Experimental Evaluation of Lightweight Cryptographic Algorithms

[1]Shreya Manjunath

Student Department of ISE, BMSCE
Bengaluru, India

Abstract: In today's era where data is the new oil, data being collected from devices might be a target of cyber-attacks in IoT systems that make use of data in the real world. As a result of this, countermeasures based on encryption are becoming increasingly important. Lightweight cryptography is a type of encryption that has a small footprint as well as low computational complexity. Lightweight cryptography is essentially expanding the realms of cryptography to constrained devices. Encryption for sensor equipment entails data security for confidentiality and integrity, which can be a powerful deterrent to attackers. Hundreds of thousands of diverse light weight gadgets will be connected in the future. To ensure trustworthiness, it is critical to safeguard the entire system. This paper comprises of an experimental evaluation of three lightweight cryptographic algorithms- KLEIN, RC4 and PRESENT.

***Index Terms*— lightweight cryptography, encryption, decryption, image, security**

I. INTRODUCTION

In the coming future, hundreds of thousands of diverse gadgets will be connected to each other, sending and receiving data from one another. To ensure trustworthiness, it is critical to safeguard the entire system. Especially when it comes to IOT devices, security and privacy is one of the most important aspect. The Internet of Things, Sensor networks, distributed control systems, healthcare and physical cyber systems are just a few of the emerging domains where highly resource constrained devices are interconnected, usually communicating in a wireless manner with one another, and working together to complete a task.

However, many cryptographic methods do not fit into restricted devices because majority of existing mainstream cryptographic algorithms are intended for desktop/server contexts. To address these limitations, interconnecting IoT networks with cloud servers to benefit from the fluidly scalable and always available storage and compute resources enabled by the cloud computing paradigm is a viable solution. Cloud-based IoT solutions enable the storage and processing of acquired data, as well as user mobility and the usage of the same data across numerous services. However, because the cloud cannot be regarded a trusted entity, outsourcing the acquired data to a cloud server raises problems about data confidentiality and fine-grained access control.

Many researchers have turned to designing new encryption techniques to protect data from eavesdroppers and illegitimate users. The scrambling process on digital images can be done directly on pixels or on rows and columns, whereas diffusion affects the original pixel values. To simply put, the substitution procedure substitutes each and every pixel value with the S-unique box's value. However, encrypting data does not guarantee its privacy. If a single substitution box (S-box) is used to encrypt an image, the information in the replaced or enciphered image may still be visible. This indicates that encrypting the original image with a single S-box is insufficient. Despite the fact that the information being transferred is encrypted, unauthorized users can still read it due to the encryption algorithm's lack of security. As a result, to improve encryption security, there is a need for strong encryption algorithm.

Lightweight cryptography is a type of encryption intended for use in resource constrained environment, such as RFID tags, sensors, contactless smart cards, and health-care equipment. Chip size and energy usage are significant parameters to determine lightweight properties in hardware implementations whereas reduced code and/or RAM sizes are preferred in software implementations. The lightweight primitives outperform traditional cryptographic primitives in terms of implementation characteristics. Additionally, lightweight cryptography provides reasonable security. The security-efficiency trade-offs are not usually exploited by lightweight cryptography. Some lightweight block cyphers that are popular nowadays in the domain of lightweight block cyphers are PRESENT, LBlock, TWINE, KLEIN, MIBS, LED, PRINCE, Piccolo, ITUbee, EPCBC, and PRINT cipher.

The security level of the encryption technique used to encrypt the image has a significant impact on its robustness. The original image will be entirely encrypted using a highly secure encryption method, allowing it to withstand intrusions on its integrity, anonymity, and authenticity. Security as well as time complexity are significant elements to consider when choosing an encryption technology. Since various types of data have different security priorities, choosing a cryptosystem is dependent on the nature of the application to be encrypted. Furthermore, the total number of pixels in the source image influences the time complexity. The larger the number of pixels in the plain image, the longer it will take to encrypt it. If the main requirement is just to encrypt a plain picture with high security, on the other hand, processing time may not be as important. A statistical study such as correlation, energy, entropy, or homogeneity must be done on an encryption algorithm to determine its security level. This can be achieved by testing each encryption algorithm and determining the statistics of its security characteristics. We can decide the best and strongest choice from those examined after conducting such security studies on each encryption method one by one.

Based on conventional security factors of encryption algorithms, we have classified the security of encryption algorithms into three levels (strong, moderate, and weak). The details of how we split encryption methods into three security categories based on security criteria including entropy, homogeneity, contrast, correlation, energy, PSNR, and MSE are detailed below. The focus is on the encryption techniques that are employed to encrypt 8–bit pictures. The maximum entropy for 8–bit pictures cannot be surpassed

by 8. Similarly, the greatest entropy that can be computed for binary pictures is 2. As a result, in the instance of 8-bit pictures, the whole entropy interval has been partitioned into three intervals. The whole interval's range is 0 to 8.

II. LITERATURE SURVEY

"A Study of Lightweight Cryptographic Algorithms for IoT" [1] by P. Nandhini, Dr V Vanitha, in this study, the security and algorithm specification of the majority of lightweight block cyphers have been reviewed. The paper also consisted of a thorough investigation was conducted in order to paint a clear picture of how encryption algorithms are designed. As mentioned in this study, each lightweight block cypher algorithm has unique qualities. Some employ the Feistel network, while others use the SPN. Furthermore, it was discovered that the algorithms with multiple S-boxes implied that the security is better but the cost is large after investigating and analysing the existing lightweight block cypher algorithms.

"A Review on IoT Security: Challenges and Solution using Lightweight Cryptography and Security Service Mechanisms Offloading at Fog" [2] by Vaishali Hitesh Patela, Sanjay Patel, in this paper the constraints of IoT devices has been discussed and these devices are unable to deliver secure hardware as well as software design due to resource limitations. This paper discusses IoT systems, fog computing and its two architectures, fog computing characteristics, how fog can address IoT challenges, IoT security concerns, and IoT security techniques.

"Revisiting Lightweight Block Ciphers: Review, Taxonomy and Future directions" by Aaqib Bashir Dar, Mashhood Jeelani Lone [3], we examine the state of the art and cutting-edge lightweight block cyphers that have been suggested over time by academicians. The author also explores the patterns in design approaches, categorizes the light-weight block cyphers according to a number of criteria, and then describes the results of the parametric evaluation. When it comes to elements in the field of cryptography, a security model will be a blessing. It is clear that the computational complexity of attacks on cyphers has been taken into account when assessing the security of block ciphers, but this measurement lacks concreteness due to the emergence of numerous attack methods with the rapid advancement of technology and the expansion of extremely powerful processing.

"Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things" by Mohammad Ali, Mohammad-Reza Sadeghi, and Ximeng Liu [4], in this paper the author has created a configurable lightweight hierarchical attribute-based encryption system. In our system, data owners who model miniature sensors and smart devices in an IoT network can encrypt their acquired data by conducting very efficient computational processes. Additionally, users can delegate to the cloud server the majority of the computational tasks involved in the decryption phase.

"A review on Lightweight Cryptographic Algorithms for Data Security and Authentication in IoTs" by Isha Bharadwaj and Ajay Kumar [5], in this paper many IoT applications and infrastructures have been briefly discussed. The security issues around information sharing and assaults have also been brought up. Any use of cryptography as a defence against these attacks is explained in length along with safety precautions for data protection and authentication. It is done to compare and contrast various lightweight encryption and authentication techniques. According to the results of the comparison investigation, the lightweight algorithms outperform traditional cryptographic algorithms in terms of memory requirements, operations, and power consumption.

"Review Paper On Lightweight Cryptography: Hummingbird on Different Platform" by Dr. T C. Thanuja, Usha S [6], in this paper the author has a discussion about how cryptography is one of the key components in ensuring security or maintaining data secrecy. Hummingbird cryptography is a more effective method for protecting devices with limited resources. Sensor nodes are like RFID tags. Hummingbird is immune to the most frequent attacks, including linear and differential cryptanalysis, and can provide the intended security with small block sizes. In this article, we examine the work on the Hummingbird cryptographic algorithm that has been done on several platforms, including microcontrollers, Sparton-2 FPGA, Sparton-3 FPGA, etc.

"A Light-Weight White-Box Encryption Scheme for Securing Distributed Embedded Devices" by Yang Shi and Hongfei Fan [7], in this research, the author presents a novel lightweight white-box encryption strategy for distributed embedded devices security that is resistant to all known attacks on WBEAs. The efficiency of the encryption operation and the modest static data size make our novel approach appropriate for devices with limited resources. Additionally, this system provides effective key updating at a relatively low cost, which is typically disregarded in related studies. Numerous experimental findings on actual embedded devices demonstrate the effectiveness of our new encryption algorithm, which makes it well suited for practical use.

III. METHODOLOGY

High Level Design

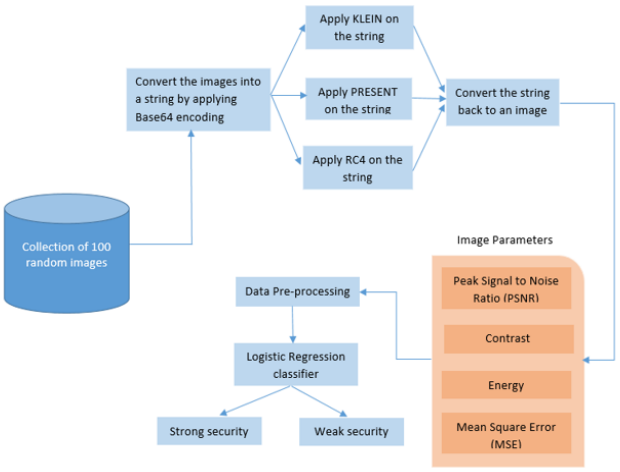

Fig 1: High Level Design

In the above figure, the initial dataset of hundred random images are put in a folder and the path of the folder path is used in each of the encryption algorithms. In order to apply any lightweight cryptographic algorithm the image must be converted to a string. In order to fulfil this, the image is read as a line of bytes and the bytes undergo Base64 encoding. The base64 encoding system converts binary data into ASCII strings to represent it in text. Base64 is intended to transport binary-formatted data across channels. It converts any type of data into a lengthy string of plain text. Once the string is encrypted, each of the three lightweight algorithms are applied

Image Paramerters

- Contrast: The distinction between an object and its depiction in an image or display is made possible by contrast, which is a variation in luminance or colour. Contrast in visual perception of the physical world is determined by the contrast between an object and other things in the same field of vision in terms of colour and brightness. We can view the environment similarly regardless of the dramatic variations in illumination throughout the day or from location to location because the optical system is more perceptive to contrast than absolute luminance. The contrast ratio, also known as dynamic range, determines an image's maximum contrast.

Fig 2: Same Image with Varied Contrast Levels

An image with little contrast (on the left) still has detail, but it tends to look flat and fuzzy. An image with standard contrast (middle) looks crisp and maintains detail and dimension. Especially in areas with sharply defined tones, a high-contrast image (right) loses clarity and can appear cartoonish or posterized.

$$Contrast = Maximum\ Pixel\ Intensity - MinimumPixel\ Intensity$$

- Energy: When expressing an operation within a probabilistic framework like MAP (maximum a priori) estimation in association with Markov Random Fields, energy is utilized to describe a quantity of "information." Energy can be a measure with negative and positive aspects that should be minimized and enhanced, respectively. The functions were still utilized within the models that are initialized, even if their capabilities aren't explicitly mentioned in the project's code. The image's localized change is measured by the energy. The term "energy" is used to describe the same thing across a wide range of contexts and names. It is the pace at which the pixels' colour, brightness, and size vary over local areas. This is especially true for the edges of objects within the image. These regions are also the hardest to compress considering the nature of compression, thus it is safe to assume that they are more significant. These areas are frequently edges or fast gradients. Although they appear in various situations, these all allude to the same thing.
- Mean Square Error: The MSE evaluates the performance of either an estimator or a predictor (a function that maps arbitrary inputs to a sample of values of a random variable). The preeminent quantitative performance metric in the field of signal processing has been (MSE). It continues to be the accepted yardstick for judging the fidelity and quality of a signal, the method of choice for contrasting various signal processing techniques and systems, and, perhaps most significantly, it is the almost universal preference of design engineers looking to optimise signal processing algorithms.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2$$

- Peak signal-to-noise ratio- PSNR i.e. Peak Signal to Noise Ratio is the ratio of a signal's maximum allowable value (power) to the strength of distorted noise that reduces the signal's ability to be represented accurately. As a result of the large number of signals with extremely high dynamic range, the PSNR is frequently expressed using the logarithmic decibel scale (ratio between the largest and the smallest attainable values of a variable quantity). The quality of a digital image can be subjectively improved through image augmentation. Whether or not one strategy produces visuals of a greater caliber depends on the individual. Quantitative and empirical metrics must be devised in order to compare how image enhancement techniques affect image quality. Below, we can see how an image's quality is impacted by the PSNR value.

Fig3: Images with low and high PSNR

Algorithm

Logistic regression is one of the Machine Learning algorithms that is most frequently employed in the Supervised Learning category. It is used to forecast the dependent variable which can be classified into categories using a specified set of independent variables.

Logistic regression is used to predict the output for a dependent variable that is categorical. The outcome must therefore be a discrete or categorical value. It offers the probabilistic values that lie between 0 and 1 rather than the precise values between 0 and 1. Either true or false, yes or no, 0 or 1, etc., are possible outcomes. Logistic regression and linear regression are fairly similar, with the exception of how they are used. Instead of fitting a regression line in logistic regression, we fit a "S" shaped logistic function that predicts two maximum values (0 or 1).

The logistic function's curve demonstrates numerous possibilities, such as whether or not the cells are cancerous, whether or not an animal is obese dependent on its weight, etc. Using both continuous and discrete datasets to classify fresh data, logistic regression is a significant machine learning technique. Logistic regression can be used to quickly determine the parameters that will perform best when classifying observations using different sources of data. The illustration below shows how the logistic function works:

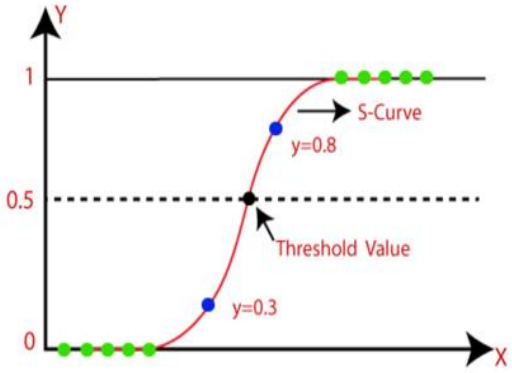

Fig 4: Logistic Regression Curve

The sigmoid function, a mathematical function, is used to translate the predicted values into probabilities. Any actual value between 0 and 1 is changed into another value. The outcome of the logistic regression must be between 0 and 1. It cannot exceed this value, it takes the shape of a "S" curve. The S-curve is also known as the logistic function or sigmoid function. In logistic regression, we use the threshold value concept, which determines the chance of either 0 or 1. Examples include numbers that tend to 1 above and 0 below the threshold value. The following method is used to generate the equation for the sigmoid curve

$$y = b_0 + b_1 x$$

Where the value of x ranges between -∞ and +∞. Since the values of the logistic regression ranges between 0 and 1, the above equation on the LHS becomes y/(1-y). After taking log on both sides, the final equation is:

$$y = \frac{e^{(b_0 + b_1 x)}}{1 + e^{(b_0 + b_1 x)}}$$

IV. IMPLEMENTATION

As the block diagram suggests, the first and foremost step in the implementation is to read the image and convert the image to a string. The hundred images being in varied sizes are first resized to a standard 500x500 resolution for the sake of uniformity. Then the image is first read as a stream of bytes and then Base64 encoding is performed on them and the string is stored in a variable. This initial step is common for all the three lightweight cryptographic algorithms.

Once the algorithms are applied and the string is encrypted, the encrypted string is converted back to an image. Once the strings are converted to image, these images are analyzed for image parameters and the values for Energy, Contrast, MSE and PSNR are calculated.

For calculating the image contrast, the difference between maximum value of contrast and minimum value of contrast is calculated. The Mean Square Error for an image is calculated as the cumulative of the squared error between the encrypted image and the original image. The energy of the image is measured through the localized change of pixels in an image.

V. RESULTS

TThe dataset formulated using the image parameters is fed to the system and a few observations have been made looking at the graphs and tables generated during data pre-processing. From the pre-processing performed, there were observations made with respect to the image parameters comparing the three algorithms. The average contrast, energy and Mean Square Error for PRESENT is higher compared to the KLEIN and RC4. Consecutively, the average PSNR for PRESENT is the least since PSNR is inversely proportional to MSE. The table below shows the efficiency of the machine learning model i.e. Logistic Regression used on test data from the dataset of 100 images.

TABLE I. EFFICIENCY OF THE LOGISTIC REGRESSION MODEL ON THE TESTING DATA

Efficiency of Logistic Regression Model		
KLEIN	***RC4***	***PRESENT***
81.15	80.64	94.28

REFERENCES

1. Arslan Shafique, Jameel Ahmed, “Detecting the Security Level of Various Cryptosystems Using Machine Learning Models”, IEEE Access, 9383 – 9393, December 2020
2. G. Arslan Shafique , Jameel Ahmed, Wadii Boulila , Hamza Ghandorh , Jawad Ahmad , Mujeeb Ur Rehman; Detecting the Security Level of Various Cryptosystems Using Machine Learning Models. IEEE Access 9, pp. 9383-9393 , 2021
3. Aaqib Bashir Dar, Mashhood Jeelani Lone, Nuzhat Hussain, “Revisiting Lightweight Block Ciphers: Review, Taxonomy and Future directions”, IACR 2021: 476, 2021.
4. Mohammad Ali, Mohammad-Reza Sadegh, “Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things”, IEEE Access, pp. 23951 - 23964, February 2020
5. Isha Bhardwaj, Ajay Kumar, Manu Bansal, “A review on lightweight cryptography algorithms for data security and authentication in IoTs”, International Conference on Signal Processing, Computing and Control (ISPCC), pp. 21-23, September 2017.
6. Dr. T C. Thanuja, Usha S, “Review Paper on Lightweight Cryptography: Hummingbird on Different Platform”, IJAHS, 2349-5235, Volume 2 Issue 3, pp. 29-33, June 2020.
7. Yang Shi, Wujing Wei, Hongfei Fan, “A Light-Weight White-Box Encryption Scheme for Securing Distributed Embedded Devices”, IEEE Transactions on Computers , October 2019.
8. L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", Comput. Networks, vol. 54, 2787-2805, Oct. 2010.
9. L. Liu, Y. Lei and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation", IEEE Access, vol. 8, 27361-27374, December 2020.