International Journal of Computational Research in Science and Technology
Volume 1 Issue 1
Sep-Oct 2025, PP 12-28

Design and Implementation of Cryptographic Data Security for IoT Devices Using Unicode & ASCII

Eberechukwunemerem John Sunday

Computer Science and Informatics

Federal University Otuoke

eberechukwunemeremjohnsunday@gmail.com

Abstract. The study on the design and implementation of cryptographic data security for IoT devices using Unicode and ASCII is motivated by the high rate of insecurity of data observed during data transfers on IoT devices. IoT devices are one of the popular channels that assist users to communicate virtually from the comfort of their homes. Therefore, the purpose of this study is to design software for cryptographic data security that can encrypt data while in transit to another IoT device using a cipher algorithm based on symmetric encryption. Some related encryption algorithms were also reviewed. In gathering data, secondary sources were deployed for useful information. The waterfall development methodology was utilized in this work. It is a methodology where phases do not overlap and the input of the current phase is the output of the previous phase. The use of Unicode and ASCII in substitution and transposition techniques helped to achieve confidentiality, authentication, integrity, and guaranteed data security. The system was implemented using the PHP programming language, HTML, and CSS. The results obtained from this research indicate that the software outperforms other conventional encryption algorithms in terms of speed (it encrypted 148 kb of data in 0.00267 MS) and also in terms of cryptanalyst attacks such as brute-force and dictionary attacks. The software is highly recommended to individual users, network administrators, medical centers, educational institutions, and government organizations.

Index Terms: Cryptography, Encryption, Decryption, Plaintext, Cipher text, Confusion, Diffusion, Public Key (asymmetric), Private Key (Symmetric), Confidentiality, Integrity Manipulation, IoT (Internet of Things), Data, Security, Authorized, Unauthorized, Authenticated, Privacy, ASCII (American Standard Code for Information Interchange).

I Introduction

1. Background to the Study

The current trend of connecting various electronic devices, such as thermostats, robots, and smart devices, has given rise to the Internet of Things (IoT) prototype. These devices often handle sensitive data, such as those used in smart homes, cars, the health sector, educational institutions, and factory floors. IoT is a network of interconnected devices that generate data about the surroundings in which they operate. The term internet of things ‖ was first coined by British technology pioneer Kevin Ashton in 1999. He coined the term while he was working in an auto-ID lab center, and he was referring to a global network of RFID connected objects. Since 1999, this technology has been on the rise and is dominating the market for smart solutions to everyday problems.

It has the ability to generate data continuously for a long period of time, process this data, and give specific feedback to other devices that are connected to it. It also has the ability to communicate among other devices using specific modules, both remotely and locally. These IoT devices are connected to the internet and also use the internet as a medium of communication. In this modern era, modern cryptography techniques (mechanisms) are used to facilitate the necessary data security features required by these IoT devices. The two important concepts of modern cryptography, namely confusion and diffusion, were introduced by Claude Shannon (1945). Confusion ensures that the cipher text generated by the algorithm must be entirely different from the plain text and should never render any clue about the plain text. Confusion is achieved by using

different suitable substitution techniques. Diffusion, on the other hand, is achieved by using the transposition techniques, which help to increase the redundancy of plain text bits in such a way that any change in the plain text bits affects the cipher text bits.

To design a cryptography algorithm, there are a number of factors that are to be considered, the primary of which is the strength of the cryptography algorithm and the length of the key. To strengthen the algorithm, the concepts of confusion and diffusion are applied. The key lengths are chosen such that crackers (hackers) cannot obtain the original plain text message by applying a brute force attack. Other important parameters include the processing time taken by the algorithm and memory requirements.

The Internet has witnessed growth since the last two decades, due to its availability and cheaper cost, which attracted organizations such as government agencies, educational institutions, humanitarian organizations, businesses, and financial applications. The Internet has been integrated into our daily activities, fundamentally playing a vital role in our lives. Though there are many advantages to the internet today, it also has its own challenges, like every other modern technology, such as maintaining the privacy of data and the confidentiality and integrity of that data, which internet users are avoiding.

The cryptography algorithm or mechanism is not of one method (there are various ways to apply cryptography), it is not restricted to a domain, and producing unbreakable cipher text is an art of genius and not of technology. We found ourselves in an intelligent and tech-savvy generation, with the availability of high-end processing tools; there is a continuous need to develop strong cipher text (Suryavanshi H. and Dr. Bansal P., 2012).

To achieve this, unique keys are used for encryption and decryption of data, which are generated and stored by the authorized end users. Many developers use highly sophisticated hybrid encryption (a technique that merges two or more encryption algorithms), which ensures the security of data at all times. This hybrid encryption technique combines asymmetric and symmetric encryption to gain the strengths of each technique. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. (Ekwonwune, E. N., 2020). We need complicated and complex algorithms that generate strong cipher text to stand the test of attacks. This study proposed a cryptography algorithm to encrypt data transmitted over IoT systems using Unicode and ASCII, similar to that by Suryavanshi H. and Dr. Bansal P. (2013) but more enhanced in speed and security.

2. Statement of the Problem

The growing number of these interconnected IoT devices continuously generates a large amount of data daily and exchanges this data using the internet as a medium of communication, which exposes it to high risk such as;

- The fraudulent act of some internet and IoT device users, who can manipulate, alter, disclose, and destroy these data for their own selfish interests, thereby putting the data owners at risk.
- The increase in the unauthorized accessing of organizational data by cybercriminals, which puts these organizations' financial data, trademarks, and trade secrets in the hands of these criminals.
- These data stored on the IoT devices are very sensitive in nature, and therefore, there is a need to secure the confidentiality and integrity of these data while they are generated, sent, received, and transmitted. Therefore, there is a need for the development of cryptographic data security for IoT devices to eliminate these issues.

3. Significance of the Study

This study will have a tremendous impact on healthcare organizations, financial institutions, and government agencies as they guard against the growing risk of data breaches on IoT devices and protect sensitive individual and organizational data. Privacy for data provides valuable benefits to everyone as it ensures that data are not manipulated or altered when transmitting or being stored. One of the fundamental properties of data availability is to access data as at when needed, by individuals or organizations. This study will solve the issues of confidentiality, integrity, and privacy, ensuring a secured data system that will benefit individuals and organizations. This study will also help users have access to secured data, which gives them the right to control their data and improves the flow of data between IoT devices and their endusers. To design and implement a system that guarantees confidentiality and integrity of data usage and makes data processing more efficient by ensuring the availability of data. Therefore, it would guarantee a secured network environment.

4. Aim and Objectives of the Study

The aim of this project is to design and implement a cryptographic data security system for IoT devices using Unicode and ASCII. The objectives include the following:

- To develop a cryptographic data security system for IoT devices.
- To implement a lightweight cryptographic data security system using substitution and transposition techniques.
- To design a data security system for IoT device using PHP, HTML and CSS.
- To develop an enhance data protection system using Unicode and ASCII encoding system.

5. Scope of the Study

This study is focused on the area of data security. As its scope indicates, the primary focus of this study is centered on cryptography, data security systems, access control, and privacy issues. This study went further to determine how the breach of data would be reduced to an acceptable minimum. It also considers the effects of data breaches and solutions for individuals and organizations. To validate the architecture and evaluate the applicability and efficiency of the construction.

6. Definition of Terms

Cryptography: is the process of ensuring that data are secured by transforming them into a form that an unintended user cannot read or understand.

Encryption: It is the process of transforming a plaintext into a cipher text using a technique. Decryption: It is the process of transforming a cipher text back to plaintext using a technique. Plaintext: It can be described as anything that humans can read, understand, or relate to. Any human-readable word that you can make sense of (e.g., I am a student).

Cipher Text: It can also be called encrypted text, is a string of randomized letters and numbers that humans cannot understand or make any sense of. It is encrypted plaintext, and it is not readable until you decrypt it. (e.g., YBV5TROGH568H).

Confusion: It is the process of ensuring that the cipher text generated by the algorithm is different from the plaintext and does not show clues that will lead to the plaintext.

(Confusion = Substitution, e.g., J --;j Caesar Cipher).

Diffusion: It is a process that helps to increase the redundancy of plaintext bits so that a change in plaintext bits is replicated in the number of cipher text bits. It is achieved

using transposition techniques. (Diffusion = transposition or permutation, e.g., John—njho—DES.) Public Key (asymmetric): It is a cryptography that uses two keys; one key is used for encrypting the data, and the other key is used for decrypting the data. One key (the public key) is used by the sender to encrypt the plain text into cipher text, and another key (the private key) is used for the decryption of cipher text back to plaintext by the receiver.

Private Key (Symmetric): It is a cryptography algorithm in which the same key (secret key) is used for encryption and decryption of data.

Confidentiality: is the act of protecting data from unauthorized access or disclosure. Integrity: It is the process of protecting data from unauthorized alteration, modification, and manipulation.

IoT (Internet of Things): It is the network of interconnected devices, such as smart homes, fitness trackers, thermostats, and solar lights with sensors that are located in different locations and generate and share resources together through the Internet.

Data: It is a raw file. It is an unprocessed piece of information.

Security: is the state of being free from threat, manipulation, alteration, and danger. Authorized: It is a process in which the system grants access to resources only to authorized users (users allowed to use resources).

Unauthorized: It is a process in which access to resources is denied to users who are not allowed to use resources.

Authenticated: It is the process of a system verifying the identity of users before granting or denying them access.

Privacy: It is the state of the user that determines when, how, and to what extent data about them is disclosed to other users.

ASCII: It stands for American Standard Code for Information Interchange. It is a common character encoding format for data text in or the internet computer.

II Literature Review

1. Introduction

This chapter is for the review of related literature (related works). Cryptography is all about security, and every device that connects to the internet needs security for its sensitive data, which if breached could result in the loss of valuables or even cause death. There are a number of related works that can be reviewed, since security is everyone's business, but only a few will be selected, as well as some technologies used in this work. Furthermore, all the literature reviewed was on works that were related to the scope of this project.

2. Related Works

Introduction

A literature review was conducted among works on the same subject and beyond it to list out the features and shortcomings of these articles and hence the subject.

Review of Related Works

The article by Surendran et al. (2020) explains how lightweight cryptography is intended for extremely resource-constrained devices and is employed not only for encryption designs but also for authentication and hashing on vastly resourceconstrained devices. The article starts by describing different kinds of cryptography algorithms, after which the writers explain the attacks on lightweight ciphers. Lastly, a performance-based comparison in terms of run-time is shown for the algorithms chosen. A major disadvantage is that this article has not proposed any algorithm; only a comparative study between algorithms was discussed and analyzed.

The paper by Kumar and Patel (2014) discussed various usages of the Internet of Things and how this department is gathering success in the cyber security and privacy control fields. Various usages discussed are healthcare, smart homes, and intelligent community security systems (vehicle administration systems, enclosing security subsystems, property administration). Finally, security and privacy companies related to the IoT were also discussed. One disadvantage is that this article is completely theoretical and explains primarily the usage of the Internet of Things. No implementation model has been proposed for how to enhance the existing security systems.

The paper by Iqbal et al. (2020) suggests that with the increase in the number of IoT devices, the volume of data to be processed and analyzed has also increased.
When such large amounts of data are processed, there's a high threat of risks and security problems for the IoT devices. This article reviews the risks, challenges, and attack vectors of IoT networks and their security demands. A combination of network-grounded IoT frameworks and software-defined networking has been proposed. Finally, security solutions for software-defined security were discussed. The architecture proposed by the authors for the countermeasure is actually big and computationally extensive; it cannot be implemented on a large number of devices having lower performance power.

A comparative analysis was conducted by El-Haii et al. (2018) in terms of power consumption, throughput, energy performance, and time consumption of various algorithms such as DES, AES, MD5, SHA, and RSA. These are all heavyweight algorithms and have been implemented previously; no invention towards lightweight cryptography was discussed. The article by Abomhara and Kien (2015) classified risk, analyzed it, and then characterized the types of intruders and their attacks on data and their applications. The ACID properties were also discussed, after which various security risks, attacks, and vulnerabilities of data were discussed. Finally, the authors have discussed intruders and organized groups for attacks. The article is a check on various dangers and vulnerabilities in data networks. It concentrated on security challenges on IoT devices and services but failed to suggest a real-time solution for the classified attacks.

The article by Arabo (2015) concentrated on analyzing the threats of smart devices in a smart home network and the challenges faced while protecting these devices. The author has done risk assessments and formulated a table containing the terms ―risk,‖ ―risk vector,‖ and ―security steps.‖ The risks taken into account are data loss, data exfiltration, tampering, and malware, for which risk vectors and security steps have been explained. No test bed has been provided for their proposed analysis on how to address the rising risks.

Corresponding to the paper by El-Haii et al. (2018), the article by Dhatrak et al. (2020) concentrated on studying the security risks on IoT devices and providing

countermeasures for the found risks. Also, the authors have discussed the application areas of the Internet of Things, like drug and health care, smart cities, business, and automotive. The authors failed to provide an implementation model.

Safi (2017) proposes a hybrid encryption to reduce safety threats and the time consumption of doing the same with less computational complexity. They've formulated the algorithm bearing in mind overall insight, intelligent processing, and dependable transmission. For data trade-off in the IoT, focus was given toward integrity, nonrepudiation, and confidentiality. Finally, they've used MATLAB software to test the speed and effectiveness of their proposed algorithm. The proposed algorithm is a hybrid of the HAN, AES, and RSA algorithms, all of which are actually heavyweight and can make a system heat up after running continuously.

Lu and Xu (2019) reviewed cyber security in the Internet of Things in an organized manner. The crucial factors associated with their work are the integration and protection of smart devices that have different functionalities and data communication technologies. Their investigation is applicable to the cyber security of IoT, its framework and taxonomy, and strategies and countermeasures for attacks and vulnerabilities in an IoT network system. The article could have explained how intrusion detection and prevention could have been integrated while planning a smart home network.

The paper by Tawalbeh et al. (2020) focused on the background of IoT networks and their security steps and the identification of various security and privacy issues. The approach and systems for having a secure IoT medium were also discussed, which also included the enhancement of existing solutions. A new IoT layered model has been suggested, which improves the privacy and security elements and the identification of the tier. The writers could have employed lightweight cryptography systems to enhance the power constraint factor and for the implementation of their model on devices with lower performance power.

Thakor et al. (2021) work on resource-constrained devices such as sensors, smart cards, etc. that have restricted processing power, low memory, limited energy application, or a mixture of all of these in their work. To provide communication by these devices with greater security, lightweight cryptography has been suggested and compared in terms of time consumption, memory application, key and block size, energy efficiency, latency, and hardware effectiveness. The paper made lightweight algorithms for pre-existing algorithms, and no hybridization was suggested.

Corresponding to the article by Safi (2017), the article by Bugeja et al. (2016) presented an overview of security and privacy issues in data processing systems. The only contrast is that the article was concentrated on the broader area of data processing systems, whereas this article is concentrated on smart home data. The constraints have been identified, solutions have been rated, and challenges have been discussed in this paper for the privacy and security issues. Although the article didn't give an execution model for the proposed solution based on the review conducted,

The main base of the algorithm suggested by Khari et al. (2020) is given to healthcare systems. This article suggested a new cryptography algorithm that was used to encrypt confidential data coming from various medical sources. To embed the encrypted information at a lower level of complexity, the steganography method was applied. To optimize the selection of cover blocks within an image, the Adaptive Firefly algorithm was applied. The final algorithm formulated is actually computationally extensive and would be optimized by applying lightweight cryptography algorithms.

3. Data Security

Security is a fundamental part of any system. Data security can be described as the process of ensuring that authenticated users have access to only what they are authorized to have access to. Often, people don't really consider security as an important aspect of their lives, but when you make mention of terms like data confidentiality, data integrity, the sensitivity of data, and data ownership, they become interested. There are a variety of techniques or mechanisms that are implemented to secure data from IoT devices. According to Mitnick et al. (2002), ―the human factor is the weakest link in security.‖ Security is often very difficult to achieve because of the ignorance of some users. The author further said that ―security is not a technology problem,‖ it is a people and management problem. I can say that the technology factor and human factor work together to achieve maximum IoT data security. Data access control is the process of ensuring that a permit is granted or denied for the use of a specific data resource by a particular entity.

4. What Is Cryptography?

Cryptography is the art of securing data through the process of transforming it into a form that an unauthorized receiver cannot read or understand. Cryptography ensures that readable plaintext is converted, using an algorithm or mathematical instructions, into something a computer or human cannot understand or read, which is called ―cipher text.‖ To read an encrypted message, you need a decrypting algorithm to read the message as an intended receiver, which will enable you to convert the cipher text back to plaintext.

5. Encryption

The conversion of plain text into cipher text is called encryption. It is one of the fundamental properties of cryptography. In encryption, you need an algorithm and a key to enable you to perform the encryption process. The key could be an alphanumeric piece of information, which will initiate how the algorithm is implemented on the plaintext to encrypt it into a cipher text. Without the key, it is an extremely difficult task or even impossible mission to decrypt the message, no matter how well you know the encryption system.

6. Types of Cryptography

There are many categories of cryptography algorithms, but three main categories are more popular: secret key cryptography, public key cryptography, and hash functions. Each of the following categories of cryptography algorithms has its own unique features and role to play within the cryptography landscape.

- Secret Key
- Public Key

III Materials and Methods

1. Introduction

The design of the proposed algorithm is classified into three parts. Section 1 describes in detail the architectural design, while Section 2 is about the proposed algorithm, and Section 3 presents the proposed algorithm in a flowchart diagram.

International Journal of Computational Research in Science and Technology
Volume 1 Issue 1
Sep-Oct 2025, PP 12-28

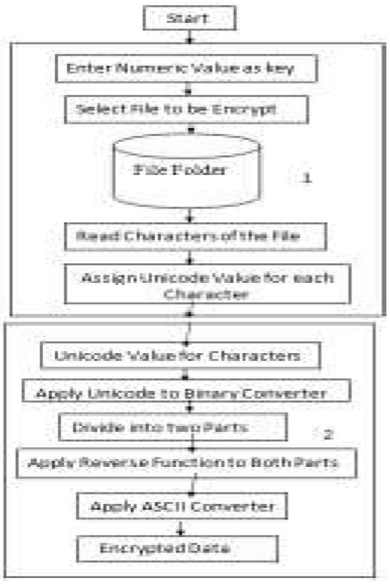

Figure. 1: Flowchart of the algorithm.

2. Architectural Design

The proposed architectural design is classified into two main subsections, as seen in Figure below; these subsections function independently of each other as they perform their tasks, but they synchronize.

- File Selection and Substitution
- Transposition.

File Selection and Substitution

The first block in the architectural design is the file selection and substitution block. Here, the user enters the private key value, which is a numeric value. The user will now select the file to be encrypted from the file folder. After the user has finished with the file selection process, the algorithm will proceed by reading each character of the selected file and substituting each character with its corresponding Unicode value.

Transposition

The functionality of this block is a little bit complex. In this block, the Unicode value of each character obtained from the file above is converted to a binary value using the Unicode to binary converter. The binary value goes through a series of transpositions, such as dividing the value between two parties and reversing both values. After the series of operations on the obtained binary value, the two values will be joined to obtain a different binary value. At this stage, the ASCII converter will be applied to the binary value, and this will generate an encrypted character that will be transmitted over the network.

3. Proposed Algorithm

In this section, a step by step explanation of the method used to encrypt the plain text to a Cipher character using assign, divide and reverse will be described. Enter the Key, is a numeric value.

- For (Each character in the File). do
  {
- Assign their Unicode value
- Convert the Unicode value of each character to Binary value

- Divide into two parts the value obtain in the above step
- Reverse first part
- Reverse second part
- Join (link) first part and second part
- Generate ASCII for the value obtain from the above step. }

End for

4. The Flowchart of the Algorithm

This section presents the flowchart of the proposed algorithm, as shown in Figure 3.2 above. The flowchart diagram helps to provide a clearer picture and a better understanding of how the algorithm functions, as well as a good representation of the workings of the algorithm. Representing the functionality of the algorithm in a flowchart helps to explain the algorithm in a more simplified way. It also illustrates the proposed algorithm in a symbolic way.

5. Methodology

Methodology is the theoretical analysis of the methods applied to a research work. Waterfall development methodology is the methodology of choice used in this project work.

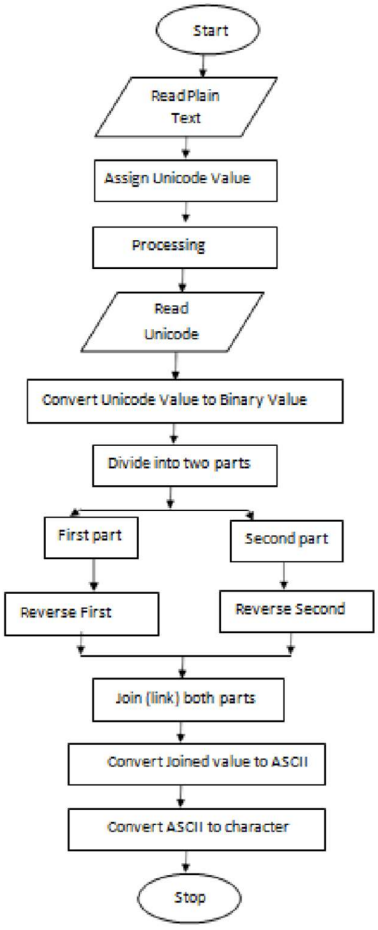

Figure. 2: Flowchart of the algorithm.

6. Waterfall Methodology

Waterfall methodology, the requirements and their implementations are well understood, and must be sequentially followed, without overlapping stages. It is a methodology that supports define before design and design before implementing.

Phases of Waterfall Methodology

Requirements: The first phase involves understanding what needs to design and what is its function, purpose, etc. Here, the specifications of the input and output or the final product are studied and marked.

System Design: The requirement from the first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture.

Implementation: With inputs from system design, the system is developed and constructed and tested.

System Testing: The system is deployed and tested in the environment of operation.

Maintenance: This step occurs after installation, and involves making modifications to the system or an individual component to alter attributes or improve performance.

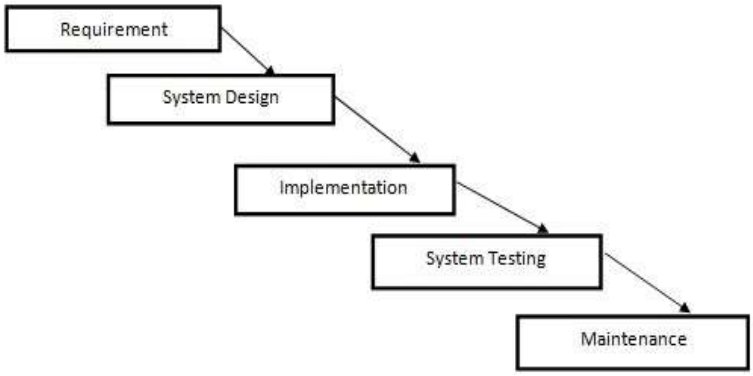

Figure 3: Waterfall Methodology Diagram

7. Example

This section is a step-by-step guide that describes and illustrates the encryption procedure of the proposed algorithm. Let's encrypt ―Hello FUO,‖ and it is assumed that the key has been entered, the file selected by the user, and Unicode assigned to each character in the file.

Table 1: Step 1: Assigned character to their Unicode value.

Character	Unicode Value
H	48
e	65
l	6C
l	6C
o	2F
	20
F	46
U	55
O	4F

Table 2: Step 2: Conversation of Unicode value to Binary value.

Unicode value	Binary value
48	0011010000111000
65	0011011000110101
6C	0011011001000011
6C	0011011001000011
6F	0011011001000110
20	0011001000110000
47	0011010000110111
55	0011010100110101
4F	0011010001000110

Table 3: Step 3: Divide the Binary value obtain above into two each parts.

Binary value	First Part	Second Part
0011010000111000	00110100	00111000
0011011000110101	00110110	00110101
0011011001000011	00110110	01000011
0011011001000011	00110110	01000011
0011011001000110	00110110	01000110
0011001000110000	00110010	00110000
0011010000110111	00110100	00110111
0011010100110101	00110101	00110101
0011010001000110	00110100	01000110

Table 4: Step 4: Reverse First Part

First Part	Reverse
00110100	00101100
00110110	01101100
00110110	01101100
00110110	01101100
00110110	01101100
00110010	01001100
00110100	00101100
00110101	10101100
00110100	00101100

Table 5: Step 5: Reverse Second Part

Second Part	Reverse
00111000	00011100
00110101	00110101
01000011	01000011
01000011	01000011
01000110	01100010
00110000	00001100
00110111	11101100
00110101	10101100
01000110	01100010

Table 6: Step 6: Join (Link) reversed value obtain from step 4 and step 5 above.

Joined(Linked) Reverse Value
0010110000011100
0110110000110101
0110110001000011
0110110001000011
0110110001100010
0100110000001100
0010110011101100
1010110010101100
0010110001100010

Table 7: Step 7: Convert Joined value obtained from step 6 above to ASCII value.

Joined Value	ASCII Value
0010110000011100	,
0110110000110101	l5
0110110001000011	lC
0110110001000011	lC
0110110001100010	lb
0100110000001100	L
0010110011101100	,ì
1010110010101100	¬¬
0010110001100010	,b

At this point, the message ―Hello FUO‖ has been encrypted into an unreadable message, which ensures that the confidentiality and integrity of the message are secured

and all messages being transmitted over the network are encrypted as shown in Table 3.7 above before being transmitted.

IV Results and Discussions

1. Introduction

This is the implementation section of the algorithm design; it describes a step-bystep guide on how to implement the algorithm. It gives a better description of the technology required to implement the algorithm, such as the operating system to run the algorithm, programming language support, etc. Furthermore, it discussed the performance assessment of the proposed algorithm, such as the time to encrypt and decrypt different sizes of files. Implementing software requires a well-organized approach to help identify and integrate components or services that will be useful to an organization or end-user.

2. Hardware and Software Requirements

The project is on security, for which we have used the PHP Cryptography library to develop the system, and the system requirements are as follows:

- Hardware Requirements: Memory: RAM size 512 MB Storage: Hard disk 10 GB
- Software Requirements: Web Browser: Chrome Operating System: Windows 7
- Programming Language: HTMT, CSS and PHP Local Server: XMAPP 8.01

3. Result of Performance

This section is for the assessment of the performance of the algorithm. An assignment tool has been deployed to analyze and assess the results generated by the algorithm using the PHP programming language. The results obtained have been shown below in Table 1, as it assesses the encryption and decryption of various sizes of files while also considering the time of encryption and decryption.

Table 8: Encryption and Decryption Time for different size of file

No	Size(KB)	Encryption Time(MS)	Decryption Time(MS)
1	148KB	0.00267	0.000947
2	200KB	0.0061	0.0027
3	250KB	0.0136	0.00903

4. Operational Guild

The algorithm is best with XAMPP 8.0.1, any Windows operating system but preferably best with Windows 7 and above, using also any browser of choice but Google Chrome is preferred.

Encryption and Decryption

This section is divided into two subsections, such as encryption and decryption;

- **Encryption:** This subsection is in charge of the encryption of plain text into cipher text. It described in comprehensive operational detail the encryption processes for a layman's understanding.
- **Decryption:** This subsection is in charge of the decryption of cipher text to plain text. It provides a simplified operational description of the decryption processes.

Operational Processes

- Use XAMPP, Windows 10, and Chrome Web Browser to execute the algorithm. Go to the XAMPP control panel and start Apache and MySQL.
- Use the web browser to generate the algorithm's home interface to execute encryption and decryption as shown in Figure 4.1 below, which is divided into two sections (encryption and decryption).

Encryption Process

- On the Encryption and Decryption Home Interface, click on Encryption to enter the encryption interface.
- On the encryption interface, enter the numeric key into the encryption key box as shown in figure 4.1 below.
- Click on the Choose File button to select the file to encrypt, as shown in figure 4.1 below.
- Click the Encrypt button to encrypt the file from plain text to cipher text, as shown in figure below.

Figure 3: Encryption Interface

Decryption Process

- On the Encryption and Decryption Home Interface, click on Decryption to enter the decryption interface.
- On the Decryption interface, enter the numeric key into the decryption key box as shown in Figure 4.3 below.
- Click on the Choose File button to select the file to decrypt, as shown in figure 4.3 below.
- Click the Decrypt button to decrypt the file from cipher text to plain text, as shown in Figure 4.4 below

Figure: 4: Encrypted interface after preforming Encryption

After executing encryption or decryption, click on the Windows Exit button to exit the Cryptogram web app.

Figure 5: Decryption Interface

Fig: 6: Decrypted Interface after preforming Decryption

V Summary, Conclusion and Recommendation

Summary The immersion of the Internet has changed the way we live; the interactions between people can now be done virtually in several contexts, from the professional life to social relationships. The advent of the IoT added a new dimension to this process by creating a communication environment for smart devices. To this purpose, the data shared between these smart devices should be encrypted before being transmitted over the network to ensure that access to data is granted only to authorize users. These devices have the ability to generate data continuously for a long period of time, process this data, and give specific feedback to other devices that are connected to them. It also has the ability to communicate among other devices using specific modules, both remotely and locally. So therefore, it is necessarily important to secure data on these smart devices using cryptographic security, whether they are in storage or transmitting, since sensitive data are stored on them.

Conclusion The Internet has been integrated into our daily activities, fundamentally playing a vital role in our lives. Though there are many advantages to the internet today, it also has its own challenges, like every other modern technology, such as maintaining the privacy of data and the confidentiality and integrity of that data, which internet users are

avoiding. Therefore, to guarantee more security of data on the internet, there is a need to adapt encryption and decryption, which is a common approach to ensuring the security of data.

In this system, two universal encoding systems were used, such as Unicode and ASCII (the American Standard Code for Information Interchange). The Unicode encoding system has three encoding formats. In implementing the algorithm, the Unicode UTF8 encoding format was used, based on its backward compatibility with the ASCII encoding system and also since Unicode UTF16 and UTF32 are too complicated for a lightweight, constricted device. The use of two 8-bit encoding systems helps reduce the number of bits the algorithm operates with, which drastically reduces memory space usage and increases execution speed due to direct support from the CPU. The use of divide and reserve function operators on the binary values ensures a strong encryption system and gives the algorithm an advantage in data security. The algorithm has faster encryption and decryption execution times as compared to conventional algorithms; its CPU load time is also reduced, and this is mainly due to the reduced number of transposition boxes. The system provides a solution to unauthorized access to data, data manipulation, illegal data modification, and data theft.

Recommendation The algorithm uses features such as substitution and transposition, which help reduce the processing time and enhance its security. This makes the algorithm a good choice to use when confidentiality and integrity of data need to be preserved at reduced execution and transmission times. It is recommended that software developers, organizations, manufacturers, and end-users adopt and start implementing cryptographic data security using Unicode and ASCII encoding systems when developing IoT devices or designing IoT networks.

References

1. Arabo, A. (2015), ―Cyber Security Challenges within the Connected Home Ecosystem Futures‖, Procedia Computer Science, 2015.
2. Dhatrak, A., Sarkar, A., Gore, A., Paygude, M., Waghmare, M., and Sahane, H., (2020), ―Cyber Security Threats and Vulnerabilities in IoT‖, International Research Journal of Engineering and Technology, 2020, Vol. 07, No. 03. 3. Safi, A., (2017) ―Improving the Security of Internet of Things Using Encryption Algorithms‖, International Journal of Computer and Information Engineering, 2017, Vol. 11, No. 5
4. Ekwonwune, E.N. and Enyinnaya, V.C. (2020) Design and Implementation of End to End Encrypted ShortMessage Service (SMS) Using Hybrid Cipher Algorithm. Journal of Software Engineering and Applications, 13, 25-40. https://doi.org/10.4236/jsea.2020.133003
5. Bugeja, J., Jacobson A., and Davidson, P., (2016) ―On Privacy and Security Challenges in Smart Connected Homes‖, 2016 European Intelligence and Security Informatics Conference.
6. Kumar J. S., and Patel, D. R., (2014) ―A Survey on Internet of Things: Security and Privacy Issues‖, International Journal of Computer Applications (0975 – 8887), Volume 90, No 11, March 2014
7. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwainder, M., (2020), ―IoT Privacy and Security: Challenges and Solutions‖, Applied Sciences. 2020, Vol. 10, No. 12
8. Abomhara, M., and Køien, G. M., (2015), ―Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks‖, Journal of Cyber Security and Mobility, 2015, Vol. 4, pp. 65-88

9. El-Haii, M., Chamoun, M., Fadlallah A., and Serhrouchni, A., (2018), ―Analysis of Cryptographic Algorithms on IoT Hardware platforms,‖ 2018 2nd Cyber Security in Networking Conference (CSNet), 2018, pp. 1-5.
10. Mitnick, K. D., and Simon, W. L. (2002) the Art of Deception: Controlling the Human Element of Security. Indianapolis, IN: John Wiley & Sons
11. Khari, M., Garg, A.K., Gandomi, A.H., Gupta, R., and Patan, R., (2020), ―Securing Data in the Internet of Things (IoT) Using Cryptography and Steganography Techniques‖, IEEE Transactions on Systems, Man, and Cybernetics: Systems, January 2020, Vol. 50, no. 1, pp. 73 – 80
12. Shannon C., (1949) Communication Theory of Secrecy Systems. Bell Systems Technical Journal 1949; 28:656–715p
13. Surendran, S., Nassef, A., and Beheshti, B. D., (2018) ―A survey of cryptographic algorithms for IoT devices,‖ 2018 IEEE Long Island Systems, Applications, and Technology Conference (LISAT), 2018, pp. 1-8, DOI: 10.1109/LISAT.2018.8378034
14. Suryavanshi H., and Dr. Bansal P., (2012) Conference Proceedings of Ninth IEEE and IFIP International Conference on Wireless and Optical Communication Networks, IEEE ISBN: 9781467319881, IEEE.
15. Suryavanshi H., and Dr. Bansal P., (2013) ―Design and Implementation of an Improved Cryptographic Algorithm using Unicode and Universal Colors‖ Current Trends in Information Technology Volume 3, Issue 1, ISSN: 2249-4707. CTIT (2013) 1-10 STM Journals 2013
16. Thakor, V. A., Razzaque, M. A. and Khandaker, M. R. A., (2021), ―Lightweight Cryptography Algorithms for Resource Constrained IoT Devices: A Review, Comparison, and Research Opportunities‖, IEEE Access, 2021, Vol. 9.
17. Web Reference: https://www.home.unicode.org/basic-info/overview as at 2nd February 2022 Web Reference: Kevin Ashton coined IoT (Internet of Thing) https://www.historyofinformation.com/detail.php?id=3411 as at 15th January 2023
18. Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., and Bangash, Y. A., (2020), ―An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security‖, IEEE Internet of Things Journal, Vol. 7, No. 10, October 2020.
19. Lu, Y. and Xu, L. D., (2019), ―Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics‖, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103-2115, April 2019.