IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 65-75
www.iosrjournals.org

Survey of Symmetric Cryptographic Algorithms

Ayyappadas ps[1],Anurose Devassy[2],Sherin C George[3],Anju Devassy[4]
[1]*M-Tech Scholar, Embedded Systems, Sahrdaya College of Engineering and Technology, India*
[2]*Assistant Professor, EC Dept, Sahrdaya College of Engineering and Technology, India*
[3] *M-Tech Scholar, Embedded Systems, Sahrdaya College of Engineering and Technology, India*
[4]*M-Tech Scholar, Embedded Systems, Sahrdaya College of Engineering and Technology, India*

Abstract: *The significance and the value of exchanged data over the Internet or other media types are increasing, the search for the best way out to offer the necessary protection against the data thieves' attacks. Encryption algorithms play a most important role in information security systems. Technologies such as CPU and memory are increasing and so is their need for power, but battery technology is increasing at a much slower rate, forming a "battery gap". It means that it is a considerable matter to choose the energy- and a memory-efficient cryptographic algorithm suitable for WSNs. This paper provides evaluation of six of the most common encryption algorithms namely: AES,DES, 3DES, RC2, Blowfish ,and RC6. We examine an efficient method for analyze trade-offs between energy and security. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types and sizes, battery power consumptions, different key sizes and finally encryption as well as decryption speed. So that this paper focus on a comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key sizes and finally encryption as well as decryption speed.*

Keywords: *Energy gap, Cryptography, Encryption, Decryption, Symmetric Algorithms*

I. Introduction

Before move on further to discuss more about power consumption, let's first we take a review of encryption algorithms because encryption algorithms and encryption techniques plays an important role in information security. These encryption algorithms and the techniques of encryption which we used for the security purposes, uses symmetric algorithms. Symmetric key encryption scheme or secret key encryption scheme has the following five ingredients:-

- Plain text:-This is the original intelligible message or data is fed into the algorithm as input.
- Encryption algorithm:-The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key: - The secret key is also input to the encryption algorithm .The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time .the exact substitutions and transformations performed by the algorithm depend on the key.
- Cipher text:-This is the scrambled message produced as output .It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands is unintelligible.
- Decryption Algorithm: - This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext .

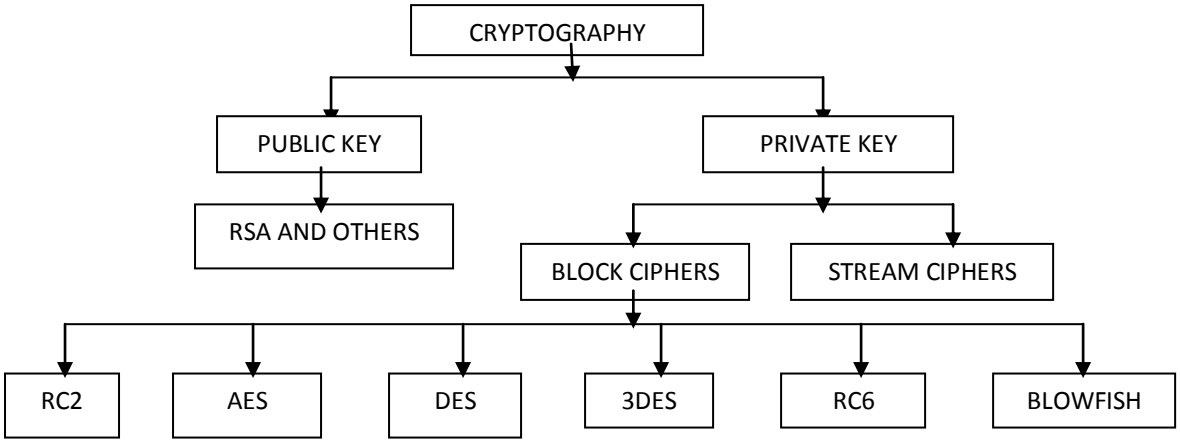

Fig 1: overview on field of cryptography

DES (Data Encryption Standard) was the first encryption (National Institute of Standards and Technology). DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weakness of DES, which made it an in secure block cipher .

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that3DES is slower than other block cipher methodsRC2 is a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits.RC2 is vulnerable to a related-key attack using 234chosen plaintexts .

Blowfish is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable-length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to Two fish .

AES is a block cipher .It has variable key length of128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices . Also, AES has been carefully tested for many security applications .RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard.

II. Motivation

Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. Strength of Symmetric key encryption depends on the size of key used. There are many examples of strong and weak keys of cryptography algorithms likeRC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits, while RC6 is used various (128,192,256) bits keys. The performance measure of encryption schemes will be conducted in terms of energy for wireless devices, changing data types -such as text or document, Audio files, Video files and images- on power consumption, changing packet size and changing key size for the selected cryptographic algorithms on wireless devices.

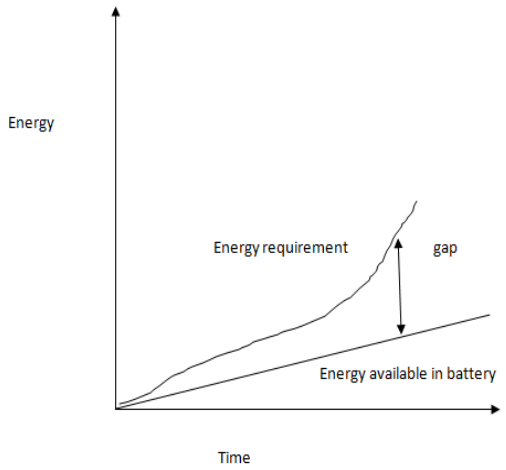

Fig 2: Battery gap

This paper examines a method for evaluating performance of selected symmetric encryption of various algorithms on power consumption for wireless devices. A wireless device is limited in resources such as less memory, less processing power and limited power supply (battery). Battery power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at a slower rate than other technologies. This causes a "battery gap" .We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices. This study evaluates six different encryption algorithms used or suggested for wireless local area network (WLANs) namely; AES, DES, 3DES, RC6, Blowfish, and RC2.

III. Related Works

Studies shows that the different popular secret algorithms such as DES, 3DES, AES, Blowfish etc. were implemented and their performance was compared by encrypting input files of varying contents and sizes. The results showed that blowfish had a very good performance compared to other algorithms. It was also concluded from that AES is faster and more efficient than other encryption algorithms. It was shown in that energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly.

IV. Experimental Design

For our experiment, we use a laptop IV 1.5 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 321vK byte to 7.139Mega Byte139MegaBytes for text data, from 33 Kbytes to 8,262 Kbytes for audio data, from 28Kbytes to 131 Kbytes for pictures(Images) and from 4,006Kbytes to 5,073 Kbytes for video files. We measure directly the current and voltage of CPU while running cryptographic algorithm so as to calculate the energy consumption as well as execution time. Based on LabVIEW, we made a special data acquisition program which can simultaneously carry on the data acquisition of current and voltage. The cryptographic algorithms are encapsulated into a measuring unit that can send specific signals to this program through GPIO port, and the signals are used to distinguish whether the acquired samples are valid for the running cryptographic algorithm. To entirely evaluate the various characteristic of security algorithms, we choose a widely used security library Cryptlib, which includes complete implementations of common cryptographic algorithms. Additionally, to minimize the effect of operating system itself, the real-time embedded system microcontroller is used to manage the hardware platform and to support the execution of the only task running cryptographic algorithms. The current and voltage is presented by discrete points after acquired by computer. Let U= {u0 ,u1,...,uN} denote the set of voltage samples and denote the set of current samples. Therefore, the set of power samples can be got as the product To simplify the calculation, the approximate energy consumption can be calculated with equation .τ is the sampling

period, which is the inverse of the sampling frequency. The execution time is equal to the product of sample number N and sampling period τ . In our experiment, we set the sampling frequency as 10000Hz, which can bring precise and efficient measuring data comparing to the results of using another instrument.

1.1 Analytical Framework

Different applications on embedded real-time systems may concern different performances such as data throughput, and power except the total energy consumption. Hence, it will be very useful to identify these performance features in embedded real-time systems. To investigate the relationship among different dimensions for energy consumption, we mainly conduct analysis from angles of unit energy consumption, power and processing speed. The relationship among various dimensions is illustrated in Figure 1, where the dimensions denoted by blocks with light gray background are measured by the instrument and others can be deduced by specified meanings.

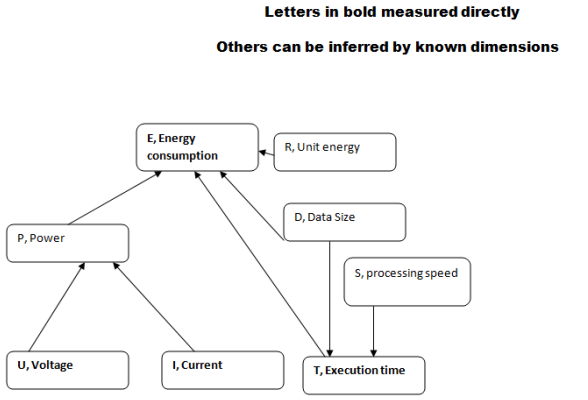

Fig 3: Relationship among different dimension

This method could completely tell the characteristics of an algorithm. Unit consumption reflects the energy cost to process a unit of data, while data processing speed indicates the latent requirement such as the speed or working frequency of processor and power represents the energy growth ratio varying with time. Those characteristics can guide the choice of corresponding algorithm to fit different engineering applications. The unit of a symbol denoting certain dimension is listed in TABLE 1. The mean of each symbol is explained in Fig.3.

$$R=E/D \text{ (J/B)} \quad (1)$$

$$S=D/T \text{ (KB/S)} \quad (2)$$

$$P=E/T(mW) \quad (3)$$

For our experiment we are collecting the following performance metrics that are given below.

- **Power consumption -** As we all know that energy measured in joule and power in watts or may be power measured in joule/sec but here the question is not that, that in which unit energy or power is measured but here the question is how to calculate how much power or energy is consume during encryption. For this purpose we are using the techniques that are described in previous section. We present a basic cost of encryption which is represented by the product of total number of clock cycles taken by the encryption and the average current drawn by each CPU clock cycle. The encryption cost is calculated in the unit of ampere-cycle. With the help of these cycles such as CPU clock cycle (the operating voltage count by the CPU) and the average current drawn for each cycle (ampere-cycle) we can easily calculate the energy consumption of cryptographic functions. For calculation of energy consumption by a any program (P) to achieve its goal of encryption or decryption is given by E=Vcc*I*T joules and Vcc is fixed for every process.
- **Encryption Time -** Encryption time is yet another an important issue because it is basically used to calculate the throughput of an encryption scheme as well as it indicates its speed. The encryption time can be define as the time that an encryption algorithm takes to produce a cipher text from a plaintext .The throughput of the encryption scheme can be calculated as the total plaintext in bytes encrypted divided by the encryption time.

- **CPU Process Time -** This time reflects the load of the CPU and this load depends on the CPU time used in the encryption process, the more time the CPU will consume in the encryption process, the higher will be the load of the CPU and it is important to notice that; it is concern only in some particular process of calculations.
- **CPU Clock Cycles -** CPU clock cycles is one of the major concern of our paper because it reflects the energy consumption or power consumption of the CPU while operating an encryption standard and it is assumed that each CPU clock cycle will consume a small amount of energy or power.

The following major tasks or operations that we performed to analyze the power consumption and the security aspects are as follows:-

- A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time, battery power and throughput.
- A study is performed on the effect of changing packet size on power consumption, throughput, and CPU work load for each selected cryptography algorithm.
- A study is performed on the effect of changing data types -such as text or document, Audio file, Video file and images- for each cryptography selected algorithm on power consumption.
- A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

V. Simulation Results

5.1 The Effect Of Changing Packet Size For Cryptography Algorithm On Power Consumption (Text Files)

5.1.1 Encryption Of Different Packet Size

- CPU Work Load

In Fig 4.we show the performance of cryptographic algorithms in terms of sharing the CPU load for encryption process. With a different data block size.

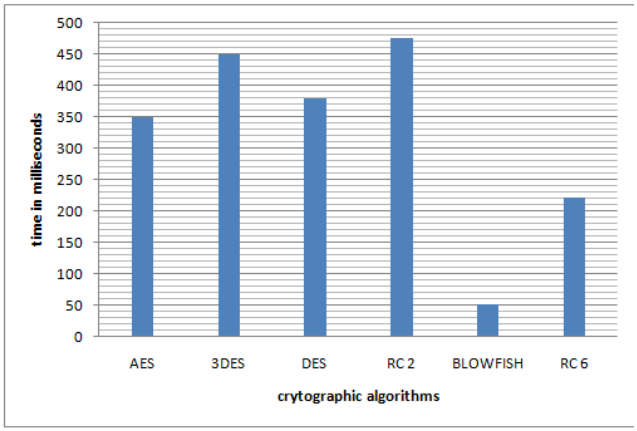

Fig 4: Time consumption for encrypt different Text Data

- Encryption Throughput

The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the through put value is increased, the power consumption of this encryption technique is decreased.

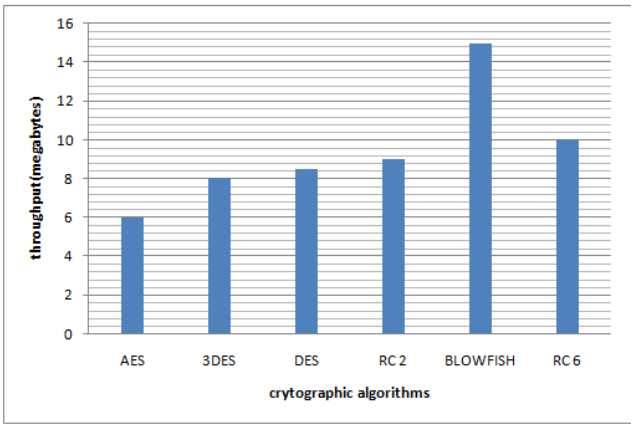

Fig 5: Throughput of each encryption algorithm

- Power Consumption

In Fig 6 we show the performance of cryptography algorithms in terms of Power consumption for encryption process. With a different data block size

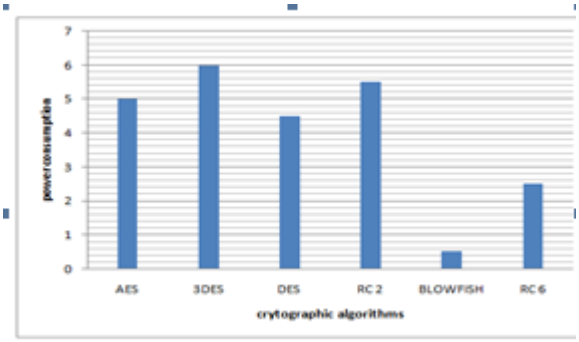

Fig 6: Power consumption for encrypt different Text document Files

The results show the superiority of Blowfish algorithm over other algorithms in terms of the power consumption, processing time, and throughput (when we encrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 16% of the power which is consumed for AES).Another point can be noticed here that RC6requires less power, and less time than all algorithms except Blowfish

5.1.2 Decryption Of Different Packet Size

- CPU Work Load

Experimental results for this compassion point are shown in Fig 7 below

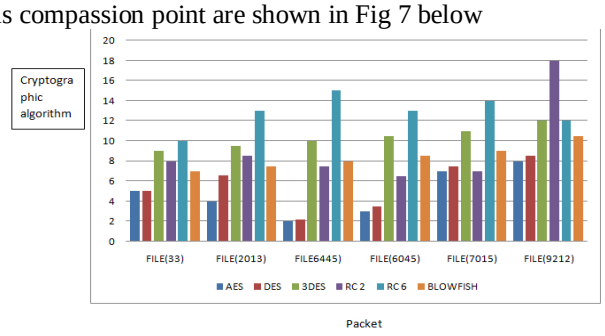

Fig 7: Time consumption for decrypting different Text Data

- Decryption Throughput

Experimental results for this compassion point are shown in Fig 8 below

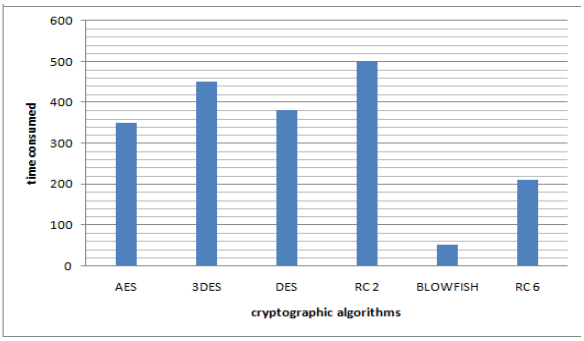

Fig 8: Throughput of each decryption algorithm

- Power Consumption

Experimental results for this compassion point are shown in Fig. 9

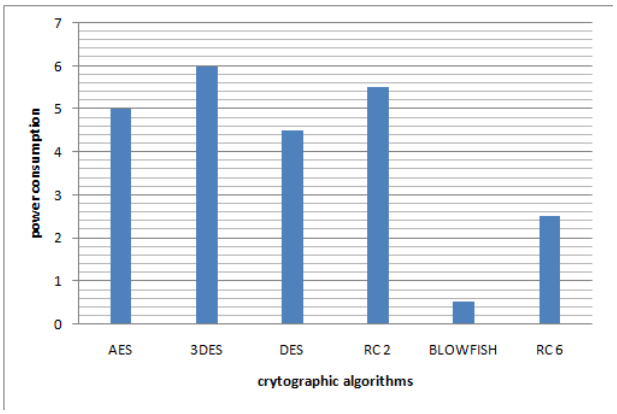

Fig 9: Power consumption for Decrypt different Text document Files

We can find that in decryption Blowfish is better than the other algorithms in throughput and power consumption (when we decrypt the same data by using Blowfish and AES, we found that blowfish requires approximately 34% of the power which is consumed for AES). The second point which should be noticed here is that RC6 requires less time than all algorithms except Blowfish (when we decrypt the same data by using RC6 and AES, we found that RC6 requires approximately 87% of the power which is consumed forAES). A third point that can be noticed is that AES has an advantage over other 3DES, DES RC2.The fourth point that can be considered is that RC2 still has low performance of these algorithm. Finally, Triple DES (3DES) still requires more time than DES.

5.2 The Effect Of Changing File Type (Audio Files) For Cryptography Algorithm On Power Consumption.

5.2.1 Encryption Of Different Audio Files (Different Sizes)

- Encryption Throughput

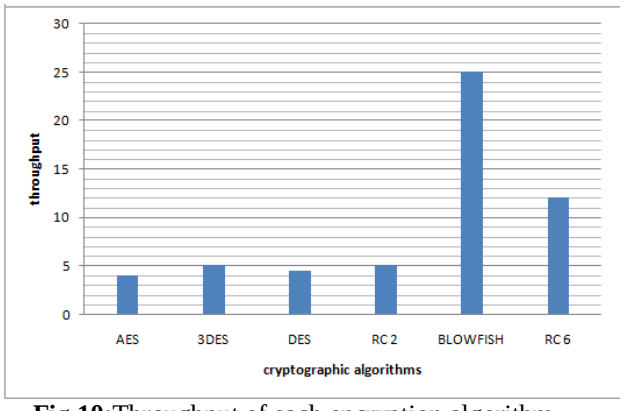

Fig 10: Throughput of each encryption algorithm

In the previous section, the comparison between encryption algorithms has been conducted at text and document data files. Now we will make a comparison between other types of data (Audio file) to check which one can perform better in this case. Simulation results for audio data type are shown

- CPU Work Load

In Fig. 11, we show the performance of cryptographic algorithms in terms of sharing the CPU load for encryption process. With a different audio block size

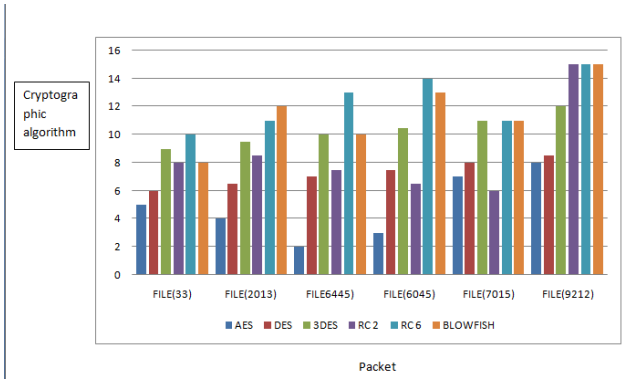

Fig 11: Time consumption for encrypt different Audio Files

- Power Consumption

In Fig. 10, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process. With a different audio block size

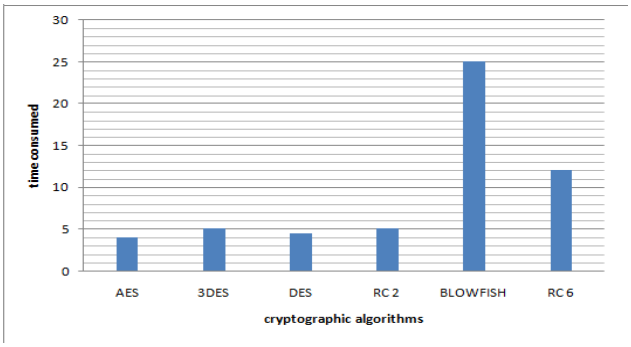

Fig 12

Power consumption for encrypt different Audio Files (Micro Joule/Byte)Results show the superiority of Blowfish algorithm over other algorithms in terms of the power consumption, processing time (CPU work load), and throughput (when we encrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 13% of the power which is consumed for AES).Finally, it is found that C2 has low performance and low throughput when compared to the other five algorithms in spite of the small key size used.

5.2.2 Decryption Of Different Audio Files (Different Sizes)

- Decyrption throughput

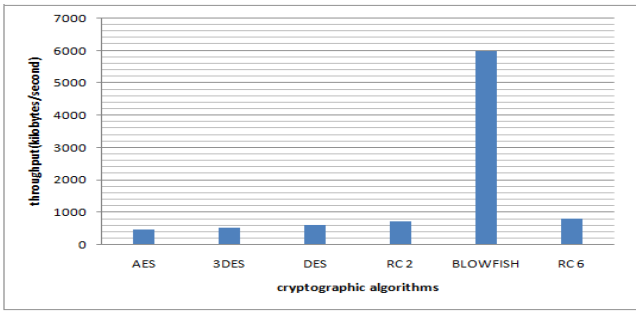

Fig 13

- CPU work load

Experimental results for this compassion point are shown Fig14.

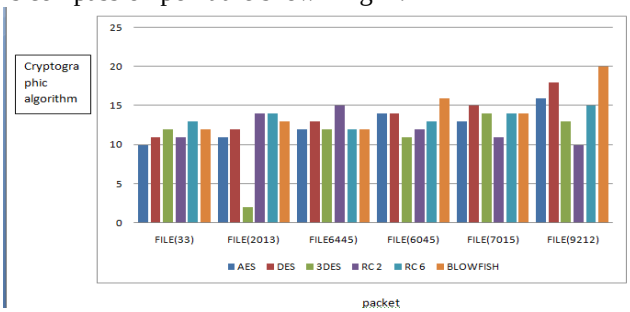

Fig 14

- Power consumption

Experimental results for this compassion point are shown Fig. 15 (Megabyte/Sec)

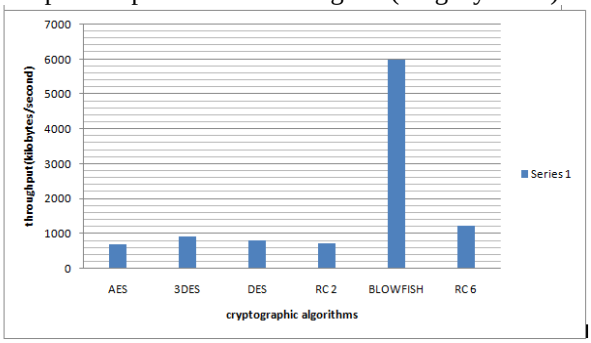

Fig 15: Power consumption for decrypt different Audio Files

Blowfish requires approximately 18% of the power which is consumed for AES. When we decrypt the same data by using RC6 and AES, we found that RC6 requires approximately 84% of the power which is consumed for AES.

5.3 The Effect Of Changing File Type (Video Files) For Cryptographic Algorithms On Power Consumption

5.3.1 Encryption Of Different Video Files (Different Sizes)

- Encryption Throughput

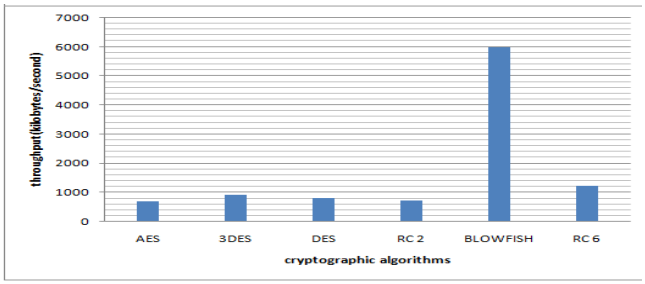

Fig 16

Now we will make a comparison between other types of data(Video files) to check which one can perform better in this case. Experimental results for video data type are shown Fig.at encryption.

- CPU Work Load

In Fig. 17, we show the performance of cryptographic algorithms in terms of sharing the CPU load. With a different video block size.

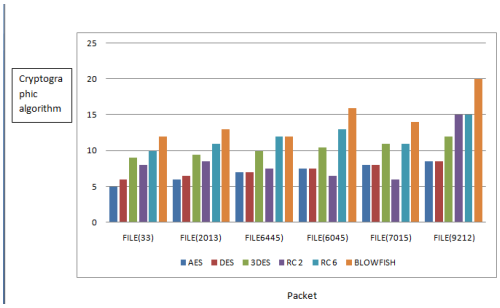

Fig 17: Time consumption for encrypt different video Files

- Power consumption

In Fig.18, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process. With a different video block size

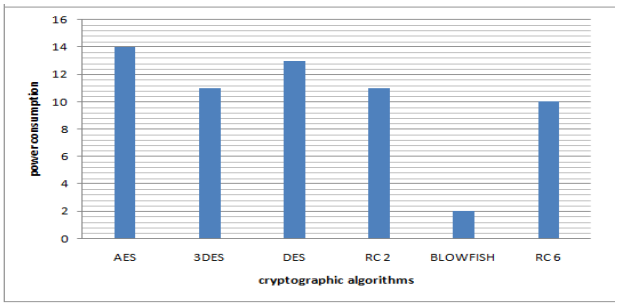

Fig 18: Power consumption for encrypt different Video File

The result is the same as in text and audio data. The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time, power consumption, and throughput.

References

[1]. D. D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede, "Securing embedded systems," IEEE Securiyt and Privacy, vol. 4, no.2, pp. 40-49, 2006.
[2]. V. Tiwari, S. Malik, A. Wolfe, "Power Analysis of Embedded Software: A First Step towards Software Power Minimization," IEEE/ACM International Conference on Computer-Aided Design, pp. 384-390, 2004.
[3]. V. Tiwari, M. Lee, "Power Analysis of A 32-bit Embedded Microcontroller," In Proceedings of Asia and South Pacific Design Automation Conference, pp. 141-148, 1995.
[4]. A. Muttreja, A. Raghunathan, S. Ravi, N. Jha, "Automated Energy/Performance Macromodeling of Embedded Software," In Proceedings of the 41st Annual Design Automation Conference, vol. 26, no.3, pp. 99-102, 2004.

[5]. A. Muttreja, A, Raghunathan, S. Ravi, N. Jha, "Hybrid Simulation for Embedded Software Energy Estimation," In Proceedings of the 42nd Annual Design Automation Conference, pp. 23-26, 2005.
[6]. W. Freeman, E. Miller, "An Experimental Analysis of Cryptographic Overhead in Performance-Critical Systems," International Symposium on Modeling, Analysis, and Simulation of Computer and Telecomm Systems, pp. 348-357, 1999.
[7]. R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, R. N. Uma, "Battery Power-Aware Encryption," ACM Transactions on Information and System Security, vol. 9, pp. 162–180, 2006.
[8]. N. R. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithm and Security Protocols," IEEE Transactions on Mobile Computing, vol. 5, no.2, pp.128-143, 2006.
[9]. A. Acquaviva, L. Benini, B. Ricco, "Energy Characterization of Embedded Real-time Operating Systems," ACM SIGARCH Computer Architecture News, vol. 29, no.5, pp.13-18, 2001.
[10]. C. Chang, S. Muftic, D.J. Nagel, "Measurement of Energy Costs of Security in Wireless Sensor Nodes", Proceedings of 16th International Conference on Computer Communications and Networks, pp. 95-102, 2007
[11]. C. Comaniciu, "On energy-Security Tradeoffs and Cooperation for Wireless Ad Hoc Networks", Journal of Cyber Security and Mobility, January, pp.53-64, 2012.
[12]. M. Qiu, W. Gao, M. Chen, et al, "Energy Efficient Security algorithm for Power Grid Wide Area Monitoring System", IEEE Transactions on Smart Grid, vol.2, no.4, pp. 715-723, 2011
[13]. NI, Make Accurate Power Measurements with NI Tools, http://zone.ni.com/devzone/cda/tut/p/id/7077.
[14]. Peter Gutmann, Cryptlib Security Toolkit Version 3.4, http://www.cryptlib.com.