-based random generator, as well as specialized confusion and diffusion components. Unlike existing tools, the tools developed here excel in resource optimization, ensuring low memory usage, swift encryption and decryption processes, and minimal energy consumption. This contribution stands out not only for its enhanced performance but also for its adaptability across various hardware boards and data types, establishing its potential significance in real-world IoT scenarios.

Chapter IV

Proposed Methodology

3.1 Overview of the cryptosystem

As it was pointed out in the previous section, the currently proposed approaches do not meet all the needs when designing a secure IoT network. Therefore, the main objective is to:

- Implement a powerful and less complex cryptosystem to secure IoT communications
- Validate the proposed cryptosystem in real use case covering the whole IoT lifecycle from data acquisition to data exploitation.

As illustrated in Fig. 4.1, the proposed cryptosystem is based on three essential blocks:

(1) random generator block to generate a key with high statistical proprieties

(2) chaotic permutations block to permute data with variable permutations, and

(3) diffusion block to xor the output of the previous step with a key to produce ciphered data.

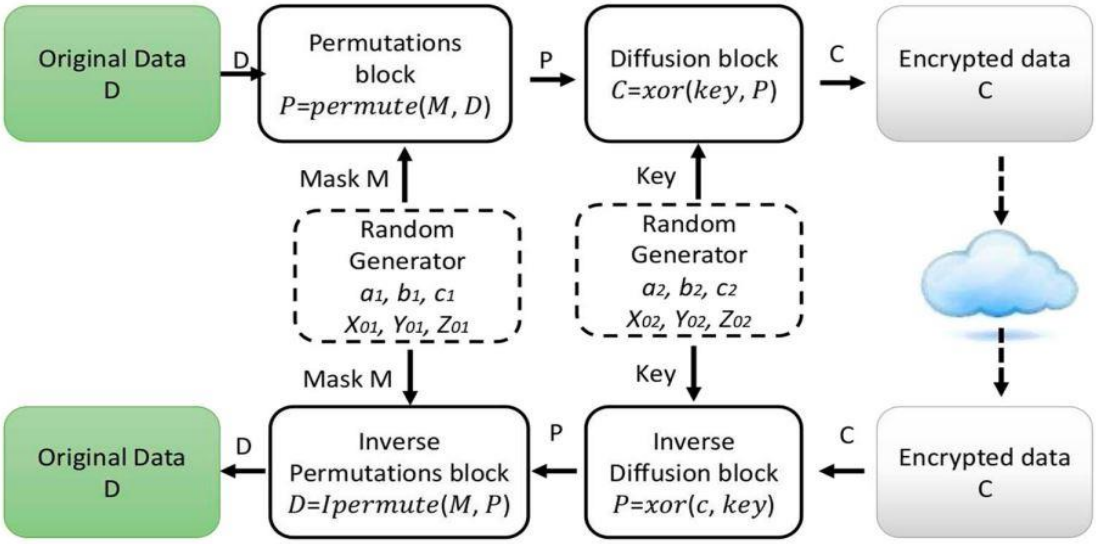

Fig 4.1: Overview of the proposed cryptosystem

In the following sections, we will discuss the details of each block.

3.2 Random Generator

For the random generator, we have chosen a chaotic system. As illustrated in the earlier section, several systems can be used. Among them, the Lorenz system is adopted to generate random keys. This choice is based on its better statistical performances and low computational resource requirements compared to the existing chaotic systems. Lorenz system is a deterministic chaotic system described by Eq. below:

$$\frac{d\,x(t)}{dt} = a(y - x)$$

$$\frac{d\,y(t)}{dt} = cx - y - xz$$

$$\frac{d\,z(t)}{dt} = xy - bz$$

where a, b, and c are the system parameters and x_0, y_0, and z_0 are the initial conditions. By knowing the initial conditions, it is possible to determine the system's evolution over time. However, with a slight difference in these values, the predictions will be fundamentally changed. For such a system, the chaotic effect is in x, y, and z solutions. To solve the Eq., numerical solution methods can be used, such as the Runge–Kutta method.

3.3 Encryption Process

Primarily the below algorithm is designed to perform encryption process:

Algorithm 1 Pseudo-code of the proposed permute function

Input: Data D (n bits), Mask M (n bits)
Output: Permuted data P (n bits)
Initialization: i=1, j=n
  for each bit k of M **do**
    if M_k = 0 **then**
      $P_k = D_i$
      i = i+1
    else
      $P_k = D_j$
      j = j-1
  end if
end for

3.4 Decryption Process

Primarily the below algorithm is designed to perform decryption process:

Algorithm 2 Pseudocode of the proposed inverse permute function

Input: Permuted data P (n bits), Mask M (n bits)
Output: Data D (n bits)
Initialization: i=1, j=n

```
for each bit k of M do
    if M_k = 0 then
        D_i = P_k
        i = i+1
    else
        D_j = P_k
        j = j-1
  end if
end for
```

Chapter V

Performance evaluation, Results and Discussions

In this section, a key size analysis is performed to study the robustness of the key generator against classical brute force attacks. If a generator can produce more than 2^{100} different key combinations, then it is considered unbreakable against this attack.

In this work, the generated key depends on 6 values: three initial conditions (x_0, y_0, and z_0) and three parameters (a, b, and c). Each value is encoded on 32 bits. Therefore, the key space is: $2^{32}\times2^{32}\times2^{32}\times2^{32}\times2^{32}\times2^{32} = 2^{192} \geq 2^{100}$. This value is far above the required keyspace making this scheme robust against brute force attacks.

Chapter VI

Conclusion

To secure IoT communications, this report proposes a new lightweight and efficient chaos-based cryptosystem for resource-constrained IoT nodes. The proposed cryptosystem is based on three essential components: (1) a chaotic generator based on the Lorenz system to generate random keys, (2) a new chaotic permutation that creates confusion and (3) diffusion using the xor operation with a chaotic key. Result analysis show that this cryptosystem is very promising to provide a robust tool against many attacks.

In future work, we intend to improve the proposed cryptosystem by proposing a key sharing mechanism. A lightweight security protocol that involves authentication of deployed IoT devices and hash functions to ensure data integrity are also in the perspective of this work.

References

- J. Cosgrave, "Ready to respond–skills gaps for responding to humanitarian crises in urban settings in the WASH and shelter sectors," [Online]. Available: https://www.urban-response.org/help-library..
- H. N. N. O. S. &. A. C. Jean-Paul A. Yaacoub, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 2, no. 14, pp. 115-158, 2021.