Arab American University

Faculty of Graduate Studies

A secure trusted Lightweight mechanism for IOB devices

By

Mohammad Yousef Mohammad Shadeed

Supervisor

Prof. Labib Arafeh

This thesis was submitted in partial fulfillment of the requirements for the master's degree in Cybercrimes and Digital Evidence Analysis

FEB / 2023

I

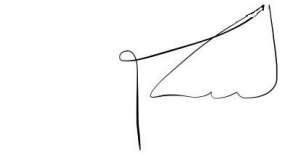
Thesis Approval

A secure trusted Lightweight mechanism for IOB devices

By:

Mohammad Yousef Mohammad Shadeed

/This thesis was defended successfully on 07/03/2023 and approved by:

Committee members	Signature
1. Proof. Labib Arafeh,/Supervisor	
2. D. Mohammad Abu Taha/ External examiner	
3. D. Mohammad Hamarsheh/ Internal examiner	

Declaration

I am the undersigned who submitted the thesis entitled:

A secure trusted Lightweight mechanism for IOB devices

I declare that this thesis has been composed solely by myself and has not been submitted, in whole or in part, in any previous application for a degree, except were stated by reference or acknowledgment that the work presented is entirely my own.

Students name: Mohammad Yousef Mohammad Shadeed

Date: Monday, August 21, 2023

Student ID: 202012845

Signature:

Dedication

I am sincerely grateful to the Almighty for the countless blessings and opportunities. He has bestowed upon me throughout my life. Without His divine guidance and affection, I would not have accomplished all that I have.

I dedicate this Master's degree to my beloved parents, spouse, son, and family who have constantly believed in me and provided me with unwavering support throughout my academic pursuits. Their love, guidance, and encouragement have been instrumental in my success, and without them, I would not have reached my present accomplishments. I am eternally grateful for everything they have done for me.

I would also like to express my gratitude to my supervisor, Professor Labib Arafeh, who has encouraged and motivated me to engage in critical thinking and aim for excellence. His valuable insights and expertise have had a significant impact on my growth and progression as a researcher and professional.

I would like to extend my gratitude to Dr. Muhammad Abu Taha, who made invaluable support to the completion of this study. Additionally, I am thankful to Engineer Yasser Abu Zneid for providing me with insightful guidance and support. Furthermore, I would like to express my appreciation to Muhammad Abu Joudeh and all others who have played a role in this endeavor.

Lastly, I dedicate this degree to my dear friends and colleagues who have been invaluable sources of support, inspiration, and camaraderie during my academic journey. I am deeply grateful for their presence in my life and for being there for me through both the triumphs and difficulties, making this experience even more significant and enjoyable.

Acknowledgment

I want to express my great thanks to Allah Almighty for his generosity and grace in granting me the health and the ability to accomplish this thesis.

I am privileged to have been a student of a truly exceptional supervisor, Professor Labib Arafeh, who imparted knowledge in such a way that the more one learned, the greater the desire to learn more. He taught us the importance of moral and ethical behavior above all else. I am immensely thankful for his inspiration, support, guidance, and constructive criticism throughout the preparation of my thesis. I will always treasure every piece of advice, comment, and word of wisdom he shared with me.

I would like to express my sincere gratitude and appreciation to the committee examiners for their dedication and invaluable time in reviewing my thesis and offering me the necessary feedback to improve it.

I extend my deepest gratitude to my parents for their unwavering support and encouragement.

Abstract

This study highlighting the most pressing challenges and areas of research interest. A review of various lightweight encryption algorithms is conducted and a modified version of a hybrid AES algorithm combined with the Huffman compression algorithm is proposed. These algorithms and their implementation are thoroughly presented.

In addition, the effectiveness of the master AES algorithm in encryption and decryption is evaluated through 100 tests with different text sizes. The obtained results indicated that the proposed algorithm exhibits improved execution time, with an average improvement of 18.75% across all test rounds. As an illustration, the performance of the algorithm is compared where an 8-byte text is encrypted and decrypted. The results show an 18.31% improvement over the master AES algorithm.

100 tests of encryption only were conducted using texts of varying sizes. The obtained results indicate that the proposed algorithm consistently outperforms the master AES algorithm in terms of speed across all test rounds. Subsequently, 100 rounds of decryption only are performed using the same texts as in the previous encryption rounds. The results show that the proposed algorithm also outperforms the master AES algorithm in terms of execution speed.

The security of the algorithm was evaluated making use of two tests namely, the Avalanche Effect and the Key Sensitive Attack. The obtained results indicated which results in a 53.54% difference in ciphertext for the proposed algorithm and 51.56% for the AES algorithm. Additionally, the results of the Key Sensitive Attack test demonstrated convergence in terms of security and protection of 99% between the two algorithms, as a substantial difference in ciphertext was observed when a single letter in the key was altered.

Keywords: IoT, IoB, WBAN, LWC, Cryptography, AES, Lightweight

Table of Contents

1. Chapter One

1.1 Introduction

Industry 4.0, also known as the Fourth Industrial Revolution, is a popular subject of study that encompasses the integration of cutting-edge concepts and technologies. This encompasses technologies such as RFID, big data analysis, cloud computing, intelligent sensors, machine learning, robotics, 3D printing, AI, augmented reality, IoT, and IoB. These advancements are transforming traditional, centralized production systems into modern, digital, and decentralized ones by seamlessly integrating people, machines, and data [1].

The IoT refers to a network of interconnected devices that communicate with each other. These "Things" are smart devices that have basic computing abilities and can react to their environment. The IoT has greatly impacted our lives by providing convenience and versatility through applications such as home automation, connected cities, vehicles, health monitoring, and many other services [2].

The IoT is rapidly growing, with projections of billions of interconnected devices in the near future. As IoT expands, it is also producing large quantities of data that are being collected and analyzed in real time across these devices. However, many IoT devices are constrained by limited computational resources such as processing power, memory, battery capacity, and connectivity capabilities [3].

The Medical IoT, which integrates the Internet of Things with medical technology, is advancing rapidly. A key part of this is the wireless body area network (WBAN), which is a network of wireless wearable or implantable devices. These devices monitor and transmit

physiological data to a server that can be accessed by medical professionals for remote diagnosis or treatment, improving the efficiency of medical services and promoting healthy living. However, these devices often rely on intermediate nodes due to their limited resources and can be vulnerable to unauthorized access or tampering, making it important to have a secure authentication and key agreement mechanism in place to protect sensitive data [4].

IoBs is a growing aspect of IoT, where devices worn, implanted, or in close proximity to the human body are connected to create a network. This technology has the possibility of offering a variety of benefits and uses in industries like healthcare, security, wellness, and entertainment. The IoBs have the potential to impact public health and safety greatly. To make the most of the benefits of IoBs, it's crucial to address and minimize the potential risks, limitations, and concerns associated with it [5].

1.2 Motivation:

With the advent of the technological revolution, an increasing number of devices, including medical and health devices, have become connected to the Internet. However, this connectivity has also led to an increased risk to patient health as these devices are vulnerable to attacks. This has prompted researchers and specialists to focus on enhancing the communication of information security of these devices to mitigate the potential dangers they pose.

In the healthcare sector, IoT sensors and devices are utilized to gather various health-related data from patients, including blood pressure, pulse rate, heart rate, temperature, oxygen saturation, and more. Prior to establishing a healthcare infrastructure model, it is crucial to ensure the security and privacy of this data. For instance, patients may employ smart IoT devices to collect their data, which is then outsourced to the cloud or other remote storage systems due to storage limitations. However, there exists a risk of exposing patients' sensitive information to

malicious entities or organizations aiming to derive commercial or economic advantages. Moreover, during the transmission of data, potential attacks such as eavesdropping, impersonation, man-in-the-middle attacks, collusion, and others can also occur.

The integration of IoT in healthcare service delivery is effectively tackling various data-related challenges, including seamless data transfer over the internet and the utilization of short-range wireless technologies. It is imperative to ensure robust protection of this data throughout its lifecycle, encompassing collection, storage, communication, and transmission. Additionally, strict control measures must be implemented to safeguard against unauthorized access, all while preserving the security of medical data. Moreover, the continuous and rapid growth of data plays a pivotal role in enhancing the accessibility of health information and services, facilitating advancements in this domain.

1.3 Problem statement

Data security is of paramount importance when transmitting information over a public network, where it may be vulnerable to malicious attacks. There are various types of attacks that can disrupt data transmission over a wireless channel. While unencrypted data transmission may be acceptable in certain scenarios, such as naturalistic observation. In many other cases, secure and dependable data transmission is imperative. For instance, in a natural living environment, health insurance companies may be interested in health-related data, whereas burglars may be interested in personal activities. There are numerous situations in which data security is crucial, making it a major concern in wireless data transmission [6]. Wireless Body Area Networks require security services like other systems, however, due to the hardware constraints of the devices in these networks, These services can be provided through the use of lightweight cryptography algorithms [6][7].

Securing IoT devices, particularly those implanted within the human body, such as those used for monitoring and regulating heartbeats, insulin levels in the blood, and electrical currents in the brain, is crucial. These devices are susceptible to a range of threats, including hacking, tracking, service disruption, forgeries, and tampering, and their failure can have severe consequences on the health and well-being of patients. Additionally, IoT and IoB devices have limited energy, resources, and computing power [7].

1.4 objectives of study

In order to enhance the security and efficiency of communication between these sensitive devices, this research is proposed:

- A lightweight and secure encryption algorithm that is computationally efficient and has fewer encryption cycles, and lower execution time compared to other algorithms.
- An additional code that compresses the algorithm, which results in fewer calculations, and lower consumption of resources.

The thesis is organized as follows: While chapter one briefly presents a smooth background to various related topics, chapter tow reviews and summarizes related research works. Chapter three presents the methodology. Chapter four present the result and discussion. Chapter five briefly concludes and proposes future works that can be conducted based on the obtained results.

1.5 Background

This section introduces the concepts of the fourth industrial generation, the IoT, Wireless body area network, internet of bodies, Introduction to security, LWC, lightweight cryptography, and Compression coding.

1.5.1 The fourth-generation revolution (Industry 4.0)

Several scholars and professionals have identified four major industrial revolutions throughout history, as depicted in Fig. (1). The latest and current revolution is known as Industry 4.0 and it represents a continuous and ongoing transformation of the industry. This revolution marks a significant shift in the way businesses operate, leveraging technology and data to improve processes, enhance customer experience, and drive innovation. The rise of Industry 4.0 is driven by the convergence of digital, physical, and biological systems, bringing about a new level of interconnectedness and automation in the industrial sector. As a result, Industry 4.0 is expected to have far-reaching impacts on the economy, society, and the way people work, live, and interact.

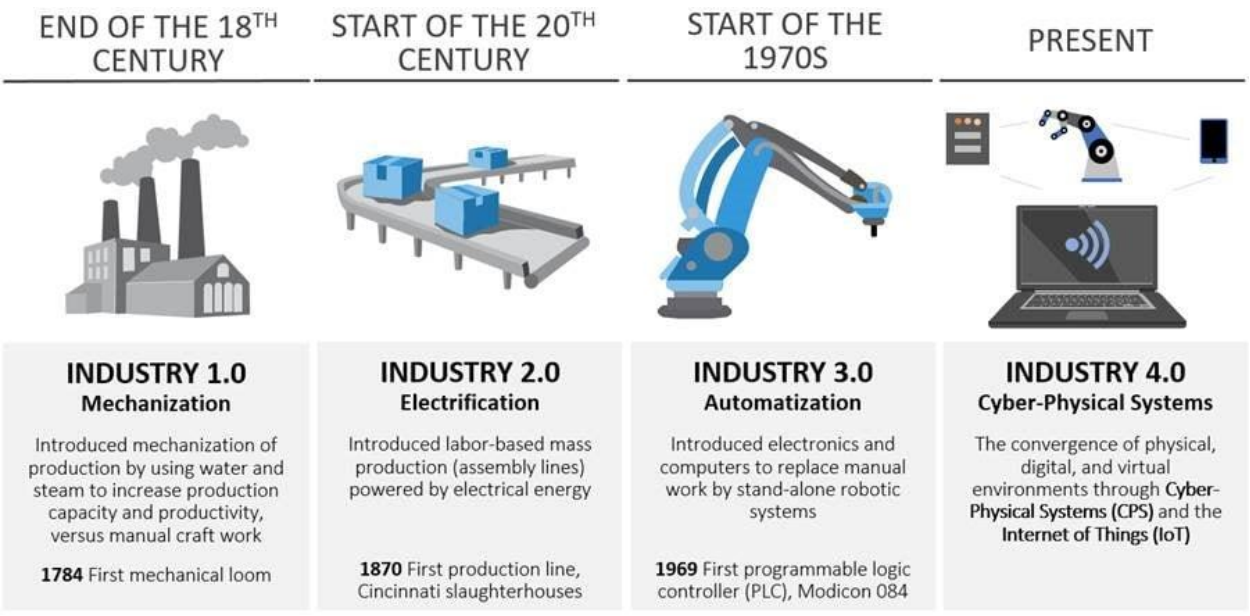


Fig.1: Diagram depicting the fourth industrial revolution[8].

Table (1) lists types of technologies frequently associated with the industry 4.0 concept.[9].

Table 1: Technologies of fourth generation [9].

Technologies	***Definition***
Computer-Aided Design and Manufacturing	"It is suggested that using computerized systems to create project and work plans for products and manufacturing will enhance efficiency and efficacy "
Integrated engineering systems	"Proposal to enhance efficiency and collaboration through the integration of IT support systems for exchanging information in product development and manufacturing ".
Digital automation with sensors	"Automation systems with embedded sensor technology for monitoring through data gathering "
Flexible manufacturing lines	"Using sensor technology, particularly RFID, to digitize manufacturing processes can help implement reconfigurable manufacturing systems (RMS) efficiently and cost-effectively by allowing for seamless integration and rearrangement of products within the industrial environment ".
Manufacturing Execution Systems (MES) and Supervisory control and data acquisition (SCADA)	"The use of SCADA technology and real-time monitoring for data collection enables remote control of production and the transformation of long-term schedules into short-term orders with improved efficiency, made possible by considering restrictions through the use of an MES.
Simulations/analysis of virtual models	Using techniques like finite elements and computational fluid dynamics in engineering projects allows for the creation of model-based designs, which can be simulated using synthesized models to test the properties of the design ".
Digital Product-Service Systems	"Proposal to improve capabilities and functionality of products through the integration of digital services using IoT platforms, embedded sensors, processors, and software ".
Additive manufacturing, fast prototyping, or 3D impression	"Versatile manufacturing machines enable flexible manufacturing systems (FMS) to turn digital 3D models into physical products, allowing for flexible manufacturing processes ".
Cloud services for products	"Cloud computing utilizes internet-based services such as databases, analytics, and storage to boost product capabilities and services. It offers on-demand access and cost savings, and has advantages over traditional systems including resource flexibility, cost-effectiveness, and faster innovation ".
Big Data	"Big data refers to a massive, fast-growing data set analyzed using data mining, storage, and visualization tools. It encompasses both the data and the processing tools, and is essential in making decisions at both operational and managerial levels ".
Internet of Things (IoT)	"IoT is a network of interconnected objects using sensors, software, and smart devices to communicate and exchange data over the internet. It offers various business and personal applications, including customizable industrial uses such as fraud detection, predictive maintenance, CRM, supply chain optimization, and healthcare sensors ".

1.5.2 IoT (internet of things)

The IoT refers to the interconnected network of physical devices, such as sensors, appliances, and vehicles, which can communicate and exchange data with each other and with the internet. This concept builds upon the idea of Machine-to-Machine (M2M) communication, which was developed in the 1970s to describe the communication between devices using wired or wireless connections. The widespread adoption of the internet in the 2000s enabled the expansion of M2M communication to a broader range of applications, leading to the emergence of the IoT. In this context, "Things" can refer to any type of device or object that is connected to the internet and can communicate with other devices, automatically sending and receiving data without the need for human intervention [10] [11]. The concept of the IoT is closely related to the idea of ubiquitous computing, which refers to the presence of computers in all aspects of life, and encompasses other concepts such as wearable computing and tangible computers [12][13][14].

The IoT is a rapidly growing field that connects physical devices with the digital world through the use of smart objects that have unique identification. Its objective is to provide a seamless connection between people and things at any time and place through any network service. According to recent research, the number of IoT devices was 22 billion in 2018 and is projected to reach 41.6 billion by 2025, resulting in the generation of 79.4 zettabytes of data [15]. This significant growth and ambitious goals make the IoT a major trend in the advancement of ICT [16][17]. The IoT incorporates various traditional telecommunications and networking technologies to enable a comprehensive approach to digitization and connectivity. This has the potential to bring about significant changes across various industries such as business, energy, media, education, public health, transportation, and logistics[18][19]. The IoT can be categorized into different fields like Internet of Industrial Things, Internet of Medical Things, Internet of Defense and Public Safety Things and more [20].

In this research, we will focus on the Internet of Bodies, which refers to the body centric IoT. The IoT is a network of devices that can be controlled using smartphones, smartwatches, and other devices [21].

The IoT ecosystem is comprised of web-enabled smart devices that are equipped with components such as processors, sensors, and communication hardware. These devices are capable of collecting, transmitting, and acting upon data. The sensor data generated by these devices is conveyed to an IoT gateway or another edge device for analysis, either in the cloud or locally. Additionally, these devices have the ability to communicate with other interconnected devices and take actions based on the information received from their counterparts. [22]. While people can interact with these devices, such as configure them or access data, they typically function independently without human intervention [23][24]. The connectivity, networking, and communication protocols used with these web-enabled devices depend on the specific IoT applications being implemented [25]. IoT can also be integrated with machine learning, a form of artificial intelligence that improves the efficiency and dynamic nature of data processing [26][27]. Fig. (2) shown the flow of data from collection to processing in the IoT.

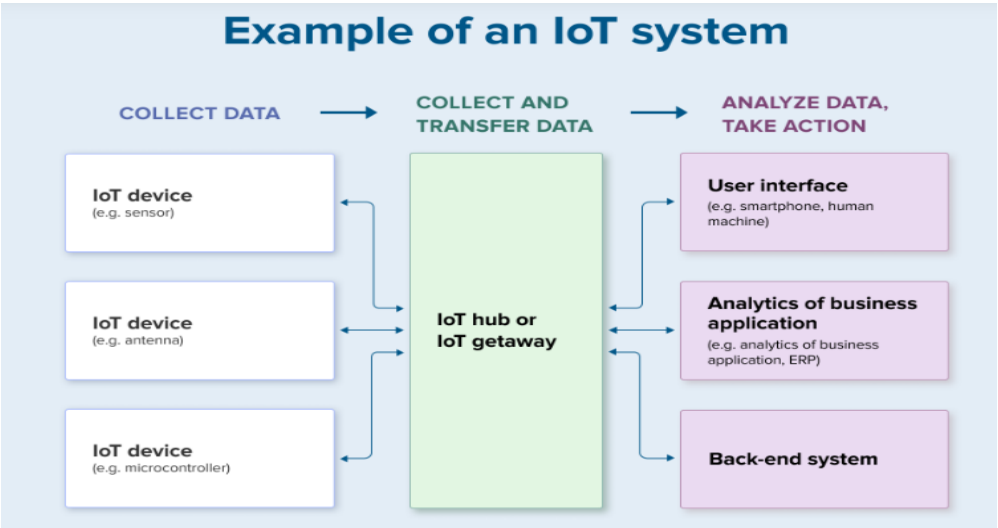


Fig.2: processing in the IoT [34]

1.5.3 Layers of IoT

It can be difficult to determine which technology will play a pivotal role in shaping the future, given the numerous innovations and advancements that are currently being made. Nevertheless, a comprehensive understanding can be gained by dissecting it into four distinct layers that contribute to the formation of the IoT, Fig.(3) shown the IoT layers [28][29].

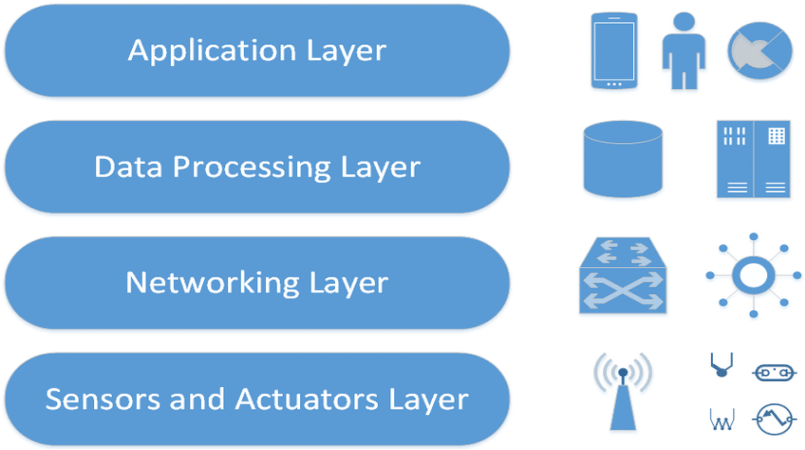


Fig.3: layers of IoT

1.5.4 Wireless body area network (WBAN)

WBAN is a type of Wireless Sensor Network that is designed to monitor vital signs of patients. It is composed of small bio-medical devices known as nodes, which are placed on or inside the human body to gather information. WBANs are designed to overcome the challenges of miniaturization, reliability, and security. The primary focus of WBAN research is to develop a framework for tracking healthcare and biomedical devices, allowing for earlier diagnosis and treatment through continuous monitoring of patients. WBANs offer greater flexibility and mobility for patients and provide doctors with a comprehensive view of a patient's status. The Sensors and the positions of a WBAN are shown in Table (2). [31][7].

Table 2: Sensors and their functionalities[30]

Sensors	***Positions***
Implant node	"They are positioned below a sink node in the human body ".
Body surface node	"It is located on the surface of human skin ".
External node	"No interaction takes place with the skin ".

As illustrated in Fig. (4), a WBAN, is a specialized network that serves to track, regulate, and exchange various crucial physiological signs of the human body. Such physiological signs, including temperature, pulse rate, and electrocardiogram (ECG), can be monitored using sensors that are attached to the body or embedded in wearable clothing. The network may also include actuators for the administration of medication. [32][31].

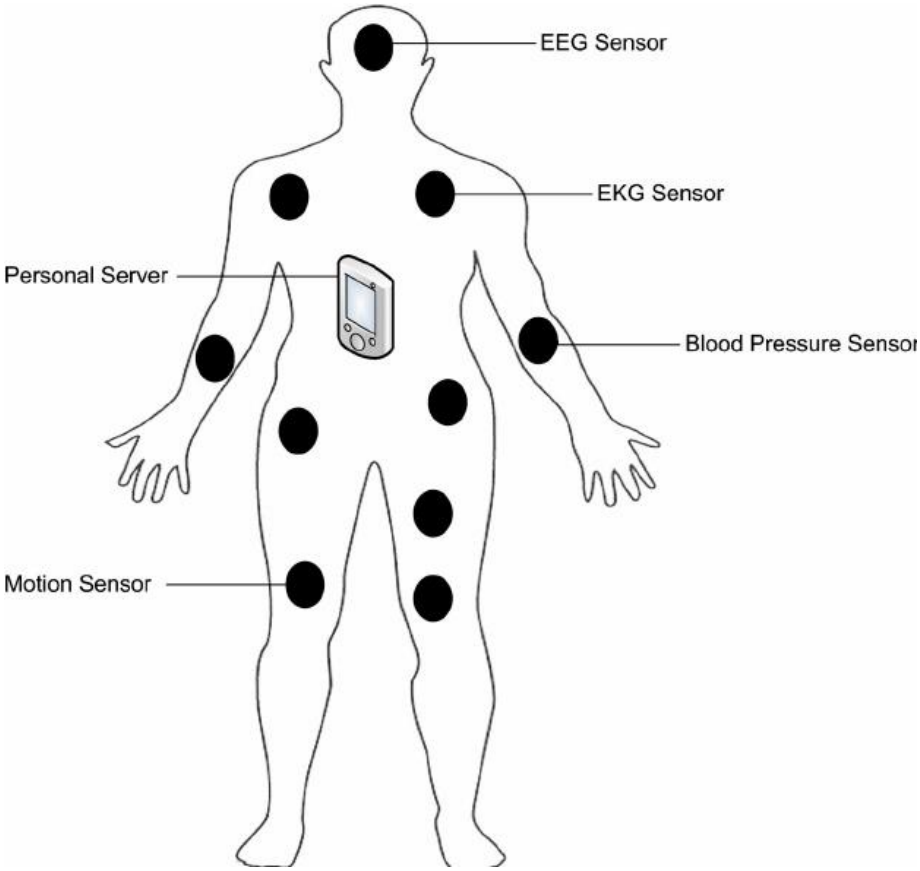


Fig.4: general view in WBAN

Issues and Challenges in WBAN

The rapid growth of the WBANs has presented significant challenges for the research community, despite the numerous applications and advantages it offers. Some of the most pressing research issues and difficulties associated with WBANs are listed as follow:

1. The efficiency of WBANs can be affected by their network topology. A well-designed network architecture is crucial for WBANs due to the limitations imposed by body movement, limited transmission range, energy restrictions, and various types of sensor nodes [33].
2. Energy efficiency and network lifetime are important considerations in a WBAN system. Each sensor node has limited resources in terms of energy, memory, computation, and bandwidth. The energy consumption of sensor nodes increases when they transmit data to each other, instead of focusing on sensing their surroundings. Recharging or replacing batteries may be impractical or undesirable due to the constraints and requirements of the specific application [34].
3. The stability period and reliability of a network are important aspects to consider in WBANs. The stability period of a network is defined as the duration from the start of operations until the failure of the first sensor node. This period is crucial as it is desired for the network to operate continuously for extended periods without requiring human intervention. To achieve this, it is necessary to minimize communication and evenly distribute the workload among the sensor nodes. This can be accomplished through the implementation of a load-balancing strategy that distributes the workload uniformly across all the nodes [35].
4. Security is a critical aspect of WBANs. The collection of sensitive personal information by the sensor nodes of a WBAN makes it susceptible to various types of attacks, both active and passive, such as eavesdropping, spoofing, and snooping. Given the multiple user transmission and receipt of data in the WBAN network, it is imperative that the data

exchange is secure. Additionally, messages transmitted and received within the network must be non-repudiable, meaning that both the sender and the receiver cannot deny the transmission and receipt of the messages [36][37].

In this research, all the concerns and challenges mentioned above will be addressed, as the proposed system will be safe, effective, work in real time, it will be protected, fast in data transfer, flexible, and it will address energy problems, protection problems, and data transmission problems in real time, and it will be very strongly encrypted.

1.5.5 IOB

The Internet of Bodies is the concept of connecting the human body to the internet to optimize everyday activities using available knowledge and services. A specific application of IOB is the Internet of Sports (IoS), which refers to devices and software that track and monitor human activity in the realm of fitness and sports [38]. These high-tech biological devices have the potential to improve medical solutions and assistive technologies, but also present new challenges. IOB also includes the use of personal mobile devices, as well as specialized devices such as smart contact lenses, cochlear implants, and electronic pills [39]. This field encompasses multiple areas of study, including the use of the internet for computing, the design and development of software, the interaction between humans and computers, and the use of data and networks for technology purposes [40]. Fig. (5): shows the some of IoB sensors.

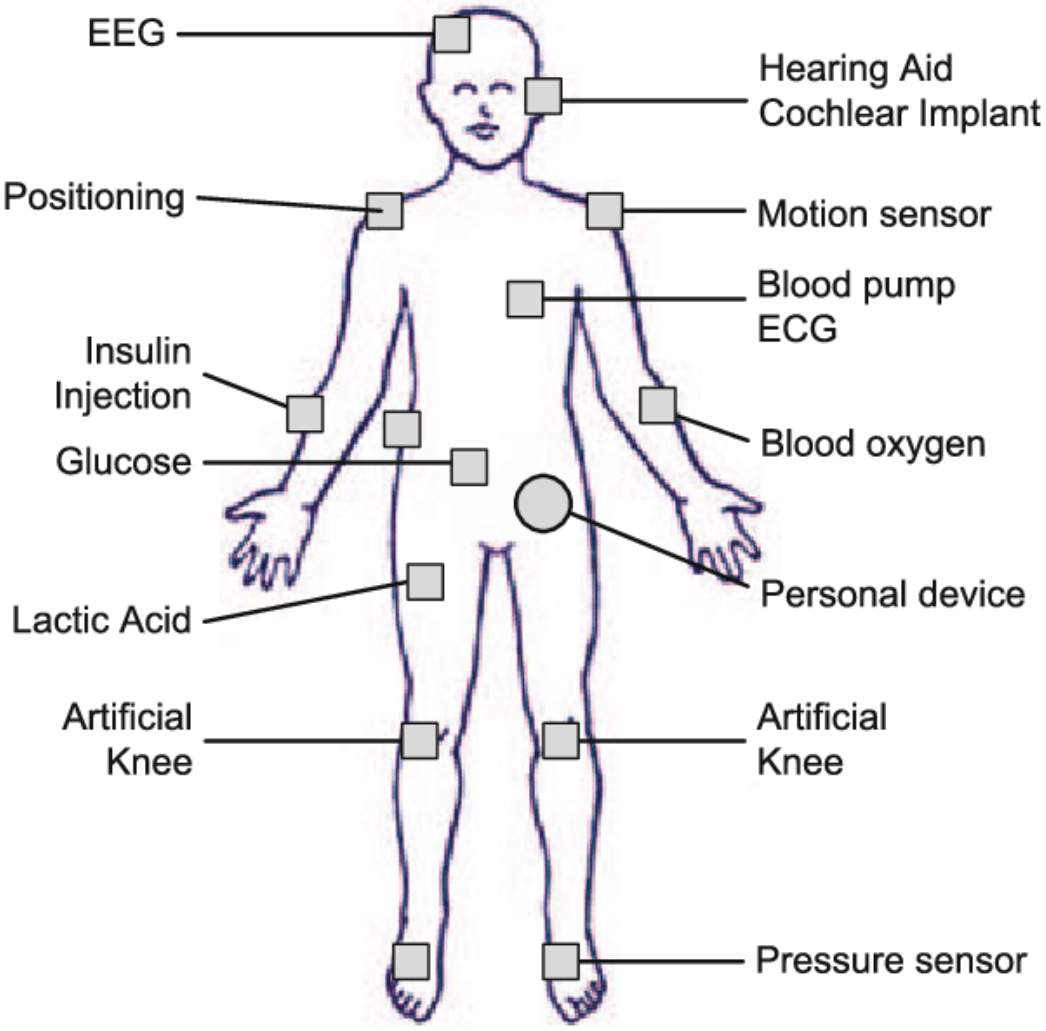


Fig.5: some of IoB sensors[38].

IoB Risks, Concerns

Despite the many benefits of the Internet of Bodies, there are also risks, concerns, and challenges that must be addressed to fully realize its potential[41][42]. Security risks and privacy concerns are major obstacles to the widespread use of IoB devices, particularly those that control vital body functions or collect sensitive user data (e.g., heart pacemakers) [43].. Additionally, it is possible to infer sensitive information from no sensitive data through data analytics, even if the data itself is not considered sensitive [44][45][46].

Subsequent to the concerns and challenges mentioned above, the topic of this research is related to addressing these concerns and challenges, and the topic of research is related to contributing to a large part of these concerns.

1.5.6 Security of IoT

The protection of information and information systems from unauthorized access, use, disclosure, alteration, disruption, or destruction is referred to as Information Security. This is crucial as information is considered a valuable asset and needs to be guarded against cyber-attacks like hacking, malware, and data breaches. Ensuring Information Security involves multiple strategies, including the utilization of secure passwords, implementation of encryption protocols like SSL/TLS for data transmission over the internet, regulating access to information and systems through authorization procedures like user accounts, permissions, biometric authentication, and physical security measures such as security keys.

It is important to keep data related to measurements and controls confidential, such as information about patient monitoring processes, as this information should not be accessible to competitors. This is why it is necessary to consider security threats when deploying IoT-based systems. Cyber attackers can easily target IoT systems for several reasons. Firstly, the IoT does not have a central system or intelligence to identify cyber attackers. Secondly, the IoT relies on wireless communication, which is easier to interfere with. Finally, IoT devices have limited power and computational capabilities, making it more difficult and expensive to implement traditional security algorithms. To ensure the secure transmission of data without any information leakage through the IoT, it is necessary to use cryptography. It is well known that data transmitted over the internet is vulnerable to being accessed by intruders who can manipulate control signals or issue unauthorized commands, leading to improper operations [47] [48].

1.5.7 Lightweight Cryptography

Lightweight is a characteristic that applies to all forms of Ubiquitous computing. These devices have limited battery life, small memory space, and quick response time because they are not standalone computers, but rather a component of a larger system, such as a machine or other hardware [49][50]. The term "lightweight software" is used to describe software that is optimized to meet these constraints of speed, encrypt / decrypt speed, data transfer in real time, and energy consumption[51][52]. The fundamental characteristics of lightweight software are its limitations in these areas [53].

One of the main challenges in designing lightweight encryption algorithms is the trade-off between security and efficiency. In general, more secure algorithms tend to be more computationally intensive, while less secure algorithms are faster and more efficient. As a result, it is important to carefully balance these factors when designing lightweight encryption algorithms [54][55].

The Cryptography Research Committees (CRYPTREC) have defined lightweight cryptography as cryptographic techniques and algorithms that are suitable for use on devices with limited computational resources and memory. These techniques are necessary due to the growing number of low-resource devices, such as IoT devices and embedded systems, that are connecting to the internet and require secure communication and data protection. As a result, lightweight cryptography systems have been developed to address these issues and provide an efficient means of securing data on these devices. Lightweight cryptography can be implemented in either hardware or software and is designed to minimize the cost, power consumption, and latency of the encryption process. These systems need to have small circuit sizes and low latency to meet the needs of real-time operating systems and computers, and to have sufficient memory storage for program development on devices with limited RAM and ROM [56][57].

According to the National Institute of Standards and Technology (NIST), Lightweight Cryptography (LWC) refers to cryptographic systems that have been optimized to cater to the needs of devices with varying specifications, especially those that are resource-constrained. This definition implies that all cryptographic methods can be deemed LWC if it is possible to adjust their resource needs to achieve the desired result. However, asymmetric encryption is a noteworthy exception due to its intricate nature and substantial resource requirements. On the other hand, symmetric encryption can be applied in such systems if it is suitably optimized to meet the specifications [58].

In the light of the previously discussed critical challenges, it has been determined that an LWC algorithm should consume minimal memory and power, while also providing efficient performance while maintaining the desired level of security. As such, the requirements for LWC can be summarized (Low memory consumption, Low power consumption, good performance, andAdequate security level)[58]. Fig. (6) displays Triangle for lightweight cryptography.

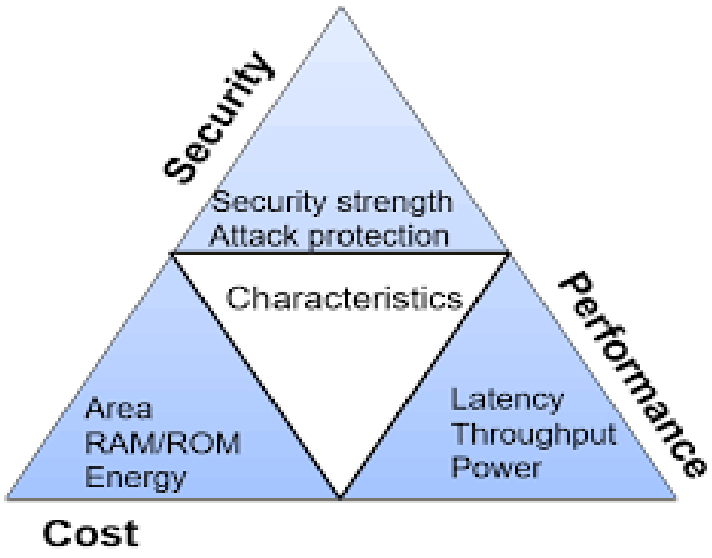


Fig.6: Triangle for lightweight cryptography[59].

The factors to consider in designing a Lightweight Cryptography algorithm include[60]:

- Key Size, Number of Rounds, Block Size, and Structure.

1.5.8 LWC cryptography algorithms

A wide range of LWC algorithms offer various strengths in terms of performance and security. After reviewing several related studies, it has been observed that there is a trend towards the use of stream ciphers due to their high efficiency in terms of performance. However, most of the algorithms reviewed were based on block ciphers, as they provide superior security with notable performance enhancements. In the following sections, a selection of LWC algorithms will be presented, categorized based on their underlying principles as stream or block ciphers. Table (3) provides a summary of these LWC algorithms [60].

Table 3: Summarize LWC algorithms[61][62]

Block cipher	***Key size(bit)***	***Block size (bit)***	***No. of rounds***	***Comment/Characteristics***
PRESENT	80, 128	128	32	"Less count, memory, encrypting small data "
GIFT	128	64.128	28.40	"Fast scheduling. high throughput "
KATAN	80	32, 48, 64	96, 144, 192	"oriented block cipher, inefficient software implementation, too much energy, low throughput "
SIMON	64~256	32~128	32~72	"Performance, easy, flexible "
RECTANGLE	80	64	25	"Hardware-friendly, faster, and high throughput "
SIT	64	64	5	"Fast key scheduling low, energy "
AES	128, 192, 256	128	10, 12, 14	"Excellent security, Flexible "
DES	64	64	16	"Not very secure but flexible "
3DES	112, 118	64	48	"Good security, flexible"
Blowfish	32-448	64	16	"Excellent security, flexible"
Twofish	128, 192, 256	128	48	"Can't be broken remotely"
Curupira	96, 144, 192	96	16	"Less space is required to store S-boxes"
TEA	128	64	32	"Security can be enhanced just by increasing the number of iterations"
HUMMING BIRD	256	16	256	"Suitable for RFID tags or Wireless Sensor Networks, Low power consumption, High speed"
TWINE	80, 128	64	36	"Ultra-lightweight, Enough speed"

LED	64, 128	64, 128	-	"Efficient hardware implementation, used for transmission of RFID tags"

Lightweight cryptography is specifically designed to provide robust and efficient communication and data protection while being more cost-effective in terms of computational resources and memory usage than traditional encryption methods [61][63]. The main objective of LWC is to guarantee the secure transmission of data between sender and receiver while minimizing the cost and resource requirements of the encryption process and minimizing the risk of attacks. This includes minimizing power and memory usage and ensuring that data encryption and decryption can be performed in real-time without causing transmission and reception delays. The AES algorithm has met all these criteria and is considered one of the best lightweight algorithms for use in resource-limited hardware environments. This research aims to achieve the same level of security as non-lightweight encryption methods while being more suitable for use on devices with limited resources [64][65].

AES Algorithm

It is noteworthy that among all block cipher algorithms, the Advanced Encryption Standard (AES) is the most thoroughly examined [66][67]. Various studies have been conducted and continue to be conducted on AES, with the goal of making it more suitable for lightweight and IoT applications. AES operates on data blocks of a fixed size of 128 bits and offers the flexibility of selecting the key size based on the desired level of security. There are three versions of AES, named AES-128, AES-192, and AES-256, each with 10, 12, and 14 rounds, respectively. Each version employs multiple operations to encrypt a data block [68][69].

The AES was officially standardized by the National Institute of Standards and Technology (NIST) in 2001, and since then, it has been extensively researched by scholars. It is important to note that different devices may have varying security requirements and may have different constraints such as power budget and processing speed [70][71]. The AES is a widely recognized and highly regarded symmetric encryption algorithm that has been considered as a major advancement in the field. AES possesses exceptional performance characteristics and an exceptional level of security in comparison to similar algorithms. The AES offers a range of key sizes, providing various levels of security [72][73]. Fig. (7) shows an AES diagram.

The AES algorithm consists of four invertible transformations: SubBytes Transformation Fig. (8) [74], ShiftRows Transformation Fig. (9) [75], MixColumns Transformation Fig. (10) [75], and AddRoundKey Transformation Fig. (11) [75].

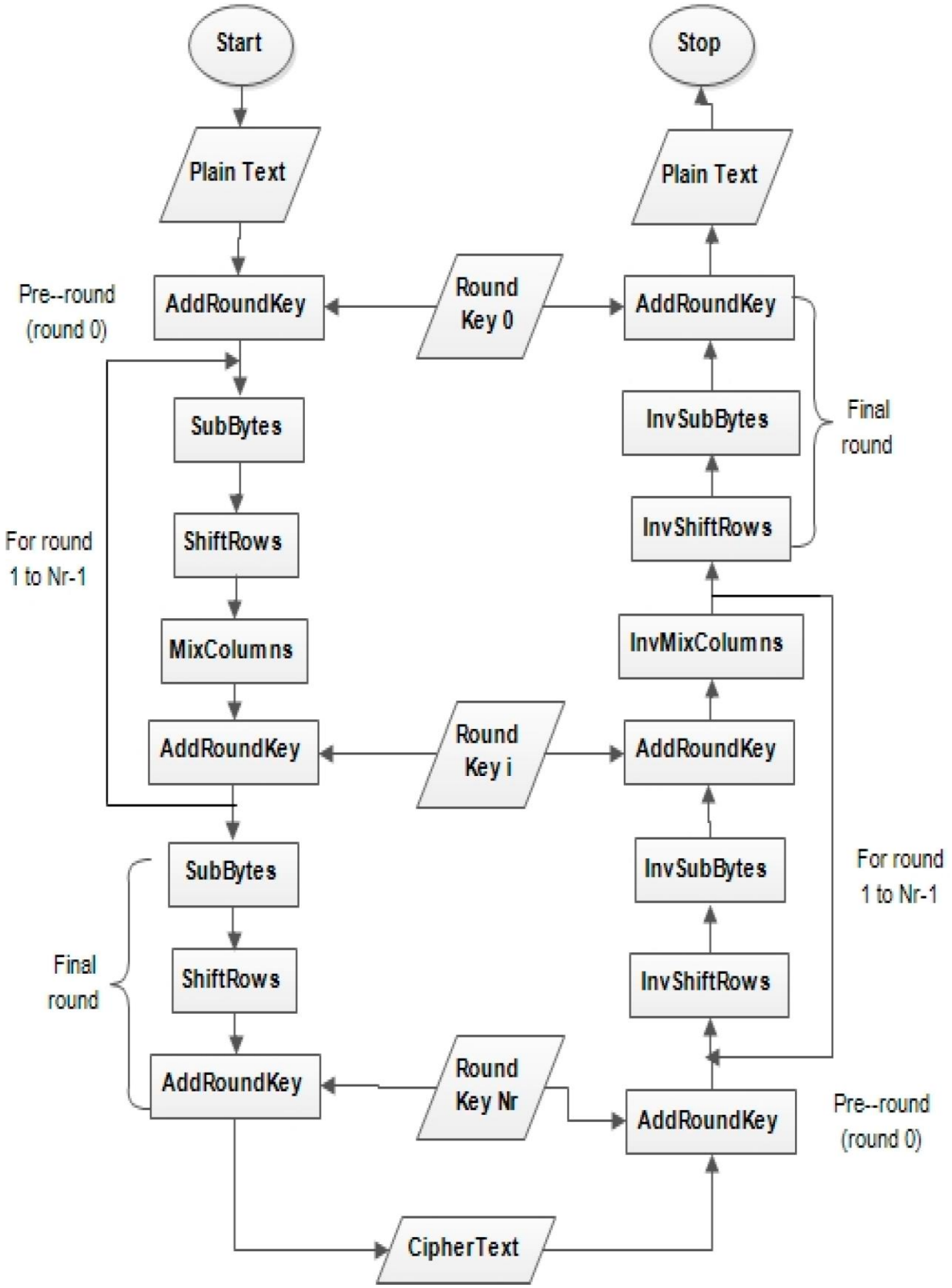


Fig.7: 10 rounds of AES - 128 (block Diagram)[74]

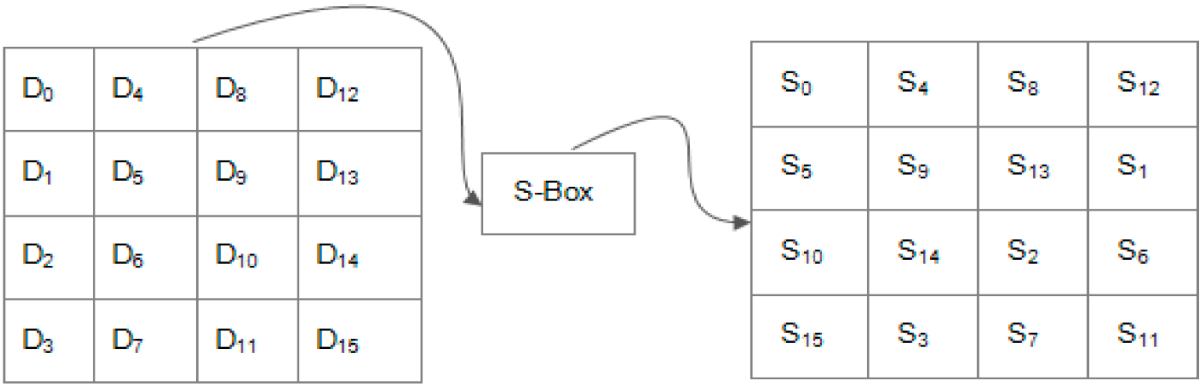


Fig.8: SubBytes Transformation [74]

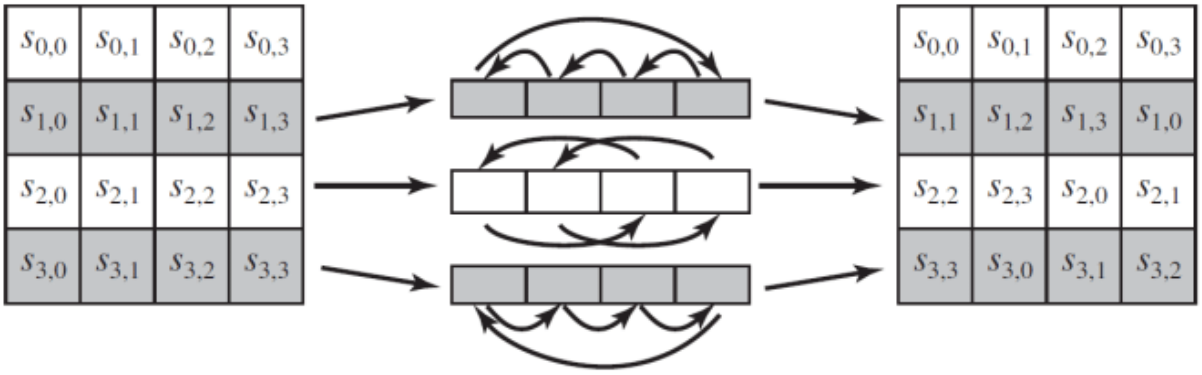


Fig.9: ShiftRows Transformation[75]

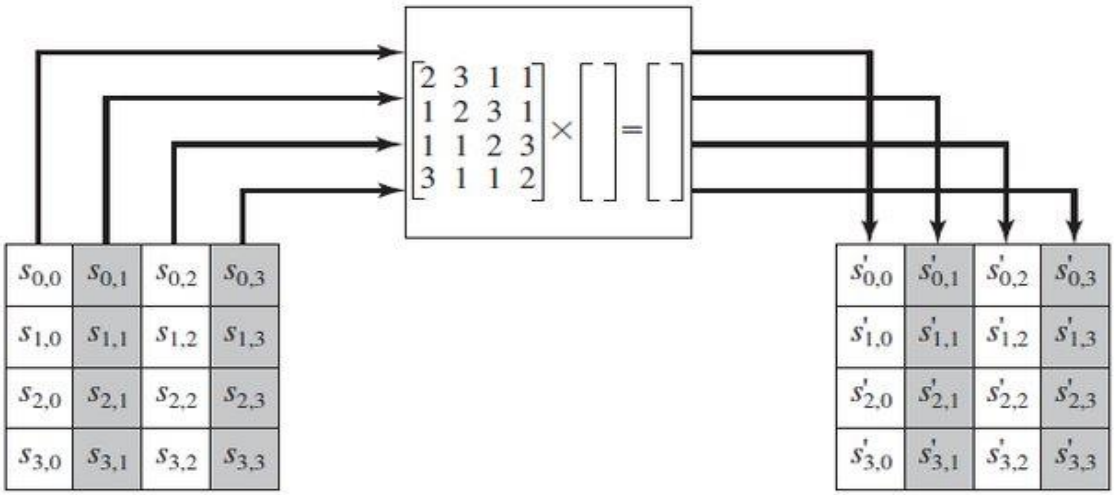


Fig.10: MixColumns Transformation[75]

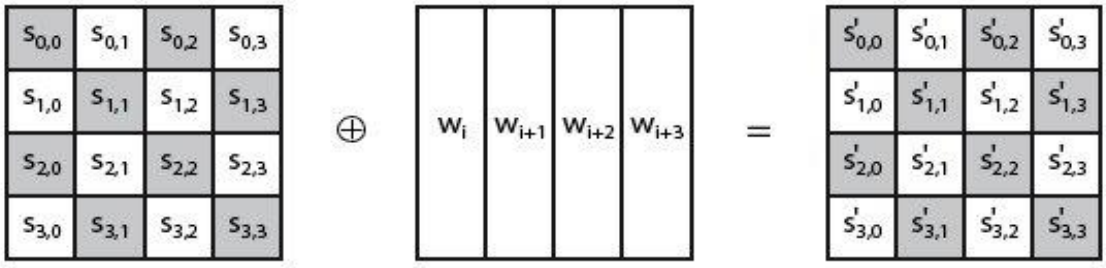


Fig.11: AddRounkKey Transformation[75]

1.5.9 Compression Coding

In this section, we'll examine various well-known coding methods used in data compressions, such as Huffman coding, Arithmetic coding, LZ coding, Burrows-Wheeler Transform (BWT) coding, Run Length Encoding (RLE), transform coding, predictive coding, dictionary-based methods, fractal compression, and Scalar and Vector Quantization. Table (4) provides a comparison of these techniques, which form the basis of the data compression field.

Huffman coding is a "widely-used coding technique that effectively compresses data in a variety of file formats. It is a form of optimal prefix code that is commonly employed in lossless data compression. The basic principle behind Huffman coding is to assign variable-length codes to input characters based on their frequency of occurrence. The output is a variable-length code table for encoding source symbols. The technique is uniquely decodable and comprises two components: the construction of a Huffman tree from an input sequence and the traversal of the tree to assign codes to characters. Huffman coding remains popular due to its simple implementation, fast compression, and lack of patent restrictions. There are several variations of Huffman coding, including Minimum Variance Huffman code, Canonical Huffman code, Length-Limited Huffman code, Non-Binary Huffman code, Adaptive Huffman code, Golomb code, Rice code, and Tunstall code. Various compression methods, such as Deflate, JPEG, and MP3, use Huffman coding as a back-end technique" [76].

Fig. (12) depicts the flowchart of the Huffman algorithm. To illustrate the concept of this algorithm, Fig. (13) indicates the Huffman tree and its final code [77][78][79].

```
start
 read the text
for:
  X: arrange source symbols in descending order of probabilities
    merge two of the lowest probabilities
     assign zero and one to the top and bottom branches. respectively
   if:
      there is more than one unmerges node
       go to X and repeat
  else:
              stop reading go to generate a code word
  end
```

Fig.12: Huffman coding pseudocode

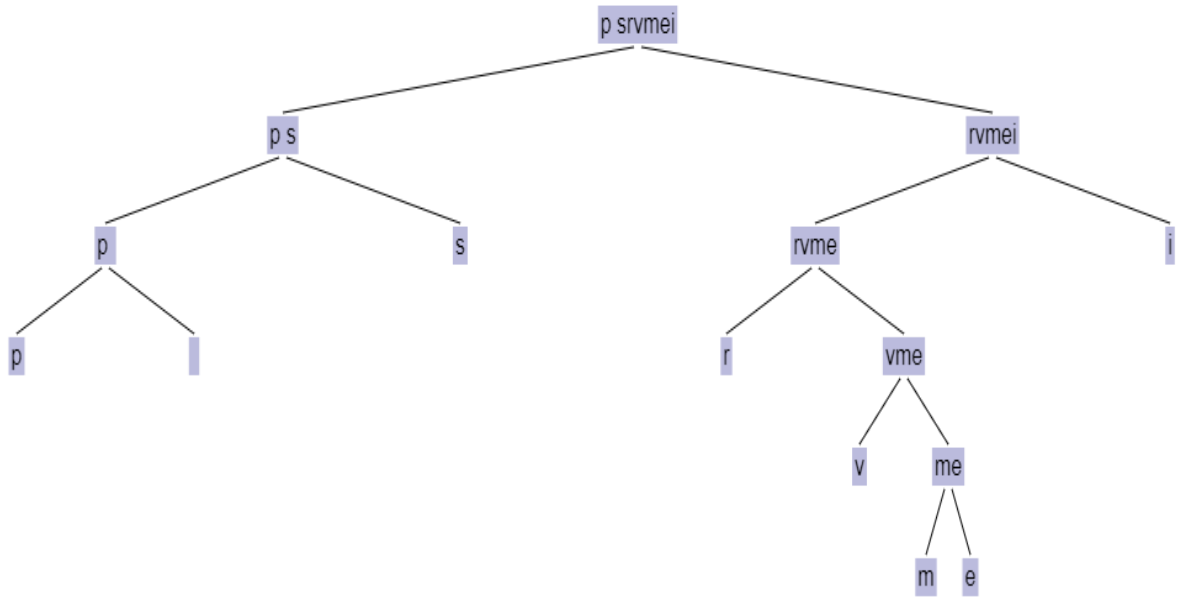


Fig.13: The Huffman tree construction process

the construction of the binary tree: the Huffman coding algorithm works as follows:

Step 1: Compile a table that lists the nodes, their symbols, frequency, and left and right values (Table 5).

Step 2: Find the two nodes in the list with the lowest frequency, and label them as "-1" and "E1".

Step 3: Combine "-1" and "E1" by creating a new parent node "E-2", with the symbol being a concatenation of "-1" and "E1" symbols, frequency equal to the sum of "-1" and "E1" frequencies, "E1" as its left, and "-1" as its right.

Step 4: Eliminate "-1" and "E1" from the list and include "E-2".

Step 5: Repeat steps 2 to 4 until only one node remains in the list.

To decode a binary array, the following procedure must be followed:

1. Start at the root node of the binary tree.

2. Read the next bit from the binary array.

3. If the bit is a '0', move to the left. If the bit is a '1', move to the right.

4. If the current node is a leaf node, output the symbol associated with that node and return it to the root node.

5. Repeat steps 2-4 until the entire binary array has been processed. This process works because each character in the original data is associated with a unique binary code that follows a specific path through the binary tree. By following that path, the decoder can reconstruct the original data. The next procedure must be followed: [80].

Step 1: Initiate the process at the starting point of the binary code.

Step 2: Proceed to the next bit and combine it to form a subgroup of bits.

Step 3: Check the code dictionary for a character translation associated with the formed subgroup of bits. If such a translation exists, add it to the decoded information and reset the subgroup. If not, continue to the next bit and include it in the subgroup.

Step 4: Repeat steps 2 and 3 until the end of the binary code is reached.

Table 4: various coding comparison

Coding	***Advantages***	***Application***	***Feature***	***Compression type***	***Ref.***
Huffman coding	*Effective in all file formats*	*All formats*	*Entropy based*	*Lossless*	[81][76]
Arithmetic coding	Flexibility	Multimedia applications	Entropy based	Lossy and Lossless	[82]
LZ coding	*Compress all kinds of data*	*Image and video*	*Dictionary based coding*	*Lossless*	[83]
Fractal compression	*Suitable for textures and natural images*	*Live video*	*Block based coding*	*Lossy*	[84]
BWT	*No need to store additional data for compression*	*Zip files*	*Block sorting compression*	*Lossless*	[85]
RLE	Faster	PDF and Fax	Employs in high redundant data	Lossless	[86]

2. Chapter Two

Related works

This chapter discusses the most recent related research. After studying these research, we categorized them into two groups. The first group is the Lightweight cryptography. the second group discusses AES compatible with LWC requirements that is related to the thesis work

2.1 Lightweight cryptography related works

This section summarizes some research that introduces the concept of LWC in terms of terminology, requirements, and how to implement them in line with the available capabilities. Table (5) summarizes these studies.

Table 5: LWC related works summary

Ref.	***Year***	***Key points and focus***
[87]	2018	• *"A study of the security threats facing the Internet of Things (IoT) underscores the importance of exercising caution and following best practices in the creation of lightweight cryptography (LWC) solutions".*
[88]	*2018*	• *"The security risks associated with the IoT emphasize the need for a cautious approach and implementation of effective methods when designing lightweight cryptography (LWC) solutions".*
[69]	*2019*	• *" Discuss some encryption techniques that can be used in IoT".* • *" Discuss AES algorithm".*
[90]	2019	• *" Discuss the future of LWC and its challenges".*
[91]	2020	• *"A review of several LWC algorithms discovered that many of them did not perform optimally and did not meet the necessary requirements. The study recommends the usage of the AES algorithm for its robustness, but with proper adjustments for improved performance".*
[61]	2021	• *"Proposed a novel lightweight block cipher algorithm is presented, which offers a balance of strong security"*
[94]	2020	• *"The proposal involves a hybrid re-encryption approach to create a more lightweight system with reduced computation time on fog nodes and end-user devices"*
[95]	2021	• *"Presents Light IoT, a lightweight and secure communication approach for exchanging data among the devices in a healthcare infrastructure".*

[97]	2020	• *"A new, lightweight genetic algorithm for the secure encryption of patient health data has been proposed"*
[98]	2019	• *"A secure and lightweight authentication scheme for wireless body area networks has been suggested. This scheme has a lower security risk compared to other lightweight authentication methods"*
[99]	2021	• *"A security approach that utilizes a lightweight three-layer encryption, with a focus on the first layer, has been presented. This approach is currently undergoing study and development and aims to address security issues within the model".*
[100]	2019	• *"A proposal has been made for a lightweight anonymous mutual authentication and key agreement scheme for (WBAN). This scheme has the benefits of lower computation cost, energy consumption, and communication cost, as well as a reduced security risk".*
[101]	2021	• *"A hybrid authentication scheme has been presented that combines physiological signals with a lightweight cryptographic method to provide strong security against commonly known attacks".*

Manifavas and others in reference [72] analyzed various lightweight encryption techniques for use in IoT devices, with a focus on streaming encryption. The researchers concluded that symmetric encryption is the most efficient option, but many of the evaluated algorithms were not secure. Out of 31 algorithms, only 6 were deemed secure.

In their work, Buchanan and others in reference [87] stressed the significance of security and privacy in IoT and reviewed current trends in lightweight encryption algorithm development. It also explored alternative approaches to traditional cryptography methods that are appropriate for IoT devices.

Sehrawat et al. in reference [88] conducted a thorough evaluation of various algorithms suitable for IoT implementation through cryptanalysis attacks. It highlighted the popularity of block ciphers in designing Lightweight Cryptography algorithms and provided suggestions for future LWC algorithm development priorities.

Dutta et al. in reference [69], presented encryption methods for IoT by comparing Lightweight Cryptography algorithms that fit IoT device constraints. It concluded that symmetric encryption is the best approach and found that a modified version of AES provides a secure solution that meets IoT device limitations. The study compared various algorithms, including DES, 3DES, Blowfish, and others.

Gunathilake et al. in reference [90] examined the potential uses, implementation methods, and challenges associated with the application of Lightweight Cryptography (LWC). The authors also revisited various algorithms for LWC that were previously addressed in their research and verified the efficacy of the modified Advanced Encryption Standard (AES) algorithm in this area.

Ramadan et al. in reference [91] proposed a Lightweight Cryptography (LWC) algorithm known as LBC-IoT, which is designed to handle 32-bit blocks with a key length of up to 80 bits. The algorithm utilizes the Feistel structure and incorporates power-saving simple operations, like XOR and 4-bit S-boxes.

Khashan in reference [94] Proposed a new approach to secure communication between fog and Internet of Things (IoT) devices, called a Hybrid Re-Encryption Scheme. This results in a lightweight system that requires fewer computational resources on both fog nodes and end-user devices, providing an efficient solution for secure communication between these devices.

M. A. Jan, F. Khan, S. Mastorakis, and others in reference [95] propose A new communication approach called Light IoT was presented as a solution for secure data exchange among devices within healthcare infrastructure. The method comprises of three stages: initialization, pairing, and authentication, which work together to establish secure sessions between the communicating entities, such as wearables, gateways, and a remote server, to guarantee the secure and reliable transmission of data.

(T. Jabeen, H. Ashraf, A. Khatoon, and others) in reference [97] proposed a new Lightweight Genetic-based Encryption Algorithm (LGBC) for safeguarding patient health data. The proposed algorithm is based on genetic principles and boasts a lower computational time complexity, making it cost-effective for the intended use case.

(Z. Xu, C. Xu and others) in [98] A secure and efficient authentication proposal was put for Wireless Body Area Networks (WBANs). The study demonstrated through practical experiments and theoretical analysis that the proposed scheme considerably lowers the computational overhead when compared to others that use asymmetric encryption, while concurrently exhibiting a lower security vulnerability when compared to other lightweight methods.

(M. Morales-Sandoval and others) in reference [99] presented a security approach that is based on a three-layer Lightweight Encryption with a primary emphasis on the first layer. This approach is still being studied and developed, with the goal of addressing security concerns in the model.

Z. Xu, C. Xu, H. Chen, and F. Yang, in reference [100] put forth a proposed lightweight anonymous mutual authentication and key agreement scheme for WBAN. The scheme is based on the use of hash function operations and XOR operations. The results of the study suggest that the proposed scheme offers a balance of lower computation cost, energy consumption, and communication cost, compared to the schemes that have less security risk.

J. Kaur, S. Garg, in reference [104], Kaur, Jasleen Garg, and Sushil proposed a lightweight, privacy-preserving anonymous mutual user authentication protocol for Industrial Wireless Sensor Networks (IWSN) that ensures that only authorized users with trusted devices can access the network. The proposed protocol focuses on the security of the physical layer in order to safeguard the sensors, even in scenarios where the sensor nodes may be compromised by an attacker. The

protocol uses lightweight encoding alternatives such as a one-way cryptographic hash function, a Physically Unclonable Function (PUF), and bitwise exclusive (XOR) operations to achieve this.

Z. U. Rehman and others in reference [101] proposed an anonymous, hybrid authentication scheme that uses physiological signals in combination with a lightweight cryptographic method to provide robust security against known attacks, particularly key escrow. The scheme was compared to other similar works, and the results of the analysis showed that the proposed scheme provides better security while also keeping computational, energy consumption, and storage overheads low.

2.2 AES Related works

In this section, we summarize some research that presents some AES-based systems, discuss these systems and highlight the differences in these AES, Table (6) summarizes these studies.

(Javed et al. in) reference [105], introduced a new design for the Advanced Encryption Standard (AES) algorithm with the aim of making it more suitable for use on mobile devices. This redesign was intended to improve the performance of AES, despite the limitations of the hardware specifications on such devices. The authors of the study first reviewed the mechanism of the standard AES algorithm before proposing their new design.

In the study [106] conducted by (Mamoun et al), a detailed examination of the AES algorithm was presented. A new model for AES was proposed, which aimed to enhance its security by incorporating an XOR operation on an additional byte of the s-box and using an additional random key. The findings revealed that this modification contributed to a varying

improvement in the level of AES security, as a result of the added random key. Additionally, it was observed that the modification improved confusion and enhanced time security.

In the study [108] conducted by (Daoud et al), the authors presented an optimization of the Advanced Encryption Standard (AES) algorithm using Vivado High-Level Synthesis (HLS) techniques, and their findings demonstrated a notable advancement in the throughput of the proposed algorithm.

(Salim et al). in reference [112] presented the development of a modified AES algorithm called multi-key AES. This proposal utilizes the AES algorithm but employs multiple keys, with the secret key used to configure a variable number of keys via Elliptic Curve Cryptography (ECC). The study specifically focused on implementing this algorithm in the IoT, on devices that possess the capability to run this algorithm. The findings indicate that this modification did not negatively affect the algorithm's performance, and instead contributed to enhancing its security.

In their study, [113] S. Das and S. Namasudra and others proposes an efficient hybrid cryptosystem by combining the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) to accelerate data encryption and secure the symmetric key. The authors employed a matrix multiplication of the AES mix-columns with the s-box, followed by the incorporation of a hardware architecture based on scalar multiplication-based ECC to optimize the cryptosystem. However, this approach does not provide a guarantee of data integrity, which can be assured through the use of a digital signature algorithm.

(Chanal and Kakkasageri) in reference [114] proposed a hybrid cryptosystem that integrates ECC, AES, and the Message Digest algorithm (MD5) to ensure data confidentiality in an IoT environment. This scheme follows a three-phase encryption process that utilizes a geo-tag between the source and destination nodes and also comprises key generation algorithm that optimizes key sizes for the encryption and decryption processes.

(Hakeem and fouad) in reference [115] proposed a hybrid encryption technique that combines AES and a Fully Holomorphic algorithm to encrypt data in the cloud, reducing file size and boosting data security and stack piling.

(Lastly Prosanta Gope et al), in reference [116] discussed the design of a hybrid algorithm to address data security issues in the hospital cloud database. The AES algorithm was improved to create the P-AES algorithm, which was then combined with the RSA algorithm to create a hybrid algorithm. The experimental results showed that the hybrid encryption algorithm had fast encryption and decryption speed, high security, good processing ability for longer data, and was able to effectively address data security issues in the cloud database.

In [117], a modified version of AES was proposed specifically tailored for image encryption and decryption, taking into account the unique characteristics of images. This modified version replaced the MixColumns transformation in the conventional AES with bit permutation. Through analysis of the computed pixel change rate and unified average change intensity, it was observed that the modified AES exhibited heightened sensitivity to differential attacks. The authors in [118] discussed various attacks that have targeted the strength of AES. Among these is the fault injection attack, which can potentially expose the AES key. To mitigate this vulnerability, the authors suggested randomizing the key generation process of AES, resulting in an increased avalanche effect in the modified AES. in [119], it was hypothesized that increasing the number of rounds in AES could enhance the algorithm's security. This hypothesis was verified by increasing the rounds from 10 to 16, and the results demonstrated that the modified AES indeed necessitated more computational time compared to the conventional AES. Efforts were also made to reduce the complexity path of AES in [120]. In [121], dynamic S-box values and initial secret keys required for encryption and decryption were generated. Since the initial secret keys were internally generated, deducing the seed value by an attacker became challenging. As a result, the

modified AES algorithm proved to be resistant to brute force attacks. Additionally, this modified AES algorithm exhibited high encryption quality, an avalanche effect of 60%, a throughput of 3.039 Gbps, and a latency of 10 clock cycles.

Table 6: AES related works summary

Ref.	***Year***	***Key points and focus***
[105]	*2019*	• *"Presented a new design for the AES algorithm"*
[122]	*2019*	• *"An enhanced version of AES was presented with several improvements.* • *"The combinational logic and number of records were reduced by optimizing the data path. The use of a clock gateway strategy, efficient key expansion, and minimizing data activities helped to reduce the energy consumption of the algorithm".*
[106]	*2017*	• *A new model for the AES algorithm was presented to increase its security level by incorporating an XOR operation with an additional byte of the s-box.*
[108]	2019	• *"Present an optimization of the AES algorithm and their results show significant progress in increasing the throughput of the proposed algorithm"*
[112]	2021	• *"Presented the development of an AES algorithm called multi-key AES".* • *"Specialized in implementing this algorithm in the IoT, provided that it is used on devices capable of running this algorithm".* • *"Did not affect the algorithm's performance".* • *"contributed to improving its security".*
[113]	2020	• *"Proposed An efficient hybrid cryptosystem has been using AES and ECC. optimizations based on AES and ECC to accelerate data encryption and protect the symmetric key".*
[114]	2022	• *"Proposed a hybrid cryptosystem that combines ECC, AES, and the Message Digest algorithm (MD5) to ensure data confidentiality in the IoT environment".*
[115]	2017	• *"Proposed a hybrid encryption technique that combines AES and a Fully Holomorphic algorithm to encrypt data in the cloud, reducing file size and boosting data security and stack piling".*
[116]	2019	• *"The AES algorithm was enhanced to form the P-AES algorithm, which was then combined with the RSA algorithm to create a hybrid encryption approach. The resulting algorithm provides fast encryption and decryption speed has high security, and offers good processing capability for longer data. It is also effective in addressing data security concerns in cloud databases".*

3. Chapter three

Methodology

3.1 Proposed modifications

In this section, a hybrid encryption algorithm is introduced. the methodology that has been used in this study is also explained. We have proposed new modifications to the AES algorithm and merging the algorithm with the compression algorithm (Hoffman coding) These will be presentation in the following sections.

Five encryption rounds will be added to the algorithm instead of ten rounds in order to increase the efficiency and effectiveness of the algorithm, and the level of security will be compensated in the next phase. These proposed modifications aim to make AES itself lightweight and to reduce AES runtime with acceptable cryptographic complexity and strength.

The (Hoffmann code) algorithm added after the fifth round in order to compress the result.

3.2 Proposed Methodology

In the section related to experiments and results, a Raspberry Pi was used in the experiment process, and the methodology was to conduct experiments that were conducted on the original algorithm by using scripts of different sizes to calculate the execution time of the encryption and decryption process, and to perform the same process on the proposed algorithm, and the C programming language was used.

3.3 Experiments Methodology

For Encryption: 100 experiments conducted on texts of different sizes, and each experiment be divided into 10 rounds using the algorithm (AES) before modification and proposed algorithm, then calculating the average execution time in milliseconds. For Decryption: 100 experiments are conducted on different texts that are identical to the previous test and divided into 10 rounds using the algorithm (AES) before modification and proposed algorithm, then the average execution time is calculated in milliseconds. Execution time (in milliseconds) for encryption/decryption is calculated, 100 experiments are conducted on different texts that are identical to the previous test and are divided into 10 rounds using the algorithm (AES) before modification and proposed algorithm.

Security Analysis:

1- Avalanche effect: Execute the encoding process and then change the amount of one character or flip a character or change it and then write the result on the ciphertext and compare it with the result before the change
2- Key sensitive attack: Execute the encoding process and then change the amount of one character or flip a character or change it in the master key and then write the result on the ciphertext and compare it with the result before the change

The key sensitivity is a crucial aspect of encryption, as it is used to determine the level of security provided by the key. During the decryption process, the sensitivity of the key is carefully evaluated in order to ensure that even the slightest alteration to the key results in vastly different outcomes, rendering it impossible for an attacker to predict the correct key and subsequently, decrypt the message.

4. Chapter four

Result

In this section, the implementation of modified AES and traditional AES algorithms are evaluated and the results, as previously raised, from testing and application will be discussed. Performance metrics of interest are execution time (for encoding and decoding) and crash impact. The avalanche effect is a highly desirable property of block ciphers, as it indicates that a single bit change in the input results in at least a 50% change in the output. Key sensitive attack: Execute the encoding process and then change the amount of one character or flip a character or change it in the master key and then write the result on the ciphertext and compare it with the result before the change Execution time, meanwhile, refers to the amount of time required for the algorithm to encrypt or decrypt a given input. and protection level, test results will be shown in the following.

4.1 Execution Time

Execution time is a time required to convert plaintext to ciphertext (encryption time) the time required to convert ciphertext to plaintext (decryption time). It is expected that the encoding time and decoding time are small in milliseconds to obtain a responsive and lightweight system. They must be very fast and must be That the in real time due to the importance of time in patients' lives and that parts of a second may save a patient's life from death, the result shown the proposed algorithm outperformed the traditional algorithm in coding time, in all rounds and tests, as the This is an indication that the proposed algorithm can be effective in the IoT environment, since it has proven to be fast and executable in this environment. This intersects with what has been reported in the literature as the encryption process has responded to the lightweight encryption standards.

Table (7) and Fig. (14) present the performance of the proposed algorithm in terms of the execution time for both of encryption and decryption processes. A decrease of 18.75% has been noted compared to the typical AES algorithm. Additionally, the data indicates a positive relationship between the text size and the enhanced speed of the proposed algorithm in executing encryption and decryption. Furthermore, it can be noted that the larger the text size, the more efficient the performance of the proposed algorithm becomes in terms of execution time.

Table 7. Executing Time to Different Files in millisecond (Encryption/Decryption)

Test Number	Text Size	AES	Proposed Algorithm	Differences %
Test (1)	1Byte	24.01	19.22	19.95
Test (2)	2Byte	24.58	19.55	20.46
Test (3)	3Byte	25.25	20.43	19.09
Test (4)	4Byte	26.39	23.29	11.75
Test (5)	6Byte	29.55	26.22	11.27
Test (6)	8Byte	33.81	26.46	21.74
Test (7)	10Byte	34.44	27.18	21.08
Test (8)	12Byte	35.18	28.74	18.31
Test (9)	14Byte	37.22	29.55	20.61
Test (10)	16Byte	38	29.15	23.29
Average differences %				**18.75**

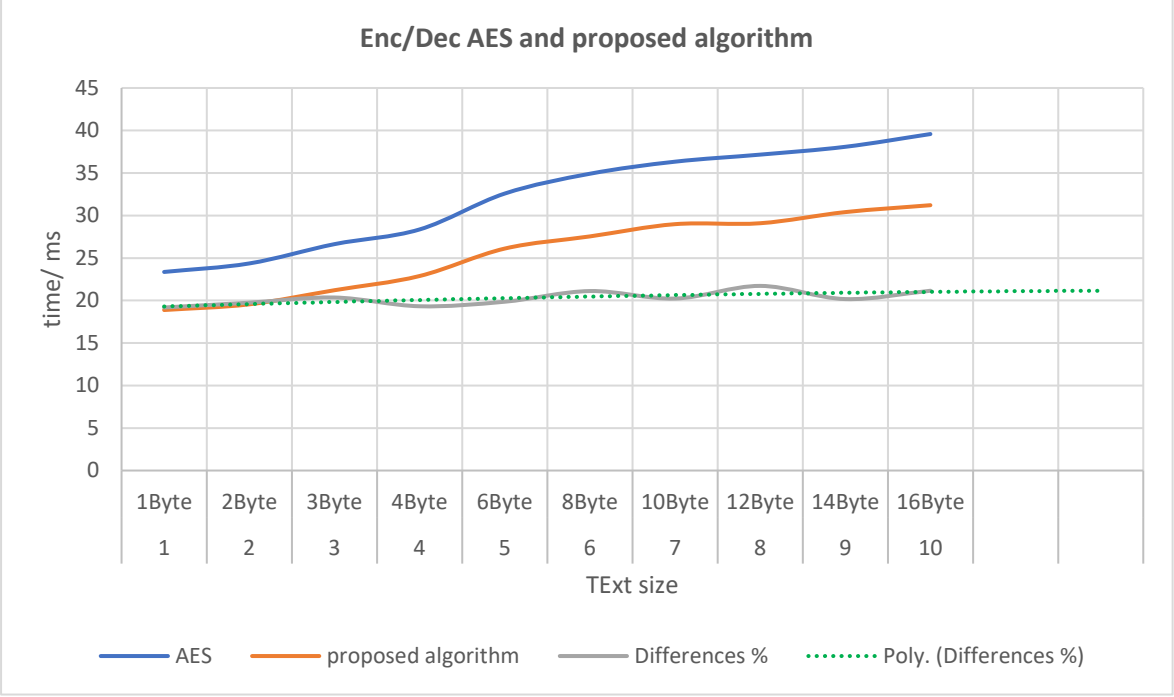


Fig.14: Enc/Dec AES and proposed algorithm

We note that there is a difference in the encryption and Decryption time between the two algorithms in general in all test rounds, The rate of decline at the time is 18.75%. The findings of Test 1, demonstrate that the Enc/Dec process for a 1-byte text using the AES algorithm takes 24.01 milliseconds, while the proposed algorithm performed better with a result of 19.22 milliseconds, a difference of 4.79 milliseconds. In Test 10, where the text size was 16 bytes, the AES algorithm took 38 milliseconds, while the proposed algorithm had a faster result of 29.15 milliseconds, a difference of 8.85 milliseconds. It can be inferred that as the text size increases, the efficiency of the proposed algorithm in encoding and decoding becomes more pronounced.

Table 8. the Encryption Time to Different Files in milliseconds (Encryption)

Test Number	Text Size	AES	Proposed Algorithm	Difference (drop in speed) %
Test (1)	1Byte	13.49	10.59	21.50
Test (2)	2Byte	14.28	11.15	21.92
Test (3)	3Byte	14.88	12.18	18.15
Test (4)	4Byte	15.87	12.88	18.84
Test (5)	6Byte	17.55	14.11	19.60
Test (6)	8Byte	18.67	15.1	19.12
Test (7)	10Byte	19.55	16.12	17.54
Test (8)	12Byte	20.22	16.01	20.82
Test (9)	14Byte	20.67	15.89	23.13
Test (10)	16Byte	21.1	15.92	24.55
Average differences %				20.52

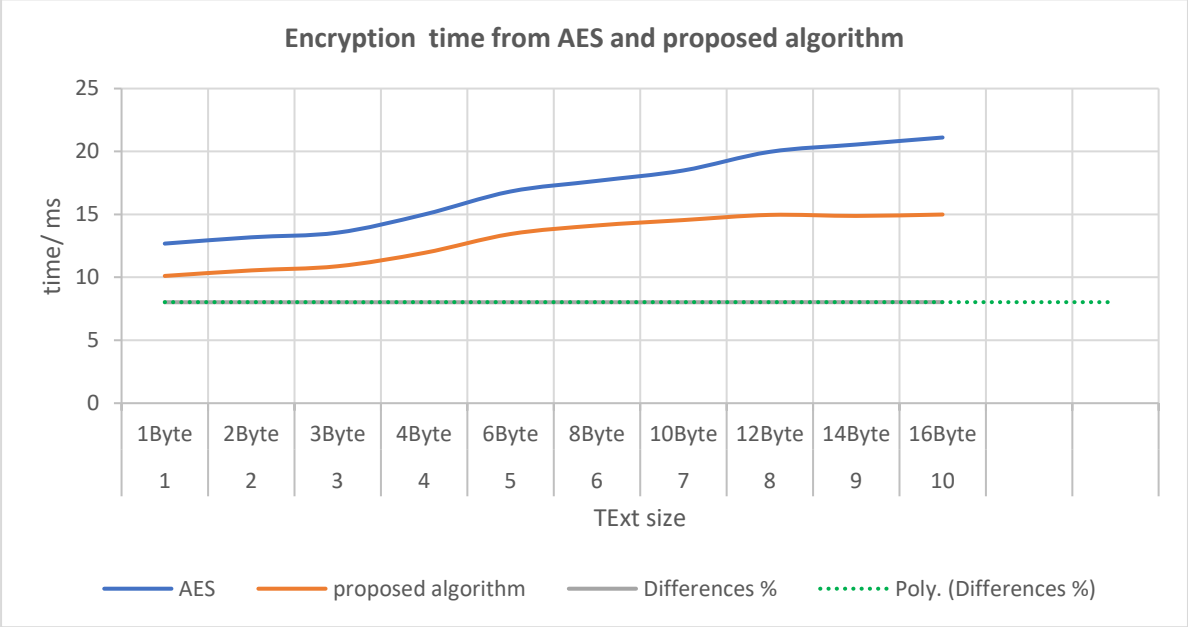


Fig.15: Encryption Test from AES and proposed algorithm

Table (8) and Fig. (15) demonstrate the encryption process for ten rounds of text with different sizes for both the typical AES and proposed algorithms. The results indicate that the proposed algorithm has better performance, with a 20.52% reduction in time compared to the typical AES algorithm. The correlation between text size and efficiency was also shown, with larger texts resulting in a more efficient algorithm. Test 1 showed a difference of 2.90 milliseconds in favor of the proposed algorithm for a 1-byte text, and Test 10 showed a difference of 5.18 milliseconds for a 16-byte text. This indicates that the longer the text, the better the encryption performance and efficiency. The proposed algorithm results in faster encryption and reduced execution time.

Table 9. Decryption Time to Different Files in milliseconds (Decryption)

Test Number	Text Size	AES	Proposed Algorithm	Difference (Drop in speed) %
Test (1)	1Byte	12.55	11.15	11.16
Test (2)	2Byte	12.62	11.22	11.09
Test (3)	3Byte	13.15	11.89	9.58
Test (4)	4Byte	13.66	12.22	10.54
Test (5)	6Byte	14.76	13.34	9.62
Test (6)	8Byte	15.55	13.88	10.74
Test (7)	10Byte	15.89	14.15	10.95
Test (8)	12Byte	16.15	14.55	9.91
Test (9)	14Byte	16.55	14.87	10.15
Test (10)	16Byte	16.87	15.22	9.78
Average differences %				10.35

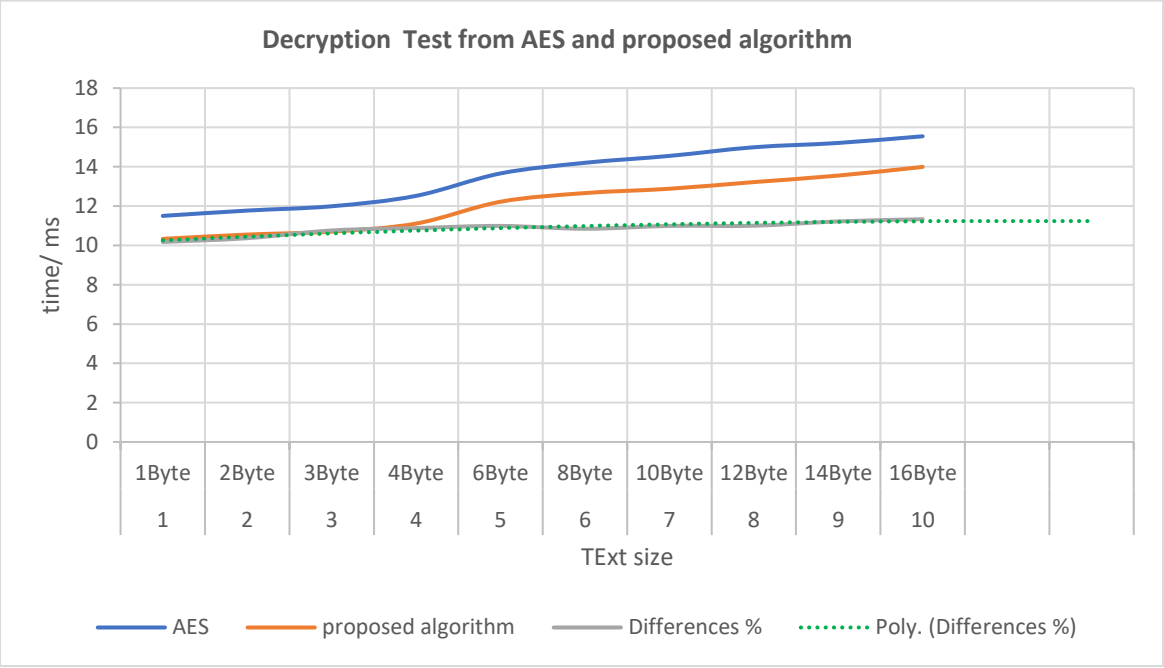


Fig16: Decryption Test from AES and proposed algorithm

Table (9) and Fig. (16) show the result of the decryption tests of 10 rounds using both the typical AES algorithm and the proposed one, with different text sizes. The proposed algorithm

slightly outperforms AES, with a decrease of 10.35% in time while keeping almost the same efficiency. The decryption performance was consistent for both small and big texts. In Test 1, the proposed algorithm had a 1.4 MS improvement for a 1-byte text and in Test 10, it had a 1.65 MS improvement for a 16-byte text. These results indicate no correlation between text length and decryption efficiency and both algorithms perform similarly in the decryption process.

4.2 Security analysis

1- Avalanche effect

only one character is shifted in the following text encryption “mohammad shadeed” where the character “m” was shifted “mohamadm shadeed” and the key used is “hdehcetoepmbxedt” and the result was a significant change in the result as shown in Table (10)

The Avalanche Effect refers to the fact that for a good cipher, changes in the plaintext affect the ciphertext. The algorithm produces a completely different output for a minimally changed input. Avalanche Effect= (Number of Changed chars in ciphertext) / (Number of chars in ciphertext). A good cipher should always satisfy an avalanche > 50%.

Upon evaluating the outcome, it was found that the proposed algorithm produced an avalanche effect of 53.54%, as opposed to the 51.56% achieved by the conventional AES algorithm. This demonstrates that a greater percentage of bits comprising the ciphertext underwent alteration when one bit of the plaintext was altered during encryption using the proposed algorithm, specifically, there is a convergence in the result between the two algorithms.

Table10: Avalanche Effect

Name	Text	Secret key	Cipher text	Avalanche Effect
AES	mohammad shadeed	hdehcetoepmbxedt	01110000100001100110110001111101011010111 00100001100101011100101110100110111110111 01100101011100111001100110100011101000011 11011111110100100110110111000100010101000 01110111111011011110110011100100010001010 00100100001100010111110101111100001001010 0001001000	51.56%
	mohamadm shadeed	hdehcetoepmbxedt	10101111110000011011010111001010101000010 00100101011110001111011010100000000001110 01111100100011001000101100101110011011000 01101111110100100110110111000100010101000 01110111111011011110110011100100010001010 00100100001100010111110101111100001001010 0001001000	
	aes encryption aes	dhgiwevgesomvgys	10111110100100000011001101000101011100101 11100111110010011001100000001010100101111 01100011000101110001111010100010111000110 01100000101111100000010011111001000000101 10101000010000100000110010110011011001111 10101111111101000101100100001010011110101 0111000011	
	aes encroption aes	dhgiwevgesomvgys	10101001100011011000011100011001011101011 01000010101111000111000101010001101001001 11101010010011011001000110100001100000010 00010000101111100000010011111001000000101 10101000010000100000110010110011011001111 10101111111101000101100100001010011110101 0111000011	

	programming test	progrtestingmode	1011101010100110011001111101100001011100 1 01011010010010011111010001101010100111010 00110100001011011110011010001110110011101 00100011000101001000010000101011011110000 10110011100010100011110111000011100110111 01100110010000100101100001010001110010111 1010011010	
	progranming test	progrtestingmode	01001000010001100010010010000100000001011 10110110011111000011010110100001111000000 11111110011100000110000101011110011101001 00000011000101001000010000101011011110000 10110011100010100011110111000011100110111 01100110010000100101100001010001110010111 1010011010	
Proposed Algorithm	mohamadm shadeed	hdehcetoepmbxedt	1001100001001011100100000000011010011111110011 0001110111100100111001110110011000101111101010 10010111011000101101101110110111111	53.54%
	mohamadm shadeed	hdehcetoepmbxedt	01101000010000001101101111011011010101111 00010001001001111000011001111111101101010 1101111111100001011101101001110010	
	aes encryption aes	dhgiwevgesomvgys	00010101001111100100100111111110111001010 00001010100111101101110111001100010001001 11011111110101111110001000001110110	
	aes encroption aes	dhgiwevgesomvgys	10000011110101111101011000011010101100011 00101101110111111100111101011001101100000 011100101000011110011011001001100	
	programming test	progrtestingmode	111100001001100110101110110111000101100011 11011000010101110001110000101101011011111 0111110101100100011111101100010	
	progranming test	progrtestingmode	10011111000101011011001111100001010000011 10101011111011101011100000001011000110110 110011101100011111010111101000101111100000 1101001	

2- Key sensitive attack

This is achieved by testing the algorithm, where during the decryption process one letter is changed and then the result is observed. The results showed in Table (11) that after changing one letter (last one) in the key “hdehcetoepmbxedt” to “hdehcetoepmbxed1” The results showed

significant changes in the results and this confirms the safety of the algorithm from where the sensitivity of the key and it is difficult to predict the key, so it is difficult to decrypt the algorithm.

this is one of the most important tests security of lightweight encryption algorithms, In comparison with the AES algorithm, the output showed convergence in the result of the key sensitivity attack between the result of the proposed algorithm and the result of the AES algorithm, as changing one letter in the key leads to different results, a complete difference in the text after decryption.

The results show the proposed algorithm is resistant to decryption attacks as evidenced by the Avalanche effect test. Additionally, the key sensitive attach test conducted in the evaluation phase confirmed the system's immunity to key-related attacks.

Table11: Key sensitive attack

Name	Text	Secret key	Cipher text	Key sensitive attack %
AES	mohammad shadeed mohammad shadeed	hdehcetoepmbxedt hdehcetoepmbxed1	0111000010000110011011000111110101101011100100001100101011100101110100110111110111011001010110011100111001100110100011101000011110111111101001001101101110001000101010000111011111101101111011001110010001000101000100100001100010111110101111100001001010000100 1001010100001001101101110100000101001010100100010000011110110110001101011011110101001110110100111111111001010101010110000000000100010110010010110111111011010100010110100011000101111011110101111011010001101100001101001000110110010001001111010001111100000010001110111	99%

	aes encryption	dhgiwevgesomvgys	1011111010010000001100110100010101110010111110011 1110010011001100000000101010010111101100011000101 1100011110101000101110001100110000010111110000000 1001111100100000010110101000010000100000011001011 0011011001111101011111111010001011001000010100111 101010111000011	99%
	aes encryption	dhgiwe5gesomvgys	1011101111011010111110111111000111001100110101101 1111100011111101101100011000001001010100111100001 1001110011110110111101000010100100001001100111101 1100010011011100100100011010111111110101101010000 0011000011001001101010110110100010000101111110101 010110001000000	
	programming test	progrtestingmode	1011101010100110011001111101100001011100101011010 0100100111110100011010101001110100011010000101101 1111001101000111011001110100100011000101001000001 0000101011011111000010110011100010100011110111000 0111001101110110011001000010010110000101000111001 01111010011010	99%
	programming test	progrtesting1ode	1100000101001010101010010110001101010110011100001 0110111111000001111000000111111100000110000000111 1010010011100111111011101111011101101101010011011 1111110111101101111011000101101100111100010110101 1000101000011101011111110100111000111101100001 010101001100100	
Proposed Algorithm	mohammad shadeed	hdehcetoepmbxed1	1110000110110010101101001111101110100111100011111 1000110011100111101011000111000001010010000010111 001111111000101100	99%
	mohammad shadeed	hdehcetoepmbxedt	0111010000011000110111000101101111010111100010001 0010011110000110100011111111010101100110111110010 1110110100111001	
	aes encryption	dhgiwevgesomvgys	0101100101111111110011011001111011011011010100011 1100001100100111000101010101000100111010011011111 0000010000111111	99%
	aes encryption	dhgiwe5gesomvgys	1001001111011100010000010011101110111110100011000 0111110001001100101111011011000110100101111000101 0000110101101010 1111	

	programming test	progrtestingmode	01000001011101111001111100010100110100111101110110110010001110101011011000111000011100101110001101	99%
	programming test	progrtesting1ode	01101100100110110011001110011110100111011110000001111100011010000100001010100110010110011011101011110010111111110010	

Discussion

The outcomes were compared to the research conducted by [74]. The encryption execution time for a 16-byte text was 16.58 milliseconds, whereas our study execution time of 15.92 milliseconds. In terms of decryption, the [74] study recorded a time of 17.89 milliseconds for a 16-byte text, whereas our study achieved a lower time of 13.99 milliseconds. These findings indicate that the proposed algorithm in our study outperforms the algorithm employed in the referenced studies. Furthermore, upon analyzing the Avalanche Effect test, our study yielded a result of 53.54, whereas [74] study using the main AES algorithm achieved a result of 50.47%, and the modified algorithm in the same study achieved a result of 55.73%. This confirms the validity of our study's findings, as our results closely align with the expected outcome of the examination, which is a result exceeding 50%, indicating a substantial alteration of the encrypted text by merely changing one character prior to encryption.

The results obtained in our study were compared to the research conducted by [123]. For the encryption process of a 16-byte text, [123] reported an execution time of 1.925 seconds, while our study achieved a significantly lower execution time of 15.92 milliseconds. Similarly, in terms of decryption, [123] recorded a time of 1.874 seconds for a 16-byte text, whereas our study achieved a faster decryption time of 15.22 milliseconds. Furthermore, when analyzing the key sensitive attack test, our study yielded a result of 99%, indicating a high level of resistance against such attacks. In contrast, [123] reported a slightly higher result of 99.56%.

5. Chapter Five

Conclusions and Recommendations

The study is demonstrated that the proposed algorithm can serve as an efficient and secure alternative to the typical (AES) when it comes to protecting sensitive data and information in devices that have limited resources. After incorporating data compression code after encryption in the proposed algorithm, the algorithm becomes highly resistant to attacks and requires a significant amount of time and computational power to break. Furthermore, the proposed algorithm shown to be faster than typical AES, making it an ideal solution for devices that prioritize speed consumption. The results of the study indicate that the proposed algorithm not only improves security but also reduces execution time compared to AES.

The study found that the proposed improved algorithm is effective, efficient, and faster than the AES algorithm in both encoding and decoding processes. The improvement in speed was 18.75% when combining encoding and decoding and 20.52% when it comes to encryption specifically. In decoding, the improvement was estimated to be 10.35% in favor of the proposed algorithm.

The study revealed a correlation between the size of the text and speed, with the proposed algorithm performing better and faster with larger texts and at a fast rate compared to the AES algorithm.

The results of the security evaluation showed that the proposed algorithm is resistant to decryption attacks, as evidenced by the results of the avalanche effect test 51.56 for typical AES, and 53.54 for proposed algorithm. The immunity of the proposed algorithm from key-related attacks was also confirmed by the key sensitive attack conducted during the evaluation phase, it

can be said that after testing the proposed algorithm, it was found that it is close in its results security features and overall, in protecting sensitive information. close and similar to the AES algorithm.

The use of Huffman coding in the final step of the data compression process after encryption has improved the security of the algorithm. This is because it makes it much harder to decrypt the information. The encryption and decryption process consists of two stages. First, the text is encrypted using modifications in the proposed algorithm, producing an encrypted output. Then, the encrypted output is compressed and encoded again using Huffman coding, resulting in a more secure representation, represented as a sequence of binary digits and a corresponding Huffman tree.

Additionally, further studies can be conducted to evaluate the scalability and adaptability of the proposed algorithm in different scenarios and environments, such as cloud computing. This will help determine its robustness and feasibility of implementation in real-world applications. Additionally, it can be tested against a wider range of attacks and different types of data, such as text, images, audio, and video, to evaluate its overall effectiveness in securing sensitive information. Ultimately, the goal is to continue to improve and refine the proposed algorithm to make it an even more efficient and secure solution for protecting sensitive data and information in devices with limited resources, and calculate computational cost (RAM, CPU, Power).

In future research, the proposed algorithm will be evaluated and compared against other test methods to determine its effectiveness in terms of both implementation and security performance. Furthermore, we plan to investigate the applicability of this algorithm to other types of data, such as images, audio and video, in future studies. This will aid in the development and advancement of the algorithm.

References

[1] S. Grabowska and S. Saniuk, “Business Models in the Industry 4.0 Environment—Results of Web of Science Bibliometric Analysis,” *J. Open Innov. Technol. Mark. Complex.*, vol. 8, no. 1, 2022, doi: 10.3390/joitmc8010019.

[2] J. Xu, B. Gu, and G. Tian, “Review of agricultural IoT technology,” *Artif. Intell. Agric.*, vol. 6, pp. 10–22, 2022, doi: 10.1016/j.aiia.2022.01.001.

[3] A. Abdelmaboud *et al.*, “Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions,” *Electron.*, vol. 11, no. 4, pp. 1–35, 2022, doi: 10.3390/electronics11040630.

[4] A. Alamoudi, A. Celik, and A. M. Eltawil, “Cooperative Body Channel Communications for Energy Efficient Internet of Bodies,” 2022, doi: 10.1109/JIOT.2022.3230719.

[5] H. Fouad, H. Kamel, and A. Youssef, “Voltage-Booster for CMOS Wide-Band High-Precision Rectifier of Energy Harvesting for Implantable Medical Devices in Internet of Bodies (IOB) Telemedicine Embedded System,” *Int. J. Electr. Electron. Eng.*, vol. 9, no. 4, pp. 19–30, 2022, doi: 10.14445/23488379/ijeee-v9i4p103.

[6] A. Mohiyuddin, A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, “Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System,” *Int. J. Fuzzy Syst.*, vol. 24, no. 2, pp. 1203–1215, 2022, doi: 10.1007/s40815-021-01104-y.

[7] M. Yaghoubi, K. Ahmed, and Y. Miao, “Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges,” *J. Sens. Actuator Networks*, vol. 11, no. 4, p. 67, 2022, doi: 10.3390/jsan11040067.

[8] “https://blog.isa.org/what-is-industry-40,” [Online]. Available: https://blog.isa.org/what-is-industry-40.

[9] L. S. Dalenogare, G. B. Benitez, N. F. Ayala, and A. G. Frank, “The expected contribution of Industry 4.0 technologies for industrial performance,” *Int. J. Prod. Econ.*, vol. 204, no. August, pp. 383–394, 2018, doi: 10.1016/j.ijpe.2018.08.019.

[10] T. R. Wanasinghe, R. G. Gosine, L. A. James, G. K. I. Mann, O. De Silva, and P. J. Warrian, “The Internet of Things in the Oil and Gas Industry: A Systematic Review,” *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8654–8673, 2020, doi: 10.1109/JIOT.2020.2995617.

[11] G. Aloi *et al.*, “Enabling IoT interoperability through opportunistic smartphone-based mobile gateways,” *J. Netw. Comput. Appl.*, vol. 81, no. September, pp. 74–84, 2017, doi: 10.1016/j.jnca.2016.10.013.

[12] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, 2019, doi: 10.1109/JIOT.2018.2847733.

[13] M. M. Gaber *et al.*, “Internet of Things and data mining: From applications to techniques and systems,” *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 9, no. 3, pp. 1–50, 2019, doi: 10.1002/widm.1292.

[14] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014, doi: 10.1109/TII.2014.2300753.

[15] C. A. da Costa, C. F. Pasluosta, B. Eskofier, D. B. da Silva, and R. da Rosa Righi, “Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards,” *Artif. Intell. Med.*, vol. 89, no. May, pp. 61–69, 2018, doi: 10.1016/j.artmed.2018.05.005.

[16] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, “A Review on Internet of Things for Defense and Public Safety,” *Sensors (Basel).*, vol. 16, no. 10, pp. 1–44, 2016, doi: 10.3390/s16101644.

[17] A. Ometov, S. V. Bezzateev, J. Kannisto, J. Harju, S. Andreev, and Y. Koucheryavy, “Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things,” *IEEE Internet Things J.*, vol. 4, no. 4, pp. 843–854, 2017, doi: 10.1109/JIOT.2016.2593898.

[18] A. Celik, N. Saeed, B. Shihada, T. Y. Al-Naffouri, and M. S. Alouini, “A Software-Defined Opto-Acoustic Network Architecture for Internet of Underwater Things,” *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 88–94, 2020, doi: 10.1109/MCOM.001.1900593.

[19] N. Saeed, M. S. Alouini, and T. Y. Al-Naffouri, “Toward the Internet of Underground Things: A Systematic Survey,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3443–3466, 2019, doi: 10.1109/COMST.2019.2934365.

[20] I. F. Akyildiz and A. Kak, “The Internet of Space Things/CubeSats: A ubiquitous cyber-physical system for the connected world,” *Comput. Networks*, vol. 150, pp. 134–149, 2019, doi: 10.1016/j.comnet.2018.12.017.

[21] Y. Sahni, J. Cao, S. Zhang, and L. Yang, “Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things,” *IEEE Access*, vol. 5, pp. 16441–16458, 2017, doi: 10.1109/ACCESS.2017.2739804.

[22] W. Zhou *et al.*, “Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms,” *Proc. 28th USENIX Secur. Symp.*, pp. 1133–1150, 2019.

[23] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[24] N. Hossein Motlagh, T. Taleb, and O. Arouk, “Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives,” *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, 2016, doi: 10.1109/JIOT.2016.2612119.

[25] F. Piccialli, S. Cuomo, V. S. di Cola, and G. Casolla, “A machine learning approach for IoT cultural data,” *J. Ambient Intell. Humaniz. Comput.*, no. 0123456789, 2019, doi: 10.1007/s12652-019-01452-6.

[26] A. Akbar *et al.*, “Real-time probabilistic data fusion for large-scale IoT applications,” *IEEE Access*, vol. 6, pp. 10015–10027, 2018, doi: 10.1109/ACCESS.2018.2804623.

[27] M. Marjani *et al.*, “Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges,” *IEEE Access*, vol. 5, pp. 5247–5261, 2017, doi: 10.1109/ACCESS.2017.2689040.

[28] Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, “Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges,” *Wirel. Commun.*

Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/3229294.

[29] S. Ahamad, P. Gupta, P. Bikash Acharjee, K. Padma Kiran, Z. Khan, and M. Faez Hasan, "The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market," *Mater. Today Proc.*, vol. 56, no. xxxx, pp. 2070–2074, 2022, doi: 10.1016/j.matpr.2021.11.405.

[30] S. Hussain, S. S. Ullah, M. Uddin, and J. Iqbal, "A Comprehensive Survey on Signcryption Security," 2022.

[31] S. Singh and D. Prasad, "Wireless body area network (WBAN): A review of schemes and protocols," *Mater. Today Proc.*, vol. 49, no. xxxx, pp. 3488–3496, 2020, doi: 10.1016/j.matpr.2021.05.564.

[32] S. Nepal, S. Dahal, and S. Shin, "Does the IEEE 802.15.4 MAC Protocol Work Well in Wireless Body Area Networks?," *J. Adv. Comput. Networks*, vol. 4, no. 1, pp. 52–58, 2016, doi: 10.18178/jacn.2016.4.1.203.

[33] R. Singla, N. Kaur, D. Koundal, and A. Bharadwaj, *Challenges and Developments in Secure Routing Protocols for Healthcare in WBAN: A Comparative Analysis*, vol. 122, no. 2. Springer US, 2022.

[34] M. 2020. yousra abdul alsahib s.aldeen and K. N. Qureshi, "Solutions and Recent Challenges Related to Energy in Wireless Body Area Networks with Integrated Technologies: Applications and Perspectives", Baghdad Sci.J, vol. 17, no. 1(Suppl.), p. 0378, "yousra abdul alsahib s.aldeen and K. N. Qureshi, 'Solutions and Recent Challenges Related to Energy in Wireless Body Area Networks with Integrated Technologies: Applications and Perspectives', Baghdad Sci.J, vol. 17, no. 1(Suppl.), p. 0378, Mar. 2020."

[35] M. M. M. Sandhu, "Mobility Modeling for Efficient Data Routing in Wireless Body Area Networks," 2014.

[36] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, "A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks," *IEEE Access*, vol. 8, pp. 131397–131413, 2020, doi: 10.1109/ACCESS.2020.3007405.

[37] G. Mehmood, M. Z. Khan, M. Fayaz, M. Faisal, H. U. Rahman, and J. Gwak, “An energy-efficient mobile agent-based data aggregation scheme for wireless body area networks,” *Comput. Mater. Contin.*, vol. 70, no. 3, pp. 5929–5948, 2022, doi: 10.32604/cmc.2022.020546.

[38] M. B. Blake, N. Kandasamy, S. Dustdar, and X. Liu, “Internet of Bodies/Internet of Sports,” *IEEE Internet Comput.*, vol. 24, no. 5, pp. 8–9, 2020, doi: 10.1109/MIC.2020.3026924.

[39] A. M. Matwyshyn, “The Internet of Bodies,” *William Mary Law Rev.*, vol. 61, no. 1, pp. 77–168, 2019, [Online]. Available: https://heinonline.org/HOL/Page?handle=hein.journals/wmlr61&id=87&div=6&collection=journals%0Ahttps://papers.ssrn.com/abstract=3452891%0Ahttps://ssrn.com/abstract=3452891.

[40] N. Makitalo *et al.*, “The Internet of Bodies Needs a Human Data Model,” *IEEE Internet Comput.*, vol. 24, no. 5, pp. 28–37, 2020, doi: 10.1109/MIC.2020.3019920.

[41] A. M. Hussain and M. M. Hussain, “CMOS-Technology-Enabled Flexible and Stretchable Electronics for Internet of Everything Applications,” *Adv. Mater.*, vol. 28, no. 22, pp. 4219–4249, 2016, doi: 10.1002/adma.201504236.

[42] E. Iob, P. Frank, A. Steptoe, and D. Fancourt, “Levels of Severity of Depressive Symptoms Among At-Risk Groups in the UK During the COVID-19 Pandemic,” *JAMA Netw. open*, vol. 3, no. 10, p. e2026064, 2020, doi: 10.1001/jamanetworkopen.2020.26064.

[43] A. Celik and A. M. Eltawil, “The Internet of Bodies: The Human Body as an Efficient and Secure Wireless Channel,” *IEEE Internet Things Mag.*, vol. 5, no. 3, pp. 114–120, 2022, doi: 10.1109/iotm.001.2100209.

[44] M. Hernandez and R. Kohno, “Coexistence of UWB-BANs with other wireless systems,” *ISPACS 2009 - 2009 Int. Symp. Intell. Signal Process. Commun. Syst. Proc.*, no. Ispacs, pp. 135–137, 2009, doi: 10.1109/ISPACS.2009.5383884.

[45] M. Simkó and M. O. Mattsson, “5G wireless communication and health effects—A pragmatic review based on available studies regarding 6 to 100 GHz,” *Int. J. Environ. Res. Public Health*, vol. 16, no. 18, pp. 1–23, 2019, doi: 10.3390/ijerph16183406.

[46] F. C. C. Radio Frequency Safety, 2019. [Online]. Available: Washington, DC, USA, and Https://www.fcc.gov/general/radio-frequency-safety-0, “No Title.”

[47] S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, “Iot security challenges: Cloud and blockchain, postquantum cryptography, and evolutionary techniques,” *Electron.*, vol. 10, no. 21, 2021, doi: 10.3390/electronics10212647.

[48] P. Prakasam, M. Madheswaran, K. P. Sujith, and M. S. Sayeed, “Low Latency, Area and Optimal Power Hybrid Lightweight Cryptography Authentication Scheme for Internet of Things Applications,” *Wirel. Pers. Commun.*, vol. 126, no. 1, pp. 351–365, 2022, doi: 10.1007/s11277-022-09748-1.

[49] W. B. Liu *et al.*, “Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum key Distribution with High Excess Noise Tolerance,” *PRX Quantum*, vol. 2, no. 4, p. 1, 2021, doi: 10.1103/PRXQuantum.2.040334.

[50] “No Titlehttps://www.tutorialspoint.com/cryptography/block_cipher.htm#,” [Online]. Available: https://www.tutorialspoint.com/cryptography/block_cipher.htm#.

[51] M. Abutaha, B. Atawneh, L. Hammouri, and G. Kaddoum, “Secure lightweight cryptosystem for IoT and pervasive computing,” *Sci. Rep.*, vol. 12, no. 1, pp. 1–15, 2022, doi: 10.1038/s41598-022-20373-7.

[52] D. J. Bernstein, “The salsa20 family of stream ciphers,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4986 LNCS, pp. 84–97, 2008, doi: 10.1007/978-3-540-68351-3_8.

[53] T. Shi, F. Zhao, H. Hao, and Z. Liu, “Costs, benefits and range: Application of lightweight technology in electric vehicles,” *SAE Tech. Pap.*, vol. 2019-April, no. April, pp. 1–10, 2019, doi: 10.4271/2019-01-0724.

[54] M. Usman, R. Amin, H. Aldabbas, and B. Alouffi, “Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography,” *Electron.*, vol. 11, no. 7, 2022, doi: 10.3390/electronics11071026.

[55] B. Atawneh, L. Al-Hammoury, and M. Abutaha, “Power consumption of a chaos-based stream cipher algorithm,” *ICCAIS 2020 - 3rd Int. Conf. Comput. Appl. Inf. Secur.*, no. March, 2020, doi: 10.1109/ICCAIS48893.2020.9096730.

[56] S. Q. Abd Al-Rahman, O. A. Dawood, and A. M. Sagheer, “A Hybrid Lightweight Cipher Algorithm,” *Int. J. Comput. Digit. Syst.*, vol. 11, no. 1, pp. 463–475, 2022, doi: 10.12785/ijcds/110138.

[57] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[58] H. Madushan, I. Salam, and J. Alawatugoda, “A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses,” *Electron.*, vol. 11, no. 24, pp. 1–21, 2022, doi: 10.3390/electronics11244199.

[59] S. A. Al-rahman, A. M. Sagheer, and O. A. Dawood, “Propose a Lightweight Block Cipher Algorithm for Securing Internet of Things Propose A Lightweight Block Cipher Algorithm For Securing Internet of Things Propuesto De Un Algoritmo De Cifras De Bloque Ligero Para,” no. January 2020, 2019, doi: 10.4206/aus.2019.n26.2.37/.

[60] S. Sivagurunathan and V. M. Ganeshan, “LIGHT WEIGHT CRYPTOGRAPHY (LWC) ALGORITHMS IN TERMS OF SOFTWARE METRICS FOR INDUSTRIAL INTERNET OF THINGS (IIOT),” vol. 22, no. 1, pp. 127–137, 2022.

[61] C. A. Buckner *et al.*, “We are IntechOpen , the world ’ s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %,” *Intech*, vol. 11, no. tourism, p. 13, 2016, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics.

[62] S. Katoch, S. S. Chauhan, and V. Kumar, *A review on genetic algorithm: past, present, and future*, vol. 80, no. 5. Multimedia Tools and Applications, 2021.

[63] C. H. Lin, G. H. Hu, C. Y. Chan, and J. J. Yan, “Chaos-based synchronized dynamic keys and their application to image encryption with an improved aes algorithm,” *Appl. Sci.*, vol. 11, no. 3, pp. 1–16, 2021, doi: 10.3390/app11031329.

[64] Y. G. Selassie, “Chapter 5 Chapter 5 (contd .),” pp. 1–34.

[65] A. Cui, H. Zhao, X. Zhang, B. Zhao, and Z. Li, “Power system real time data encryption system based on des algorithm,” *Proc. - 2021 13th Int. Conf. Meas. Technol.*

Mechatronics Autom. ICMTMA 2021, pp. 220–228, 2021, doi: 10.1109/ICMTMA52658.2021.00056.

[66] R. Sharma and S. Pansare, "Analysis of symmetric key cryptographic algorithms," *Int. Res. J. Eng. Technol.*, vol. 4, no. 2, pp. 1628–1630, 2017, [Online]. Available: https://irjet.net/archives/V4/i2/IRJET-V4I2320.pdf.

[67] M. A. Bahnasawi *et al.*, "ASIC-oriented comparative review of hardware security algorithms for internet of things applications," *Proc. Int. Conf. Microelectron. ICM*, vol. 0, pp. 285–288, 2016, doi: 10.1109/ICM.2016.7847871.

[68] N. El-Meligy, M. Amin, E. Yahya, and Y. Ismail, "130nm Low power asynchronous AES core," *Proc. - IEEE Int. Symp. Circuits Syst.*, 2017, doi: 10.1109/ISCAS.2017.8050832.

[69] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, no. January, pp. 475–481, 2019, doi: 10.1109/CCWC.2019.8666557.

[70] S. Agwa, E. Yahya, and Y. Ismail, "Power efficient AES core for IoT constrained devices implemented in 130nm CMOS," *Proc. - IEEE Int. Symp. Circuits Syst.*, pp. 2–5, 2017, doi: 10.1109/ISCAS.2017.8050361.

[71] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed, and J. J. P. C. Rodrigues, "Speeding Up the Internet of Things: LEAIoT: A Lightweight Encryption Algorithm Toward Low-Latency Communication for the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 7, no. 6, pp. 31–37, 2018, doi: 10.1109/MCE.2018.2851722.

[72] M. A. Philip and V. Vaithiyanathan, "A survey on lightweight ciphers for IoT devices," *Proc. 2017 IEEE Int. Conf. Technol. Adv. Power Energy Explor. Energy Solut. an Intell. Power Grid, TAP Energy 2017*, no. December 2017, pp. 1–4, 2018, doi: 10.1109/TAPENERGY.2017.8397271.

[73] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for IoT devices," *2018 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2018*, pp. 1–8, 2018, doi: 10.1109/LISAT.2018.8378034.

[74] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "SS symmetry for Information Security," pp. 1–16, 2019.

[75] D. O. Vadaviya and P. Tandel, “Study of Avalanche Effect in AES,” *Ncraes’15*, no. June, pp. 183–187, 2015.

[76] U. Jayasankar, V. Thirumal, and D. Ponnurangam, “A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 2, pp. 119–140, 2021, doi: 10.1016/j.jksuci.2018.05.006.

[77] X. Liu, P. An, Y. Chen, and X. Huang, “An improved lossless image compression algorithm based on Huffman coding,” *Multimed. Tools Appl.*, vol. 81, no. 4, pp. 4781–4795, 2022, doi: 10.1007/s11042-021-11017-5.

[78] J. Tian *et al.*, “Revisiting huffman coding: Toward extreme performance on modern GPU architectures,” *Proc. - 2021 IEEE 35th Int. Parallel Distrib. Process. Symp. IPDPS 2021*, pp. 881–891, 2021, doi: 10.1109/IPDPS49936.2021.00097.

[79] A. Kodir, R. Fajar, A. S. Awalluddin, U. Ruswandi, N. Ismail, and D. Miharja, “An entropy analysis of the Cirebon language script using the Ternary Huffman code algorithm,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1098, no. 4, p. 042042, 2021, doi: 10.1088/1757-899x/1098/4/042042.

[80] D. A. Huffman, “A method for the construction of minimum-redundancy codes,” *Resonance*, vol. 11, no. 2, pp. 91–99, 2006, doi: 10.1007/bf02837279.

[81] Y. Y. Tsai, H. L. Liu, P. L. Kuo, and C. S. Chan, “Extending Multi-MSB Prediction and Huffman Coding for Reversible Data Hiding in Encrypted HDR Images,” *IEEE Access*, vol. 10, pp. 49347–49358, 2022, doi: 10.1109/ACCESS.2022.3171578.

[82] G. G. Langdon, “Introduction To Arithmetic Coding.,” *IBM J. Res. Dev.*, vol. 28, no. 2, pp. 135–149, 1984, doi: 10.1147/rd.282.0135.

[83] J. Ziv and A. Lempel, “A Universal Algorithm for Sequential Data Compression,” *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 337–343, 1977, doi: 10.1109/TIT.1977.1055714.

[84] D. Saupe and R. Hamzaoui, “A review of the fractal image compression literature,” *ACM SIGGRAPH Comput. Graph.*, vol. 28, no. 4, pp. 268–276, 1994, doi: 10.1145/193234.193246.

[85] “Burrows, Michael, and David Wheeler. ‘A block-sorting lossless data compression

algorithm.’ Digital SRC Research Report. 1994.,” [Online]. Available: Burrows, Michael, and David Wheeler. %22A block-sorting lossless data compression algorithm.%22 Digital SRC Research Report. 1994.%0A.

[86] M. Hatada, “A Probabilistic Model for Run-Length Coding of Line-Drawings,” *Trans. Inst. Electr. Eng. Japan.C*, vol. 95, no. 12, pp. 277–284, 1975, doi: 10.11526/ieejeiss1972.95.277.

[87] W. J. Buchanan, S. Li, and R. Asif, “Lightweight cryptography methods,” *J. Cyber Secur. Technol.*, vol. 1, no. 3–4, pp. 187–201, 2017, doi: 10.1080/23742917.2017.1384917.

[88] D. Sehrawat and N. S. Gill, “Lightweight Block Ciphers for IoT based applications: A Review,” *Int. J. Appl. Eng. Res.*, vol. 13, no. 5, pp. 2258–2270, 2018, [Online]. Available: http://www.ripublication.com.

[89] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, “A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices,” *Symmetry (Basel).*, vol. 11, no. 2, 2019, doi: 10.3390/sym11020293.

[90] N. A. Gunathilake, W. J. Buchanan, and R. Asif, “Next Generation Lightweight Cryptography for Smart IoT Devices: : Implementation, Challenges and Applications,” *IEEE 5th World Forum Internet Things, WF-IoT 2019 - Conf. Proc.*, pp. 707–710, 2019, doi: 10.1109/WF-IoT.2019.8767250.

[91] M. Abu-Tair *et al.*, “Towards secure and privacy-preserving iot enabled smart home: Architecture and experimental study,” *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–14, 2020, doi: 10.3390/s20216131.

[92] R. A. Ramadan, B. W. Aboshosha, K. Yadav, I. M. Alseadoon, M. J. Kashout, and M. Elhoseny, “LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices,” *Comput. Mater. Contin.*, vol. 67, no. 3, pp. 3563–3579, 2021, doi: 10.32604/cmc.2021.015519.

[93] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, “A new lightweight cryptographic algorithm for enhancing data security in cloud computing,” *Glob. Transitions Proc.*, vol. 2, no. 1, pp. 91–99, 2021, doi: 10.1016/j.gltp.2021.01.013.

[94] O. A. Khashan, “Hybrid Lightweight Proxy Re-Encryption Scheme for Secure Fog-to-Things Environment,” *IEEE Access*, vol. 8, pp. 66878–66887, 2020, doi:

10.1109/ACCESS.2020.2984317.

[95] M. A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar, and N. Stergiou, “LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics,” *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1202–1211, 2021, doi: 10.1109/TGCN.2021.3077318.

[96] A. M. Almuhaideb and K. S. Alqudaihi, “A Lightweight and Secure Anonymity Preserving Protocol for WBAN,” *IEEE Access*, vol. 8, pp. 178183–178194, 2020, doi: 10.1109/ACCESS.2020.3025733.

[97] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, and A. Mosavi, “A lightweight genetic based algorithm for data security in wireless body area networks,” *IEEE Access*, vol. 8, pp. 183460–183469, 2020, doi: 10.1109/ACCESS.2020.3028686.

[98] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, “A lightweight mutual authentication and key agreement scheme for medical internet of things,” *IEEE Access*, vol. 7, pp. 53922–53931, 2019, doi: 10.1109/ACCESS.2019.2912870.

[99] M. Morales-Sandoval, R. De-La-Parra-Aguirre, H. Galeana-Zapien, and A. Galaviz-Mosqueda, “A Three-Tier Approach for Lightweight Data Security of Body Area Networks in E-Health Applications,” *IEEE Access*, vol. 9, pp. 146350–146365, 2021, doi: 10.1109/ACCESS.2021.3123456.

[100] Z. Xu, C. Xu, H. Chen, and F. Yang, “A lightweight anonymous mutual authentication and key agreement scheme for WBAN,” *Concurr. Comput. Pract. Exp.*, vol. 31, no. 14, pp. 1–12, 2019, doi: 10.1002/cpe.5295.

[101] Z. U. Rehman, S. Altaf, S. Ahmad, S. Huda, A. M. Al-Shayea, and S. Iqbal, “An efficient, hybrid authentication using ecg and lightweight cryptographic scheme for wban,” *IEEE Access*, vol. 9, pp. 133809–133819, 2021, doi: 10.1109/ACCESS.2021.3115706.

[102] E. Lara, L. Aguilar, and J. A. Garcia, “Lightweight Authentication Protocol Using Self-Certified Public Keys for Wireless Body Area Networks in Health-Care Applications,” *IEEE Access*, vol. 9, pp. 79196–79213, 2021, doi: 10.1109/ACCESS.2021.3084135.

[103] J. Habibi, H. Mahboubi, and A. G. Aghdam, “Distributed Coverage Control of Mobile

Sensor Networks Subject to Measurement Error," *IEEE Trans. Automat. Contr.*, vol. 61, no. 11, pp. 3330–3343, 2016, doi: 10.1109/TAC.2016.2521370.

[104] J. Kaur, S. Garg,] Student, M. Tech(cse, and M. Gobindgarh, "Security in Cloud Computing using Hybrid of Algorithms," *Int. J. Eng. Res. Gen. Sci.*, vol. 4, no. 2, pp. 465–472, 2016, [Online]. Available: www.ijergs.org.

[105] Javed, "No TJaved A. Fast Implementation of AES on Mobile Devices. Proc. 8th Int. Netw. Conf.; 2010. pp. 133-142itle," [Online]. Available: Javed A. Fast Implementation of AES on Mobile Devices. Proc. 8th Int. Netw. Conf.; 2010. pp. 133-142.

[106] Mamun, "No T Mamun A, Rahman S, Shaon T, Hossain A. Security analysis of AES and enhancing its security by modifying 30 Computational Semantics S-box with an additional byte. International Journal of Computer Networks & Communications. 2017;9: 69-88itle."

[107] U. Farooq and M. F. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 29, no. 3, pp. 295–302, 2017, doi: 10.1016/j.jksuci.2016.01.004.

[108] L. Daoud, F. Hussein, and N. Rafla, "Optimization of advanced encryption standard (AES) using vivado high level synthesis (HLS)," *Proc. 34th Int. Conf. Comput. Their Appl. CATA 2019*, pp. 36–44, 2019, doi: 10.29007/x3tx.

[109] J. R. Naif, G. H. Abdul-Majeed, and A. K. Farhan, "Secure IOT System Based on Chaos-Modified Lightweight AES," *2019 Int. Conf. Adv. Sci. Eng. ICOASE 2019*, no. June, pp. 12–17, 2019, doi: 10.1109/ICOASE.2019.8723807.

[110] M. Mushtaq, "Efficient AES Implementation for Better Resource Usage and Performance of IoTs," no. c, pp. 7–11, 2020.

[111] Nagalakshmi, "No TitlNagalakshmi E, Mohan V, Kumar D. AES datapath optimization strategies for low-power low-energy multi securitylevel internet-of-thing applications. International Journal of Advanced Research in Science, Engineering and Technology. 2020;2:347-355e."

[112] K. G. Salim, S. M. K. Al-Alak, and M. J. Jawad, "Improved image security in internet of

thing (IOT) using multiple key AES," *Baghdad Sci. J.*, vol. 18, no. 2, pp. 417–429, 2021, doi: 10.21123/BSJ.2021.18.2.0417.

[113] A. Hafsa, A. Sghaier, M. Zeghid, J. Malek, and M. Machhout, "An improved co-designed AES-ECC cryptosystem for secure data transmission," *Int. J. Inf. Comput. Secur.*, vol. 13, no. 1, pp. 118–140, 2020, doi: 10.1504/IJICS.2020.108145.

[114] S. Das and S. Namasudra, "A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure," *Comput. Electr. Eng.*, vol. 101, no. July, p. 107991, 2022, doi: 10.1016/j.compeleceng.2022.107991.

[115] S. Hakim and M. Fouad, "Improving Data Integrity in Communication Systems by Designing a New Security Hash Algorithm," *J. Inf. Sci. Comput. Technol.*, vol. 6, no. 2, pp. 638–647, 2017.

[116] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks," *IEEE Trans. Ind. Informatics*, vol. 15, no. 9, pp. 4957–4968, 2019, doi: 10.1109/tii.2019.2895030.

[117] H. V. Gamido, A. M. Sison, and R. P. Medina, "Implementation of modified aes as image encryption scheme," *Indones. J. Electr. Eng. Informatics*, vol. 6, no. 3, p. 301~308, 2018, doi: 10.11591/ijeei.v6i3.490.

[118] R. Saha, G. Geetha, G. Kumar, and T. H. Kim, "RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/9802475.

[119] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2341–2345, 2016, doi: 10.1016/j.ijleo.2015.11.188.

[120] M. Vaidehi and B. Justus Rabi, "Enhanced MixColumn design for AES Encryption," *Indian J. Sci. Technol.*, vol. 8, no. 35, pp. 1–7, 2015, doi: 10.17485/ijst/2015/v8i35/82302.

[121] P. P. Mar and K. M. Latt, "New Analysis Methods on Strict Avalanche Criterion of S-Boxes," *World Acad. Sci. Eng. Technol.*, vol. 2, no. 12, pp. 150–154, 2008.

[122] D. Bui *et al.*, "To cite this version : AES Datapath Optimization Strategies for Internet-of-

Things Applications," 2019.

[123] M. E. Hameed, M. M. Ibrahim, and N. A. Manap, "Review on improvement of advanced encryption standard (AES) algorithm based on time execution, differential cryptanalysis and level of security," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, no. 1, pp. 139–145, 2018.

الملخص

أدت الثورة الصـناعية الرابعة إلى انتشـار التكنولوجيا، مثل إنترنت الأشـياء، والبيانات الضـخمة، والخدمات السحابية، وأجهزة الاستشعار المؤتمتة إلكترونيًا، وما شابه. أحد المتطلبات الأساسية لهذه التقنية هو السرعة والمتانة في الوقت الفعلي لهذه الأجهزة. تُستخدم شبكات منطقة الجسم اللاسلكية (WBAN) بشـكل شـائع في أجهزة IoT و IoB للمراقبة الصـحية، حيث أصـبح هذا المجال منتشـراً بشـكل كبير في الرعاية والمراقبة الصحية والطبية.

ومع ذلك، يجب أن تلبي هذه الأجهزة أيضًـــا المتطلبات المطلوبة لكفاءة الطاقة والأمان. في هذه الدراسة، سيكون التركيز على تقييم سرعة التنفيذ والحماية. سيقدم البحث لمحة عامة عن الثورة الصناعية الرابعة وتقنيتها وتصـــنيفاتها وأهميتها، ويتعمق في إنترنت الأشـــياء وإنترنت الكائنات، بما في ذلك بنيته ومتطلبات التشـغيل والمكونات والطبقات وتقنيات الاتصـال التي يتم فيها الاتصـال اللاسـلكي. التي تعمل بتقنية (WBAN) ، بالإضـافة إلى طرق التشـفير والتشـفير الخفيف. ومتطلباته واهميته في اجهزة انترنت الاشياء المحدودة الموارد.

قدم هذا البحث عرضًا لاهمية الوقت والأمان المنفذين في أجهزة إنترنت الأشياء وإنترنت الاجسام، وســلط الضـــوء على التحديات الأكثر إلحاحًا ومجالات الاهتمام البحثي. تم إجراء مراجعة لعدد من خوارزميات التشـفير الخفيف الوزن، وتم اقتراح نسـخة معدلة من خوارزمية(AES) مع خوارزمية ضـغط هوفمان. يتم عرض هذه الخوارزميات وتنفيذها بدقة في أقسام البحث.

تم إجراء مراجعة شاملة لدراسات المسح الأخيرة والدراسات المتعلقة بالتشفير الخفيف، مع التركيز بشـكل خاص على تلك ب(AES) التي ترتبط بهذا البحث. تم اقتراح نسـخة معدلة من خوارزمية AES، والتي تم دمجها مع خوارزمية ضـغط ترميز هوفمان. كما تم وصـف المنهجية المسـتخدمة في عملية التقييم والاختبار بالتفصيل.

تم فحص فعالية خوارزمية AES الرئيسية في التشفير وفك التشفير من خلال 100اختبار بأحجام نص مختلفة. تشـير النتائج إلى أن الخوارزمية المقترحة تُظهر سـرعة ووقت تنفيذ افضـل من خوارزمية AES الرئيســية، بمتوســط 18.75٪ في جميع جولات الاختبار. مثال على ذلك، تمت مقارنة أداء الخوارزميات من حيث سرعة التنفيذ في الاختبار رقم 6 وفقًا للجدول رقم (9)، حيث يتم تشفير وفك تشفير نص بحجم 8 بايت. أظهرت النتائج أن وقت التشفير وفك التشفير لخوارزمية AES الرئيسية 33.81 مللي

ثانية، بينما كان وقت التنفيذ للخوارزمية المقترحة 26.46 مللي ثانية، مما يدل على تحسن بنسبة 21.74٪ على خوارزمية AES الرئيسية.

تم إجراء 100اختبار للتشفير فقط باستخدام نصوص ذات أحجام مختلفة و تشير النتائج إلى أن الخوارزمية المقترحة تتفوق على خوارزمية AES الرئيسية من حيث وقت التنفيذ في جميع جولات الاختبار. وبعد ذلك، تم إجراء 100 جولة فك التشفير فقط باستخدام نفس النصوص كما في جولات التشفير السابقة. تظهر النتائج أن الخوارزمية المقترحة تتفوق أيضًا على خوارزمية AES الرئيسية من حيث سرعة التنفيذ.

تم إجراء اختبار (Avalanche effect) والاختبار (Key sensitive attack) للتحقق من أمان الخوارزميتين، وأظهرت النتائج تقاربًا في نتيجة الاختبار بين الخوارزمية الرئيسية (AES) والخوارزمية المقترحة ، حيث أظهرت نتيجة اختبارAvalanche effect أن نسبة الاختلاف في النص المشفر في اختبار الخوارزمية المقترحة هي (53.54٪) ونتيجة خوارزمية (AES) الرئيسية هي (51.56٪)، كما تظهر التقارب من حيث الأمن والحماية في الخوارزميتين في الاختبار (Key sensitive attack) ، حيث لوحظ أن نسبة الاختلاف كبيرة في النص المشفر بعد تغيير حرف واحد في المفتاح.