# **Abstract**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **Acknowledgement**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

**Contents**

Abasdflj Page

Abstract 45

Introduction 75

[**Abstract** 1](#_Toc143653521)

[**Acknowledgement** 2](#_Toc143653522)

[**Chapter I** 4](#_Toc143653523)

[**Introduction** 4](#_Toc143653524)

* [**1.1** **Introduction** 4](#_Toc143653525)
* [**1.2** **Problem Statement** 4](#_Toc143653526)

[**Chapter 2: Related Works** 5](#_Toc143653527)

[**Chapter 3: Required Tools** 6](#_Toc143653528)

[**Chapter 4: Proposed Methodology** 7](#_Toc143653529)

[**Chapter 5: Experimental Studies/Evaluation** 8](#_Toc143653530)

[**Chapter 6: Conclusion** 9](#_Toc143653531)

[**References** 10](#_Toc143653532)

# **Chapter I**

# **Introduction**

## **Introduction**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

## **Problem Statement**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **Chapter 2: Related Works**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **Chapter 3: Required Tools**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **Chapter 4: Proposed Methodology**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **Chapter 5: Experimental Studies/Evaluation**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **Chapter 6: Conclusion**

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

Internet of things (IoT) provides several applications such as intelligent urban transportation, smart factory, and smart health. In such systems, the transmitted data are important and must be secured to prevent destructive and unauthorized access to critical data. Indeed, existing IoT solutions come with conventional cryptographic techniques such as AES, RSA, and DES. However, some of these algorithms are no longer reliable and others require significant resources in terms of energy, memory, and computing power, making them unsuitable for IoT nodes that may have limited resources. To address these challenges, this paper develops a new lightweight and efficient cryptosystem to secure IoT communications. The proposed cryptosystem is composed of a chaos-based random generator, confusion, and diffusion blocks. Through a use case, the experimental results, at implementation and statistical levels, demonstrate good performances. The implementation results in the Mbed microcontroller NXP LPC1768 include low memory usage, fast encryption and decryption speed, and low energy consumption. The statistical results confirm the robustness of the proposed cryptosystem against many attacks according to the NIST test, key size, key sensitivity, information entropy, and statistical histogram analysis. Compared to related works, this paper proposes an enhanced lightweight cryptosystem with optimized confusion–diffusion layers that can be implemented in different resource-constrained hardware boards. Moreover, the proposed solution does not make any assumptions about the data types to be used in IoT networks. It is open to any type (sensing value, text, voice, image, etc.). These features guarantee the potential use of the proposed cryptosystem in many real-world applications.

# **References**