HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

Peer-Reviewed Journal
Indexed at: NSP - SJIF
Impact Factor 2022 = 4.91

RESEARCH TITLE

Developing and Improving the Data Transmission System of IOT Devices to Protect Data Encryption by Applying AES Cryptography Model on the Internet Media

Walid Hasen. Atomi[(1)], Tariq Muftah Honish[(2)] , Samira Fathi Mansour[(3)]

Whatomi@elmergib.edu.ly , tmhonish@elmergib.edu.ly , sfmansour@elmergib.edu.ly

(1.2) University of Elmergib, Faculty of Art and Science , Department of Computer Science.

(3) University of Elmergib, Faculty of Education Mesalata, Department of Computer Science

HNSJ, 2024, 5(7); https://doi.org/10.53796/hnsj57/23

Published at 01/07/2024 **Accepted at 18/06/2024**

Abstract

In today's Huge data environment within the internet, as we know security is one of the hot topics for the Internet of Things (IOT). The IOT itself is still in the children's shoes and the lack of security has quickly become one of its biggest growing concerns. There have been well-publicized security violations of consumer devices containing, for example, video of wireless baby monitors abducted and published on the Internet and home automation systems that show whether a house is occupied or not. Encryption in IOT for multimedia is very important and a development system worldview that understands the connections between the penetrating things and the establishment of a secure flowering society. This study will show encryption techniques and use the internet of things for applying AES cryptography data. encryption is explained when used on IOT devices using AES technology and explain how encryption is used.

Key Words: IOT, ASE, DES Encryption, IDEA Encryption, Cryptography, Security Internet Devices.

1.0 Introduction

Since IOT are constantly identified with the customer's daily life or work, protection and safety are of enormous importance. The inevitable, overwhelming and heterogeneous properties of IOT make their security problems extremely difficult. Also, the large number of asset-limiting hubs makes an inflexible lightweight prerequisite for IOT security instruments. Directly, attribute-based encryption (AES) is an outstanding response to ensure secure information transfer, storage, selection, and participation in the targeted conditions, making it not reasonable for the asset-imperative IOT applications. This overview will focus and focus on the selection of encryption in IOT for mixed media.

Data security is very critical for multimedia platforms on the Internet such as video and pictures. Conventional cryptographic algorithms / systems (so-called full-layers), first the entire content is compressed and this compressed bit stream is then completely encrypted with a standard cipher (DES, AES, IDEA, etc.). Because of the large amounts of data generated by the systems when dealing with multimedia applications to secure this data quickly and efficiently, a challenge and real-time constraints will be much faster than that of the generated data Time to make this data secure. The default encryption algorithms are insufficient. Another limitation of fully layered systems is the change in the overall bit stream syntax, which may disable some codec functionality. In situations where few resources are available (real-time networking, high-definition provisioning, low-memory, low-power, or computational functions), this approach is insufficient, justifying the inadequacy of standard cryptography techniques for such content, Selective encryption is a new trend in content protection, it aims to encrypt the amount of data, while reducing a sufficient and cost-effective security. Thus, selective encryption techniques are used to increase the speed of encryption as compared to complete encryption, and this provides better performance with respect to the compression ratio.

1.1 OBJECTIVES

- ✓ To protect data against unauthorized access and to encrypt it.
- ✓ The cryptographic process key of varying lengths is utilized for this purpose.
- ✓ To Enhance performance quality for Cryptographic by doing some modification on Standard AES algorithm.

1.2 PROBLEM STATEMENT

When images and videos on the Internet are encrypted by things (IOT) devices, there are many problems for the limited hardware that is connected to the Internet of Things (IOT), so the devices with a limited battery power, a small memory and A slow encryption process, which can cause many security problems and inconveniences to the user due to delays.

If the device is running out of power and is shut down before it has finished encryption, the files remain in a partially encrypted state. The device must be reset at the factory and all data will be lost.

To start the encryption process, we have to make sure first that the battery has enough charge at least 80%, because when the process starts there is no going back unless starting it again from the factory setting of the device and before that we have to make sure that we are safe, especially when use it for images and videos.

Encryption of images can be very costly in terms of time and computation, which can

make their assumption impossible for some sensor networks. So, we must look to solve these problems. The best approaches can be adopted to reduce the burden of image photography in wireless sensor networks.

According to the information above, this goal can be achieved by using many works for the principle of selective encryption. Selective Encryption is the perfect method to create secrecy and reducing the complexity. will use it in the propertied of media. In practice, I guaranteed the confidentiality, authenticity and integrity while the original data is protected.

There are optimal methods to achieve protection for the visual data using the AES encryption and solving full encryption problems.

2.0 LITERATURE REVIEW

The IoT is a networked collection of connected gadgets. Any gadget with an IP address, identification, and internet connection nowadays is part of the IoT. (Gazis, 2021) IoT refers to an expanding network of electronic devices that don't typically match the definition of a computer, but instead communicate with one another over the internet to carry out certain tasks. IoT growth has been exponential since its inception. The heterogeneity of the IoT is the first challenge it has encountered, as each of these various systems or devices uses circuitry and protocols that are distinct from the others (Butun et al., 2020). The IoT is the next development of the internet. (Evans, 2011) IoT gadgets can be found in our homes, workplaces, retail establishments, and even automobiles. 500 million devices were online in 2003 when there were roughly 6.3 billion people on the planet. (Evans, 2011) The invention of smartphones provided these devices with access to network connectivity outside of the house or workplace, which served as a crucial catalyst for the IoT's rapid expansion. With a global population of 6.8 billion people in 2010, connected IoT devices had multiplied to 12.5 billion thanks to the smartphone. In 2006, more Internet of Things (IoT) devices existed than people on Earth (Evans, 2011). Evans (2011) predicted that there will be 6.58 billion people and 50 billion IoT devices on the earth by 2020. Evans' estimate of 50 billion IoT devices by 2020 was not the only one; the DHS Cybersecurity Strategy predicted that by 2020 there would be 20 billion networked devices connected to the cyber domain. (DHS Cybersecurity Strategy | Homeland Security, n.d.

With the advent of the internet and the creation of the first domain, the third industrial revolution began around 1980. (Erboz, 2017) Erboz (2017) asserts that the IoT emerged in the late 1990s as the start of the 4IR. While the IoT ushered in the 4IR, with it also came potential security flaws that could exist with any 5 gadget whose comfort of use takes precedence over security (Erboz, 2017). Numerous claims have been made by security experts about the flaws in the ever-growing number of networked gadgets. By preventing users from updating security protocols on these devices, unchangeable factory settings on the devices allow for security vulnerabilities that are exponentially made worse. The introduction of smartphones in 2007, which made it possible for IoT devices to maintain network connections while in motion, caused the IoT industry to grow. (Farooq, et al., 2015) By enabling remote access to sensors, transceivers, and other equipment in nearby or distant locations, these networked devices aimed to reduce the labor intensity for operators. IoT devices started using sensors as extra input devices in or about 2013, enabling hostile actors to use them for technical information gathering. (Simon IoT, 2022) The IoT may be used differently than it was intended to be used. The purpose of networked thermostats, wearable fitness trackers, surgically implanted medical sensors, smartphone-enabled kids' toys, 5thgeneration cellular networked cars, and/or Wi-Fi and Bluetooth-enabled peripheral computer equipment was to serve as labor-saving tools. Unfortunately, user demands for affordability and convenience of

use have led to an ever-growing security risk (Beale, & Berris, 2017). According to Representative Anna Ashoo's speech to the 116th Congress of the United States in 2016, 6.4 billion connected IoT devices were in use globally. (Statista, 2021) The world's population was just under 7 billion people in 2016. According to Ashoo's claim, there was more IoT for every person on the earth. There will undoubtedly be rapid growth in the IoT in the future. According to Moore's law, the size of a transistor on a circuit doubles every two years. A similar predictive technique was used in a Chinese study that showed the internet doubled in size every 5.32 years (Zhang et al., 2008). With this information, it is quite probable to estimate how the Internet and the Internet of Things will grow over the coming years. Although the "size" of the internet cannot be quantified, the number of connected devices is increasing rapidly in both quantity and complexity over time. Predictions are exceedingly challenging because accurate data on the state of the IoT is hard to come by. To create a forecast of what the IoT might look like in the following year, Dave Evans evaluated the IoT in 2011 using the scant data that was available at the time. Using data spanning eight years, Evans estimated that the number of IoT devices exceeded that of the world's population in or around 2007, which was close to the time the smartphone hit the market and enabled the IoT to grow rapidly. With a global population of 7.6 billion, Evans anticipated that the IoT would reach 50 billion devices by 2020, or 6.5 IoT devices for every person on the earth (Evans, 2011)

The Internet of Things (IOT): where objects can share data without human interaction, and as expected, there will be 50 billion connected objects in 2020, each with its own IP address, which is of great importance to security and privacy Prospective.

Encryption: is the process that is used to secure many types of information and the encryption algorithms play an important role to secure the information systems, complete encryption methods are slow.

Compression: is the process of reducing the size of data by eliminating or removing unnecessary or less important data. This process makes it easier and faster for the transmission and storage of data .

Selective Encryption: is a method to maintain computing performance, overload, time, speed and it also provide quick security by encrypting a selected portion of a bit stream. The selective encryption method is one of the most promising solutions to increase the encryption speed compared to full encryption, so selective encryption is useful for real-time applications such as images, video content, and audio content. This dissertation (or paper) discusses the SE method used to rise the rapidity of encryption as it compared to full encryption. As we have already mentioned.

While the communication is interrogated via multimedia components, the data are communicated like text, video, pictures and audio over a network. Cryptographic methods are used to extend the protection of information and data during the transmission of data throughout the network. The different algorithms are available for security services like data, confidentiality, integrity and authentication to protect against the attacks, for examples: - changing the message, releasing message content, masquerading, etc. Encryption is the method by which a plaintext message is modified. Decryption is the inverse process of encryption, in which cipher text is decrypted back into the original text. The algorithm in cryptography is divided into two types, the Symmetric and the Asymmetric encryption. During Symmetric encryption, the user has the same secret key for encryption and decryption, and this key should save the secret to give privacy.

A symmetric algorithm doesn’t need a lot of computing power. Such as: AES, (3DES). The

Symmetric Encryption is very essential in advance cryptography, and that's why being the symmetric encryption is faster than the asymmetric encryption cryptosystem.

Selective Encryption is a method that encrypts a few parts of a file that has compressed data, and keeping the remain parts unencrypted. Nowadays, the security is getting bigger, upon that encryption come to be popular for any kind of sensitive communication data. although, we might save the time and the cost of data encrypting by efficient encryption Scheme, which will be necessary for the associations, companies, or individuals, so the importance of Selective Encryption is to minimize the quantity of the encryption data, while it is keeping high level of protection.

IOT devices: are used in each device that connected to other related device of the environment that automate homes, industries, businesses and other interested parts, that communicate more and more usable data to users. However, in this case the technology has moved more quickly than mechanisms to keep privacy and security of the users. May some of the problems facing IOT devices during full encryption by using AES encryption and how they work in encrypting images and video, and how to find solutions to these parameters by reviewing the selective encryption. Selective Encryption (SE) is a technique used to save the computational complexity or enable new system functionality by only encrypting a part of a compressed bit stream, therefore, it keeps the process under high security.

On the other hand, SE has a lot of aims that allows preserving scalability of some codec functionalities. If we compared to the full encryption, it is more useful in increasing the speed of the encryption. and also, it provides fast security by selected only a part of a bit stream to encrypt it.

There are some important benefits for the SE, like giving the ability to make a balance between processing demands and security. According to the selective video encryption plans resistant to bit errors and compatible to video formats have been suggested for wireless environments. In addition, it protects just the most important visual parts of an image or videos, depending on a secure but not fast "classical" cipher. After encryption, the image using the selective encryption technique it will be more secure against the attacks.

In the next paragraph, details on the IOT devices and discussed with the advantages and disadvantages.

3.0 RESEARCH METHODOLOGY

3.1 IOT devices

It is any computing device we can connect wirelessly to a network that has the ability to send and receive data, because these IOT devices are always connected to the internet it makes them so easy to hack from the attackers.

There are so many kinds of the IOT devices like door locks, cars, thermostats, fridges, light bulbs, implants for RFID, pacemakers (among an almost infinite list of possibilities), concert for people in businesses, the office, in industry, city streets and beyond and at home , For example of the smart home using some IOT devices: when the user reach his home, his car communicates with the garage to open the door. The thermostat is already to change the temperature that he preferred, by sensing his proximity, and he can unlock the door using hi smart phone or RFID implant. The home's lighting is adjusted to lower intensity and his favorite color . IOT products give us better control, streamline business processes; and better connection with people, systems that makes our life easier.

Because IOT devices are new idea and often sold with old and unpatched embedded operating systems and software the makers didn't aware about the security. So, the protection is not enough.

3.2. Some limitations set limits on how the devices can be encrypted

The importance of the IOT devices is to let each device communicates to any other related device using its special ways to automate the home and industry, delivering more and more useful data to users, businesses issues, and other interested parts. On the other hand, the technology has moved faster than mechanisms for securing the privacy and security of users. There are some problems about IOT device when you need multimedia encryption:

1- Internet of Things (IOT) devices are resource-limited.

2- Proprietary protocols are embedded in the firmware.

3-Memory sizes are small.

4- Bandwidths are limited.

5- Execution time is short.

6- Power is short-lived.

7- Batteries often need to be recharged (and unfavorable).

In some cases, there is no internal power supply, as in passive radio frequency ID (RFID) tags that draw power from nearby readers with batteries.

According to the potential sensitive data flows, the Suppliers of platforms, devices, data and applications are increasingly concerned with the channels and devices through it.

3.3 Multimedia cloud transmission and storage system based on IOT

In an early stage of the study, the idea was to develop the different methodologies for evaluating the security and protection of multimedia and to examine access control. The assumption of schemes based on the combined multi-media status and the roll access control. Similarly, the internal and external data output devices were connected together within the system. IOT is then analyzed to make a judgment about the connectivity and functionality of the devices and to make an assessment of their performance to see if the accessibility is improved. On this basis, a detailed description of the complete registration process, the roll allocation, the request of the multimedia file for data encryption, and the user login and access to multimedia files is described. Based on the results, this method is a positive way to reduce the potential security risks and provide a guaranteed method of security for the multi- media files. Another method of protection is the method that uses role encryption for cloud storage. This technique, which is based on roll-based access control (RBAC) and the encrypted data was used for storage in the cloud of encrypted files, would help ensure user access security and data storage security. In this configuration, there are a number of roles: first, a system administrator, second, a role manager, third, and fourth, a multi-media owner and a user. There are seven steps in this technique:

1) Setup, 2) Extract, 3) Manage 4) Role, 5) Add user, revoke user, 6) Encrypt and 7) Decrypt

A multimedia file is decrypted after the identity verification process. Similarly, the user side has a connection to, for example, a printer, a video player, and an image viewer. This can then be used to play videos or to print images. As shown in Fig. 1 for the layout of this configuration. The first security level uses a method of encrypted file storage or the selection is used for multimedia data storage. During transmission, the session key is used for data encryption. In addition, the creation of a unique algorithm with an electronic signature for identity verification is placed.

The system uses a session key with the following process between the public cloud and the private cloud in:

- When the role manager is for adding / deleting users.
- When the multimedia file owner is responsible for data encryption.
- While exchanging information between them.
- When the user requests the data access.

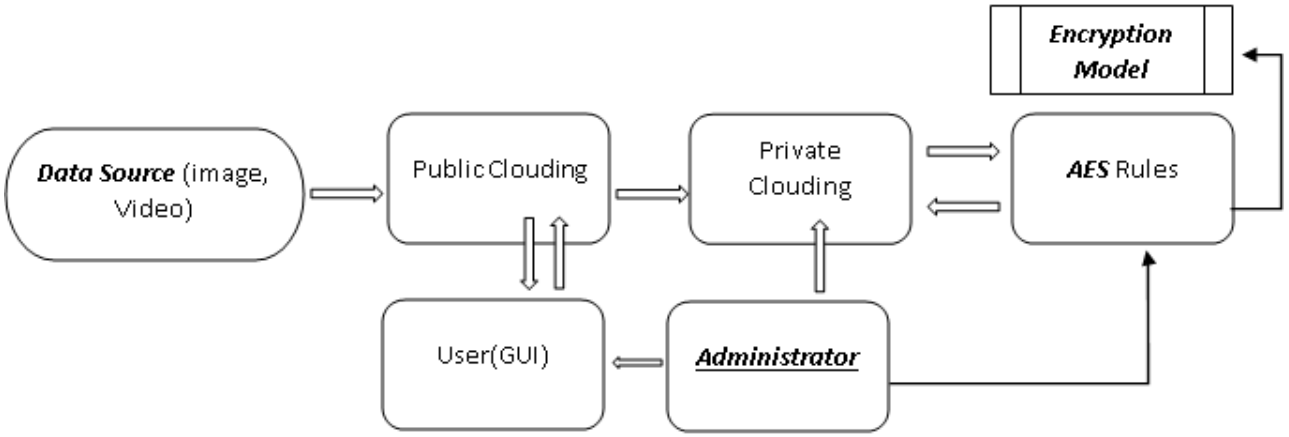

Fig.1 Layout of the complete *Methodology*

In this technique, IOT and cloud processing uses a combined proposal in mixed cloud storage system, based on the combination of multimedia data status with roll access control for real-time multimedia monitoring systems.

The analysis relevant studies provide a detailed description of five phases of this system: registration, roll allocation, user login, data encryption and decryption. The method of encrypted file storage is used for the security of multi-media data. In this transmission process, the session key is for the data encryption. During reception, the digital signature algorithm is used to check the identity of the sender. According to the analysis result, this system can effectively improve the flexibility of the user access control. At the same time, it can also resist various possible attacks and ensure system security .

Further details about the full encryption techniques will be in the next paragraph.

3.4 Fully layered Encryption

It means the compression of all data that need to be encrypted then transfer and store the encrypted data by using any types of encryption algorithm.

Firstly, the entire video content compressed after that it encrypted with optimal algorithms such as AES. This technique is not appropriate for real-time video applications according to the complicated calculations and slow speed.

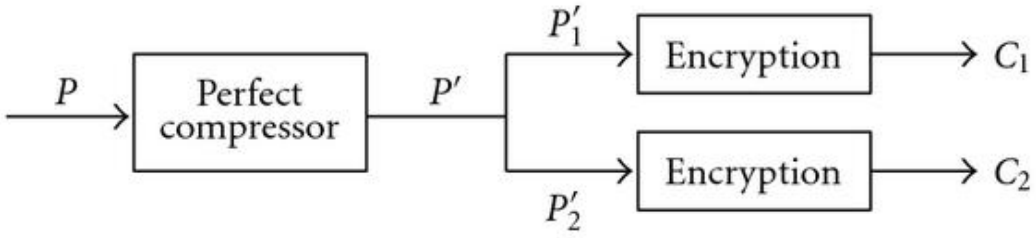

Figure 2: Fully layered system: the all plain text is encrypted.

3.5 Encryption of image and video with full encryption

A lot of digital visual data are saved in several types of IOT devices and are now being changed over different types of networks. These data contain the private confidential information or they are associated with financial interests.

When we want to protect precious data or images from the strangers, we should use encryption or decryption, as well as the dissertation for secure image passed through channels.

Digital images, which transmit the 70% of the information through the Internet, are important part of the network exchange. However, the image has a larger scale of data than the text message, and also the image has a higher redundancy, and a stronger correlation between pixels.

In comparison between the conventional encryption algorithms (such as DES) and the proposed text message, we find that it is not appropriate for digital image encryption, however a reliable digital image with its features is urgently needed for the encryption scheme AES, when we use it in image encryption and decryption. These techniques are for evaluating data authenticity and honesty, and the security for visual data, these are the most important issues in the field of multimedia security.

In the next paragraph, we find some concrete application examples which require some kind of encryption support in order to achieve the desired functionalities:

A) Telemedicine: is a systematic organization that cares of the humans' health.

A lot of medical sections agreed that in the future, the health care will be used by tele-radiology and technologies such as telemedicine in general.

Nowadays it is so important to demonstrate the necessity to provide the protection and the privacy of patients' medical image reports when it is stored in databases, and to transmit it over any kind of networks.

B) Video telephone is a technology that improve nowadays in the field of mobile radio technology. And that's need the content that should be protected from potential receivers for clear causes.

"The visual data are usually subjected to compression algorithms after the detection (or digitization)".

DESCRIPTION OF Advanced Encryption Standard AES (Rijndael)

Recently, we use the AES algorithm in many different applications in our life, like WWW servers, mobile phones, ATM machines and smart cards.

AES encrypts a plaintext and change it into a cipher text, then it uses the same private key to return the plaintext back to the original data, it is clear that the cipher text is very different form.

AES operation using cipher key for the applications of AES image encryption and decryption, an example in Figure 3 shows an encrypted image and original image.

Figure 3: AES Encryption and Decryption

In this approach, the sender and the receiver know the secret key. The AES algorithm remains secure; the key cannot be specified by any known methods, even when an attacker knows the plaintext and the cipher text. The design of AES algorithm is to use one of three key sizes (Nk), (AES-128, AES-196 and AES-156) use 128-bit (16 bytes, 4 words), 196-bit (15 bytes, 6 words) and 156-bit (32 bytes, 8 words) key sizes respectively. These keys are strong and have no weakness like other techniques until now. All key values are evenly secured, so no encryption will be more vulnerable than another.

The importance of this techniques is the combinations of encryption compression if we use a symmetric cryptographic and lossless compression method, also it shows that the process is focusing on images' privacy than on decreasing the data.

According to the increasing of our highly need of transmitted and store the data in IOT devices quickly, safely and easily, we should find a suitable way for that.

We find that; the cryptographic technique followed by the compression method is more secure and suitable in IOT devices features.

Video frames have highly required memory .it is different from any date by sending the data continuously for a period of time, and this compression is efficient for audios and videos and also images.

The quality of the compressed and then decompressed data should be good as possible as we can, and shorten complexity of this technique.

The time of the decompression algorithms should be limited and not exceed certain time spans, to avoid the problems in IOT devices, such as (losing batteries then losing all the sent information). We can use the hybrid compression techniques in multi-media systems like (audio and video data).

There are two main types of compression algorithms:

1- Lossless Compression: this type can compress the data without losing any information (data). When we decompress the data, it will be back for its original.

2- Lossy compression: When we decompress date, it might loss part of its original data.

4.0 RESULT AND DISCUSIONS

Advanced selective encryption is an improvement over the traditional full image encryption-decryption algorithms, which can be too large. In this method, multiple facets of various approaches are combined into a single algorithm: the unpredictability of pseudo random number sequences, the speed of the Arnold permutation, and the robustness benefits of AES. The goal here is to increase the legitimacy of the encrypted image and minimize execution time, as well as increase its robustness. In the decryption process, the image is compared to the image compression and errors are removed. Compared to the complicated image encryption of the AES method, this approach provides higher entropy and has a lower correlation between plain and encrypted images .

4.1 Selective Image Encryption Using DCT with AES Cipher

In this algorithm, the goal is to decompose the image into 8×8 blocks, which are then converted to the frequency domain from the spatial domain by the DCT. The lower frequencies of the image block and the DCT coefficients are correlated and encrypted. As the name suggests, the entire image is not encrypted, just selective DC and AC coefficients. It is difficult to predict the selective AC coefficients since the DC coefficients convey important visual information. Therefore, compared to other methods, this approach has a high level of security.

In order to check the robustness of this proposed algorithm, many security and statistical analysis tests have been tried. Both simulations and an analysis of the results show this system is efficient, strong against attacks, and appropriate for practical application, though it should be noted such a statement is based on a different security and statistical analysis evaluation than has been used for other methods .

4.2 Selective Encryption for Gray Images, Based on Chaos and DNA Complementary Rules

Unlike other techniques, in this method every pixel of a block is encoded and decoded. The most significant part of each block (MSB) is added to the least significant block (LSB) under the DNA addition operation. The LSB is encrypted by randomly choosing different DNA rules for each pixel. A 128-bits external input key is used to calculate the first condition and subsequently modified for each following block. The image is then permuted by Piecewise Linear Chaotic Map (PWLCM), where a logistic sequence is used to choose the encoding and decoding activity per pixel. After a simulated experiment and quantitative and qualitative security analysis, this method has been shown to provide an encryption good enough to repel exhaustive and statistical attacks. It is also the perfect technique for encrypting large, uncompressed gray images .

4.3 Chaotic Arithmetic Coding (CAC)

For the entropy coding of text and multimedia data, Arithmetic Coding (AC) is widely used. In addition to the relative occurrence probabilities of the input symbols, AC contains recursive partitioning of the range [0,1]. Chaotic Arithmetic Coding (CAC) is a data encryption method dependent upon AC. In this approach, a Shannon optimal compression performance is achieved by using a large number of chaotic maps to perform coding.

A key governs the specific choice of which map to use. CAC scrambles the intervals without generating any deviations to the width of the interval where the code word lies, thus allowing encryption without surrendering any coding efficient.

Binary CAC (BCAC) can be improved with some simple security enhancements which may alleviate some of the security issues of an AC-based encryption method. Plaintext Modulation (PM), Pair-Wise Independent Keys (PWIK), and Key and Cipher Text Mixing (MIX) modes are a few of the security enhancements that can be added to the BCAC.

It should be noted these enhancements have vital computational overhead. However, the BCAC decoder has lower hardware requirements than the BAC coder itself. This makes BCAC with SE the best choice for securing embedded multimedia systems.

To evaluate this method, experimental tests for compression performance were completed, along with a bit sensitivity analysis for key and plaintext.

Because this method has a simpler decoder that works at the same time it encrypts data, there is no loss of compression performance. Overall, the CAC method performed better than naive encryption algorithms .

In the following Figure, we compared the multi data with different size 128,192,255-bits Encryption according to its usage in the IOT devices when we encrypt images and videos.

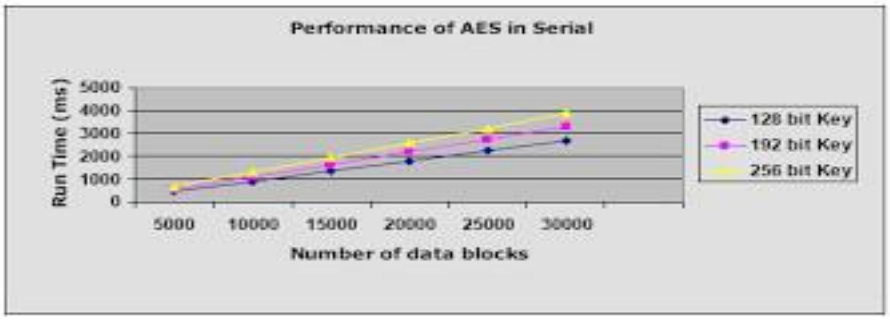

Figure 4: AES Encryption and Decryption performance with run time**.**

5.0 *CONCLUSION*

In this work, we viewed many techniques to enhance the security of video and images, as well as explained many current theories. All of these selective video and image encryption techniques provide good encryption, but also involve a high sharing cost and encryption time.

In order to increase encryption security, an attack should be simulated and the strength of the proposed encryption method should be analyzed, which would evaluate the practical possibilities of the video distribution. Several papers feature new selective encryption procedures but few attempts to present a solid security analysis of an attack. And of the ones that do, there is a notable inconsistency in testing as the encrypted part of the video and the security level is reduced. By using a perceptual mask and only encrypting those coefficients which are significant to the human visual system (HVS) for less secure transmission, the computational costs for SE can be further minimized. The most efficient method is clearly selective encryption in the entropy coding stage. This approach has suitable security, allows format compliance to compression standards, has no side-encryption effect, and has acceptable real-time performance.

Throughout both the Internet and network applications, security is one of the most challenging aspects. Encryption is the process used to safeguard data, and encryption algorithms are critical to efficient information security systems. However, full encryption techniques are sluggish. To save computing power, overhead, speed, and time, selective encryption (SE) is preferred. By only encrypting a selected portion of a bit-stream, this technique provides security quickly. The SE method is used not only to increase encryption speed, but to provide better compression ratio performance.

6.0 REFERENCES

[1] Sharma, S., &Pateriya, P. K. (2020). A Study on different approaches of Selective Encryption Technique. International Journal of Computer Science & Communication Networks, 2(6), 658.

[2]. Xiang, T., Qu, J., & Xiao, D. (2020). Joint SPIHT compression and selective encryption. *Applied Soft Computing*, *20*, 159-170.

[3] Yang, J., He, S., Lin, Y., &Lv, Z. (2020). Multimedia cloud transmission and storage system based on internet of things. *Multimedia Tools and Applications*, 1-16. [4] A Survey Jolly shah and Dr.VikasSaxena Dept. of CSE & IT, Jaypee Institute of Information Technology Noida, Uttar Pradesh 201307, India Dept. of CSE & IT, Jaypee Institute of Information Technology Noida, Uttar Pradesh 201307, India

[5] Advances in Information Security, SushilJajodia Consulting editor

Center for Secure Information Systems, George Mason University

[6] Review of Image Compression and Encryption Techniques Cryptography in Wireless

Multimedia SensorNetworks: A Survey and Research Directions .

[7] Daniel G. Costa *, SolenirFiguerêdo and Gledson Oliveira Department of Technology, State University of Feira de Santana, 44036-900, Brazil; solenir.figueredo@gmail.com (S.F.); gleddson.1@gmail.com (G.O.) December 2019; Published: 5 January 2019

[8] Selective Encryption Algorithm Implementation for Video Call on Skype Client AlwiAlfiansyahRamdan 1, Rinaldi Munir 20Informatics Engineering, Ban dung Institute of Technology 2Informatics Research Group, Bandung Institute of Technology Jl. Ganeca 10, Bandung, Indonesia 1alfiansyah.ramdan@gmail.com 2rinaldi-m@stei.itb.ac.id

[9]Qiu, H., &Memmi, G. (2018). Fast selective encryption methods for bitmap images. International Journal of Multimedia Data Engineering and Management (IJMDEM), 6(3), 51-69.

[10]Akramullah, S. (2017). Digital video concepts, methods, and metrics: quality, compression, performance, and power trade-off analysis. Apress.

[11] Liu, F., & Koenig, H. (2017). A survey of video encryption algorithms. computers & security, 29(1), 3-15.

[12] Moon, J., & Lee, K. (2015, October). Integrated visual security management for video encryption in limited battery devices. In Embedded Systems For Real-time Multimedia (ESTIMedia), 2015 13th IEEE Symposium on (pp. 1-8). IEEE.