IJEIT
The International Journal of Engineering and Information Technology
journal homepage:www.ijeit.misuratau.edu.ly
MISURATA UNIVERSITY

Cloud Computing Security and Privacy Preservation: Using multi-level encryption

Eng. Noufal Ghssan Issa
Faculty of Information Technology and Communications,
Master in Web Sciences, Syrian Virtual University

Damascus – Syria
noufalissa444@gmail.com / noufal_101083@svuonline.org

Dr. Mohamed Ali Mohamed
Lecturer at Faculty of Information Technology and
Communications, Master in Web Sciences
Syrian Virtual University
Damascus – Syria
mhamadtop@gmail.com / t_mamohamed@svuonline.org

Abstract—**Cloud computing has grown very quickly to become a promising business idea in the IT industry due to its characteristics such as cost reduction, flexibility, convenience, and scalability. The wide spread of Cloud Computing was accompanied by research fields in many aspects such as performance, storage, retrieval speed, backup and restore, security and privacy and other aspects related to it, which are still searched for today. Security and Privacy of data in Cloud Computing is of utmost importance to all its users, regardless of the nature of the stored data. In this paper, we propose a system that is secure and computationally efficient. The system focuses on three algorithms are AES (Advanced Encryption Algorithm), Blowfish algorithm and MD5 algorithm to build our proposed system. The principle goal guiding the design of any encryption algorithm must be security against unauthorized attacks and our proposed system is more security than any algorithm else. However, for all practical applications, cost of implementation and performance are also major concerns.**

Index Terms: **Cryptography, multi-level encryption, Blowfish, AES, and MD5.**

I. INTRODUCTION

Using the Cloud saves time and money for users. Cloud Computing is very promising for IT applications; However, there are still some issues to be resolved for personal and enterprise users to store data and deploy applications in a Cloud Computing environment. Data security is one of the most important barriers to adoption, and is followed by issues such as privacy, trust, and legality.

When the organization use cloud computing, they should provide their important data to service provider, but the organizations cannot take risks with their sensitive information. Due to cloud services being easily accessible and available for all so the possibility of sensitive information going to wrong hand is increasing. Secure transmissions prevent personal e-mail from being read by someone other than the intended recipient, and verify that the sender of a piece of information is who he says he is. To solve the data security and privacy issue in cloud computing, there are number of methodologies are introduced. Different ideas or solutions are applied. One of the solutions for data security, privacy and integrity problem is encryption.

In this paper, we propose a multi-level encryption system that is secure and computationally efficient. The framework consists of using a symmetric encryption algorithm AES and Blowfish, in addition to MD5 algorithm. The main purpose of this paper is to provide idea of the combination of these three algorithms to provide double security to the data stored inside the cloud. Performance and cost of implementation are also major concern, but the main goal behind this proposed system is to provide security against the unauthorized data access. The proposed system takes the advantages of the Feistel Encryption Scheme, an Advanced Encryption Standard (AES) and MD5.To satisfy high security, integrity and good throughput. This system is evaluated on real data to benchmark the encryption algorithms such as AES, RC6, 3DES, DES, and Blowfish in terms of computational running time and throughput for encryption process as well as the avalanche effect. The rest of the paper is as follows: Section 2 will present an overview of cloud service models, section 3 will present cloud deployment models with its advantages and disadvantages. In section 4 we have a simple review about cryptography; section 5 will present some of related work. Section 6 introduces the proposed system architecture, section 7 presents Results and analysis by the experimental evaluation and the last section presents the conclusions and future work [1].

II. CLOUD SERVICE DELIVERY MODELS

Cloud Computing involves the provision of computing resources (such as storages, servers, and applications) as services to end users by Cloud Computing service providers. End users access Cloud services on demand through web browsers. Cloud Computing service providers offer specific Cloud services and ensure the

Received 3 Apr, 2021; revised 3 May, 2021; accepted 1 June, 2021.

Available online 16 June, 2021.

quality of services. There are three standard models, and many derivative groups that describe, generally, the provision of Cloud services, and these services can be provided for every type of Cloud, whether private, public, or hybrid. The three individual models are often referred to as the "SPI" model, where "SPI" stands for “Software, Platform, and Infrastructure”(as a service).

A. *SaaS (Software as a Service):*

In this model, a complete client application is presented as a service on demand, with one instance of the service running on the Cloud and having multiple end users. On the customer side, there is no need to pre-invest in servers or software licenses, while for the provider, the costs are lowered, since only one application needs to be hosted and maintained. In this model, clients (users) can manage, modify and configure just the application. They cannot manage or configure the underlying Cloud infrastructure (network, storage, servers... etc.). In the event of a malfunction in this service, the responsibility for maintenance rests with the CSP provider. Currently, SaaS is offered by companies like Google, Salesforce, Microsoft and Zoho, etc. One of the commonly used services is the E-mail application [2].

B. *PaaS (Platform as a Service):*

In this model, the customer is free to create their own applications, which run on the infrastructure of the provider. Hence, the ability for the customer to deploy to the Cloud infrastructure applications created by the customer using the programming languages and tools supported by the provider (for example, Java, Python, .Net, etc.) is provided. In this model, the clients (Developers) do not manage or control the underlying cloud infrastructure, network, storage, operating systems, servers; they have control over the deployed applications and the configurations of the application hosting environment. To meet the management requirements and scalability of applications, PaaS providers offer a pre-defined set of operating systems and application servers, such as LAMP (Linux, Apache, MySQL, PHP) J2EE, Ruby, etc. [2].

C. *IaaS (Infrastructure as a Service):*

This model provides basic storage and computing capabilities as unified services across a network. Servers, storage systems, network equipment and data center space, etc. are grouped and made available to handle workloads. The ability offered to the customer is to lease processing, storage, networking, and other essential computing resources where the customer is able to deploy and run the software, which can include operating systems and applications. The user (software and network architect) does not manage or control the underlying Cloud infrastructure, but he controls storage, operating systems, identifying network components, and deployed applications (for example, firewalls, load balancers, etc.) [2].

There is a special type of IaaS called DaaS “Data Storage as a Service”. DaaS is a data storage service on demand. The main reason to use DaaS is that local and owned database systems are often restricted in separated server, post-delivery services and software license. In DaaS, consumers pay for what they are using, rather than license for the entire database. DaaS provides some features that are designed to scale out to store and retrieve a huge amount of data in a very short time. DaaS include Apache HBase, Google Big Table and Amazon S3, etc. Understanding the relationship and dependencies between these models is crucial; IaaS is the foundation of all Cloud services with PaaS built on IaaS and SaaS, in turn, based on PaaS [2].

III. CLOUD DEPLOYMENT MODELS

Regardless of the delivery model used (SaaS, PaaS, and IaaS), there are four basic ways to deploy Cloud services. Those responsible for the integration and use of Cloud services can play a vital role in determining the right Cloud path for a given organization.

A. *Public Cloud Computing:*

Public Clouds are provided by a specific service provider and can offer either a single (dedicated) or multi-tenant (shared) operating environment with all the advantages of flexibility, functionality, and benefit model for the Cloud. The physical infrastructure is usually owned and managed by the designated service provider and is located within the provider's data centers (outside the workplace -outside companies).

All clients share the same infrastructure pool with limited settings, security protection, and variations. One of the advantages of the Public Cloud is that it may be larger than the Enterprise Cloud, and thus, it provides the ability to expand smoothly on demand, and capital expenditures convert into operating expenses, and customers only pay for the services they use and need. However, the problem with Public Clouds is from a security point of view. It is owned by a third party and any data placed on these systems may be controlled by that party [3].

B. *Private Cloud Computing:*

Private Clouds are provided by an organization or its dedicated services and provide a single (custom) tenant operating environment with all the benefits and functions of flexibility and accountability. The Private Cloud aims to address data security concerns and provide greater control, which a Public Cloud typically lacks. There are two different types of special withdrawals:

- Private Clouds in the workplace.
- Externally hosted Private Clouds (third party).

Private Clouds, also known as Internal Clouds, are hosted in the workplace inside an individual's data center. This model provides more protection, but is limited in terms of size and scalability. IT departments will also need to bear the capital and operating costs. As for the second type, it is the most suitable for applications requiring full control, infrastructure configuration, and security. As the name suggests, externally hosted Private Clouds are hosted with the Cloud provider in which the provider is in [3].

C. *Hybrid Cloud Computing:*

A Hybrid Cloud is a combination of Public and Private Cloud offerings that allow for transitional information exchange, application compatibility, and portability across disparate Clouds and service providers who use standard or proprietary methodologies, regardless of ownership or location. With Hybrid Cloud service providers can take advantage of third-party Cloud service providers in a complete or partial way, thus increasing computing flexibility. Hybrid Cloud model is able to provide external scope on request. The ability to scale up the public Cloud resource can be used to manage any unexpected increases in workloads [3].

D. *Managed Cloud Computing:*

Managed Clouds are provided by a dedicated service provider and may provide a single-tenant (dedicated) or multiple-tenant (shared) operating environment with all the flexibility features, functionality, and accountability/benefit model of the Cloud. Physical infrastructure is per-owned and/or physically located in enterprise data centers with an extension of management and security control panels controlled by a particular service provider. The notion of Public, Private, Managed, and Hybrid, when describing Cloud services, really refers to attribution of management and service availability to specific consumers [3].

Table 1. Summary of the cloud deployment models

Deployment Mode	**Managed By**	**Infrastructure Owned By**	**Accessible And Consumed By**
Public	Cloud Services Provide	Cloud Services Provide	Untrusted
Private	Client	Client	Trusted
	Cloud Services Provide	Cloud Services Provide	
Managed	Cloud Services Provide	Cloud Services Provide	Trusted or Untrusted
Hybrid	Both Client &Cloud Services Provide	Both Client &Cloud Services Provide	Trusted or Untrusted

Additionally, it is important to understand the different trade-offs between the different Cloud service models [4]:

- In general, SaaS provides a great deal of built-in features directly included in the offering with minimal scalability and a generally high level of security (or at least the responsibility of security being on the part of the service provider) [4].
- PaaS provides less integrated features because it is designed to enable developers to create their own applications on top of the platform, and thus it is more scalable than SaaS in nature. However, this scalability is characterized by trade-offs in security features and capabilities [4].
- IaaS provides few application-like features, provides massive scalability, but generally has fewer security capabilities and functions other than protecting the infrastructure itself, as it expects operating systems, applications, and content to be managed and secured by customers [4].

IV. CRYPTOGRAPHY

Cryptography is the techniques of using algorithms to encrypt and decrypt files and data. Cryptography allows you to save very important information or transfer it across insecure internetworks (like the Internet) so that it cannot be hacked by hacker except the receiver. Security goals of data include three points namely: Confidentiality, Integrity and Availability Confidentiality of data in the cloud can be achieved only by cryptography [5].

A. *Cryptography has two parts:*

1. Encryption: Plain information is converted into the cipher information.
2. Decryption: Cipher information is converted back to plain information.

B. *Types of cryptographic keys:*

1. Public key: In this type each and every user must have public key as well as private key. Public keys and private keys are used during encryption and decryption.
2. Symmetric key: In symmetric key cryptography every user have own secret key. One key is used during encryption and decryption. And the Symmetric key algorithms have been divided into two types: Block cipher and Stream cipher. The current sizes of each block are 64 bits, 128 bits, and 256 bits.
3. Hash function: is an algorithm that maps data of arbitrary size (message) to a bit array of a fixed size (hash value or message digest). It is a one-way function, means it is a function which is infeasible to invert.

V. RELATED WORK

Many algorithms and approaches have been proposed to deal with the encryption/decryption problem. Besides the popular encryption (symmetric and asymmetric algorithms), there are new encryption algorithms categories. Some of these categories include: attributesbased encryption, Homomorphic encryption and multi-level encryption algorithms.

M. Xin [6] presented a hybrid approach that combines the benefits of both symmetric and asymmetric encryption algorithms to deal with IoT requirements of high security and low computation complexity. This approach uses the Advance Encryption Standard (AES) and the Elliptic Curve Cryptography (ECC); where AES is considered to be simple, reliable and fast encryption algorithm for long plain texts encryption and elliptic curves are used as a digital signature and key management. Although using AES is considered to be fast, key management and digital signature processes are encrypted using elliptic curves which considered being complex and slow, thus adding extra overhead to the hybrid approach.

S. Aljawarneh, et al. [7] proposed an encryption algorithm for multimedia data. The algorithm is a framework with multi-level encryption that includes: Fiestel encryption scheme, AES with S-box, and genetic algorithm. This scheme does not preserve confidentiality when two senders are using this scheme, because there is no mechanism to exchange the keys. Since the key is generated from the plain text so there is no key generation.

K. N. Prasetyo, et al. [8] suggested the use of symmetric encryption algorithm. Therefore, they proposed an implementation of the Blowfish encryption algorithm on FPGA resource and program it using the VHDL language. The proposed implementation was evaluated by measuring performance metrics such as security, encryption time, avalanche effect, and throughput and found to provide a good performance.

VI. SYSTEM MODEL

The system model is similar to the one proposed by [7] with an additional security level to solve the integrity problem by saving the hash function, in addition to some changes to make the system quicker. Figure 1 shows our proposed system model.

The original file to be encrypted is split into chunks, the plain text chunks are divided into 64bit blocks. The first level is encrypted using Blowfish algorithm, and Blowfish algorithm depends on Feistel network. This encryption is composed of shifting and rotation processes. Here the encrypted file is split into chunks, the cipher text chunks are divided into 128bit. The second level is encrypted using Advance Encryption Standard (AES) where the input for this encryption is the output of the Blowfish encryption. Lastly, we use MD5 hash function to calculate the hash value for the output file of the second level of encryption and this value will be as a digital signature for the encrypted file and will store it locally in database with the hash values of entered keys in the first and second level. The resulted encrypted file is sent over network to cloud to store it. The decryption is reverse of the encryption. We explain these levels in more details.

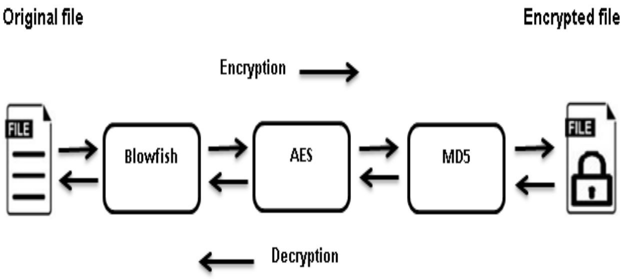

Figure. 1 our proposed system model

1. *Blowfish algorithm:*

   Bruce Schneier designed blowfish in 1993 as a fast, free alternative to existing encryption algorithms. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish algorithm is a 64bit block cipher based on Feistel rounds and F-function to provide the security with greater speed and efficiency [9].

   Blowfish is a symmetric block cipher that uses a variable length key from32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plain text into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits [9].

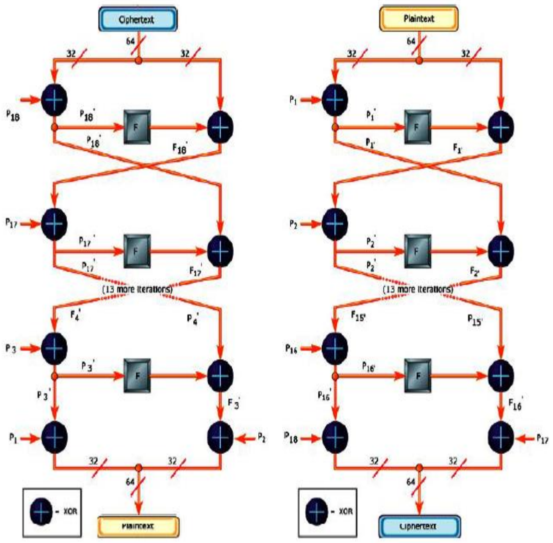

Figure 2. Flow diagram of encryption and decryption process of Blowfish algorithm

2. *Advance Encryption Standard (AES):*

   The Advance Encryption Standard (AES) is a symmetric encryption algorithm that needs one key for encryption and decryption. It uses permutation and substitution network where it iterates the encryption process for X rounds to generate the cipher text. AES is considered to be secure and fast encryption algorithm.

In AES, the size of the key will determine the number of encryption rounds. In general, AES uses 10 rounds for 128bit key, 12 rounds for 192bit key and 14 rounds for 256bit key [10].

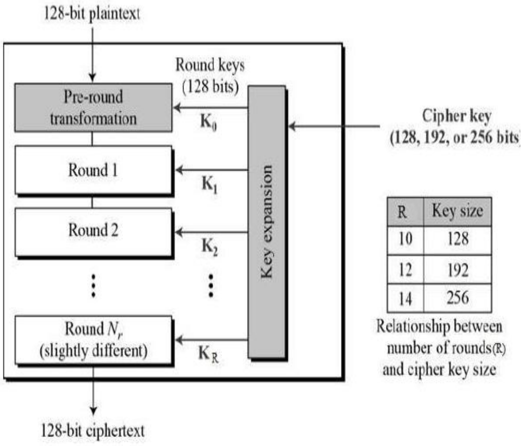

Figure 3.Flow diagram of encryption process of AES algorithm

Each round includes many processing steps and each of them comprises of four similar but different stages, while taking into account one stage that depends on the encryption key itself. We can summarize AES as follow:

- Initial Round: this round uses bitwise (XOR) technique that combined the block of the round key with each byte of the state, this is called Add Round Key.
- Rounds: this round encompass on four main processes that can be described as follows:
  - Sub Bytes process: process of replacing each byte that is located in the state with another byte by take into account the lookup table. Also is called a non-linear substitution process.
  - Shift Rows process: process of shifting each byte of the state to the left cyclically.
  - Mix Columns process: This process is implemented on each column; each of them is multiplied with a constant polynomial.
  - Add Round Key process: In this process the Rijndael's key schedule is responsible for deriving the sub-key from the main key for each round. After that, the bitwise XOR merges the corresponds byte in each state and sub key; due to insert the sub-key.
- Final Round: This process contains the same previous processes (Sub Byte, Shift Rows and Add Round Key) without Mix Columns process. After AES algorithm finishes the job completely, the plaintext is encrypted perfectly [10].

3. *MD5:*

It is one of message digest algorithm given by Professor Ronald Rivest in 1991. The Input is a message of arbitrary length and the output will be 128 bit hash code. The input message is separated into chunks of 512bit blocks. One MD5 operation consists of 64 operations, grouped in four rounds of 16 operations. In case the message is not an integer multiple of 512-bit blocks, the message is padded so that its length is divisible by 512. It can be used to verify file integrity and authenticity [11].

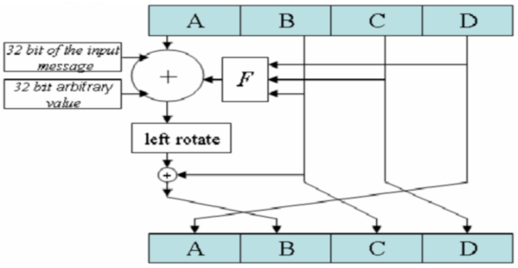

Figure 4. Flow diagram to generate hash value by MD5

The proposed system focuses on following objectives for increasing security:

1. Run the proposed system.
2. Choose and upload the desired file which you want to encrypt and store in the cloud.
3. Insert the first key for Blowfish algorithm.
4. Now implementing first level encryption. Blowfish Algorithm will be used for encryption.
5. Implementing MD5 to calculate the hash value for the first key and store it locally.
6. Insert the second key for AES algorithm.
7. Now implementing second level encryption. From the above step we get a cipher file. That file will again undergo encryption using AES algorithm.
8. Implementing MD5 to calculate the hash value for the second key and store it locally.
9. Implementing MD5 to calculate the hash value for the encrypted file and store that value locally.
10. Send and store the generated file from the above steps on the Cloud.

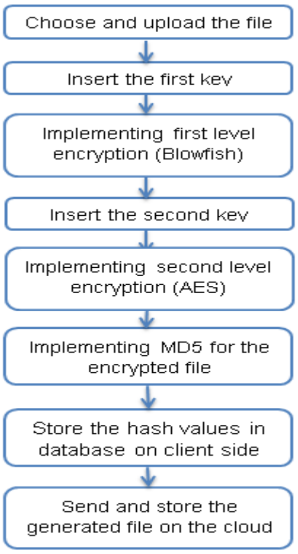
Choose and upload the file
Insert the first key
Implementing first level encryption (Blowfish)
Insert the second key
Implementing second level encryption (AES)
Implementing MD5 for the encrypted file
Store the hash values in database on client side
Send and store the generated file on the cloud

Figure 5. Flow diagram of encryption process of proposed system

For decryption: the decryption process is the same of encryption process but here it will be inversed, that means the last step in encryption will be the first step in decryption process so:

1. Choose and download the encrypted file want to decrypt from cloud.
2. Implementing MD5 to calculate the hash value for the encrypted file and compare it with the value was stored locally.
3. If the result of comparison process is false, that means the file is not integrity or damaged; but if the result of comparison process is true that means the two values are equal, the system will ask the client to enter the AES's key.
4. Implementing MD5 to calculate the hash value for the entered key and compare it with the hash value which stored locally, if equal will decrypt the first level.
5. Now implementing the first level decryption.
6. Insert the second key for Blowfish algorithm and calculate the hash value for the entered key and compare it with the hash value which stored locally. If equal will decrypt the second level.
7. Now implementing second level decryption.
8. Get the original file.

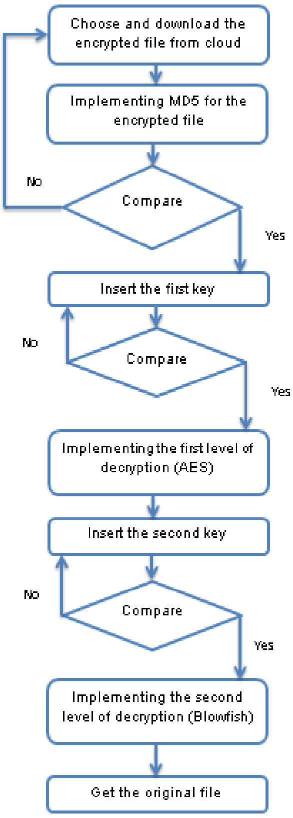
Choose and download the encrypted file from cloud
Implementing MD5 for the encrypted file
No
Compare
Yes
Insert the first key
No
Compare
Yes
Implementing the first level of decryption (AES)
Insert the second key
No
Compare
Yes
Implementing the second level of decryption (Blowfish)
Get the original file

Figure 6. . Flow diagram of decryption process of proposed system

VII. RESULTS AND ANALYSIS

The evaluation is conducted to show the efficiency and performance of the proposed framework. The proposed framework was implemented using C# and ASP.NET web forms. All experiments were conducted on an identical platform; a Windows based machine that is equipped with 4 GB of memory and an Intel(R) Celeron(R) CPU B820 @ 1.70GHz.

The proposed system results were compared to a number of symmetric encryption algorithms such as DES, 3-DES, CR6 using file sizes ranges from 1MB to 1GB. The encryption running time and throughput performance metrics are used in this evaluation.

A- *Running time:*

Figures 7a-e show the encryption running time for our proposed system compared to Blowfish, AES, RC6, DES and 3-DES encryption algorithm for files range from 1MB to 1GB. The results clearly show that the proposed system outperforms all other encryption algorithms for file sizes 1 MB to 1GB [12][13].

AES is very fast and it has very strong resistance against attacks. RC6 needs more rounds, and it uses extra multiplication operation that increases the encryption running time and less secure. DES has an S-Box structure where the encryption operation needs to use a lookup mechanism and this mechanism will lead to a slow software implementation. The 3-DES is the slowest encryption algorithm, it runs DES three times.

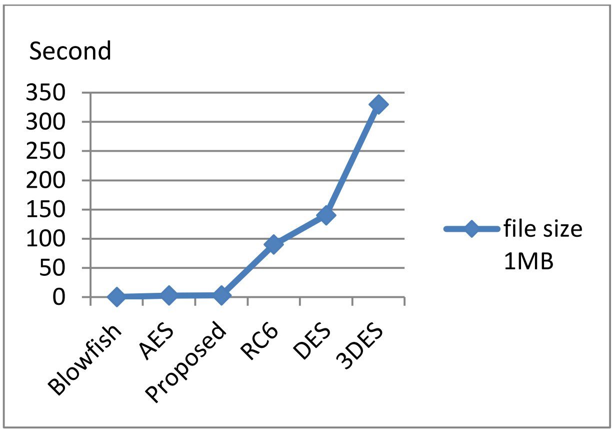

Figure 7a. Average encryption running time for file 1MB

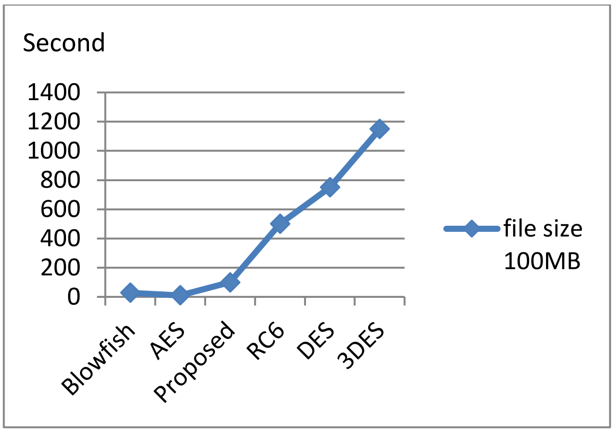

Figure 7b. Average encryption running time for file 100MB

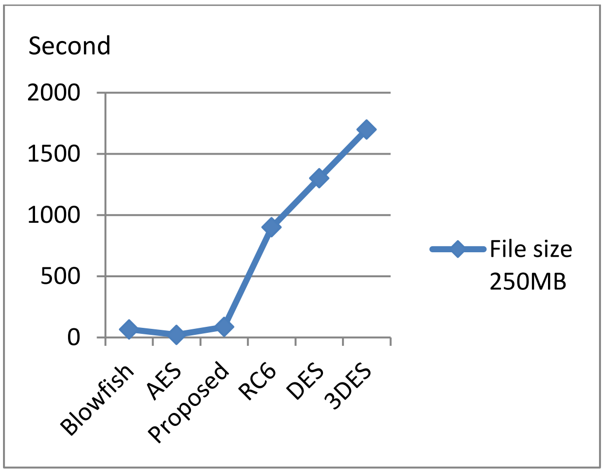

Figure 7c. Average encryption running time for file 250MB

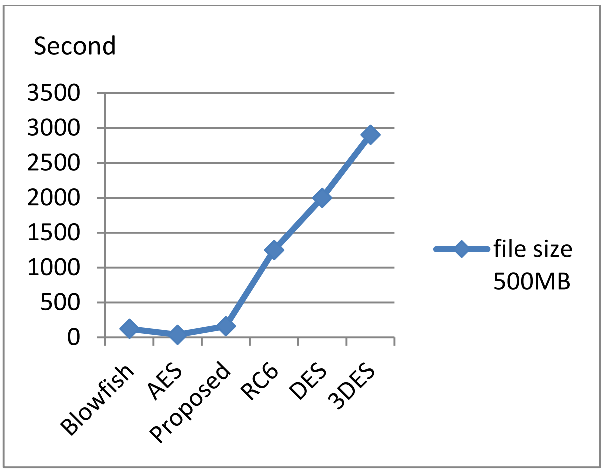

Figure 7d. Average encryption running time for file 500MB

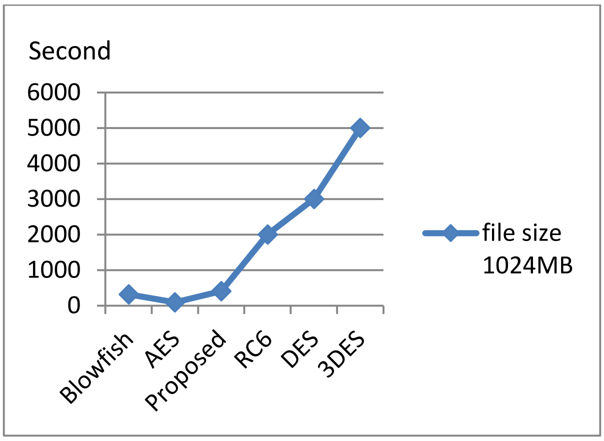

Figure 7e. Average encryption running time for file 1024MB

Figure 8 shows the average encryption running time for all ranges.

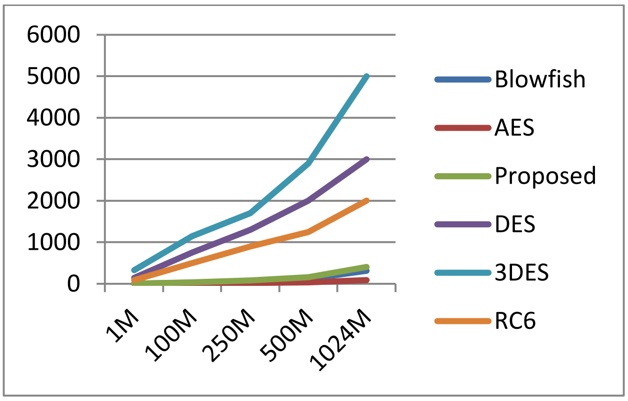

Figure 8. Average encryption running time for all ranges

B- Average throughput:

Our proposed system has the highest throughput in comparison with RC6, DES, 3-DES. Here, the results only show the encryption process since the decryption process provides almost the same results because it is just the reverse of the encryption process. Figure 9 shows the average encryption throughput [12][13].

There are two factors affect: the file size and running time. Running time: is the time that an encryption/decryption algorithm takes to produce a cipher text/plaintext from a plaintext/cipher text.

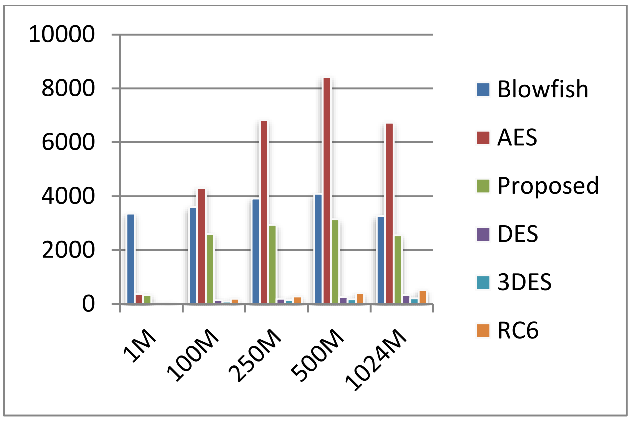

Figure 9. Average encryption throughput for all range

C- *Avalanche effect:*

In this paper we compare the Avalanche effect security metric for security evaluation.

Avalanche effect is measure the strength of the proposed algorithm against cracking and hacking threats and real time attacks such as brute force attacks. In key encryption algorithms, changing a small number of bits in plain text in order to avalanche changes in subsequent rounds resulting in a large number of cipher text bit changes. For an algorithm to satisfy the avalanche criterion, the change of one plaintext bit is expected to result in one-half of the cipher text bits changing [12][13].

The avalanche effect can be calculated as: Avalanche effect = No. of flipping bits in the cipher text / No. of bits in the cipher text * 100% for example, considering a two-byte plaintext (0100100001101011), the most significant bit is flipped (1100100001101011). After encryption, the original ciphered text is (1110101010100110) and the modified ciphered text is (1011000100000100). The Avalanche effect can be calculated by counting the number of flipped bits in the cipher text, which is 8, divided by the number of bits in the cipher text [12][13].

So, the avalanche effect is 50%. Figure 10 presents the avalanche effect for AES and other benchmark encryption algorithms (DES, 3-DES, RC6 and Blowfish). The results show that AES algorithm outperforms all other algorithms with 52.5%, Followed by Blowfish with 48.4%, CR6 46.7%, 3-DES 35.8%, and finally DES 24.2%.

The avalanche effect of our proposed system was 73.81%. From these results, it can be seen that the proposed system satisfies the avalanche effect criterion.

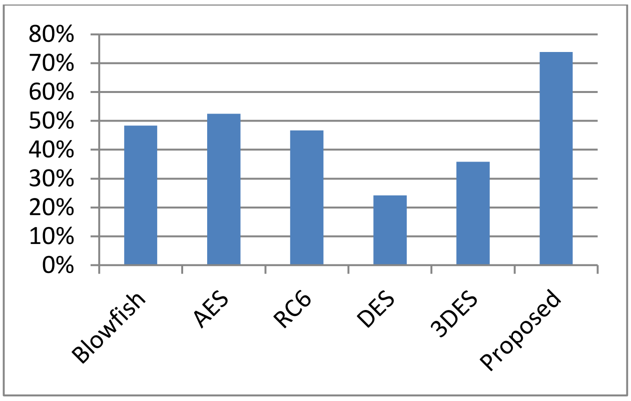

Figure 10. Avalanche effect

VIII. DISCUSSION

In reference [6] presented a hybrid approach that combines Advanced Encryption Standard (AES) to the Elliptic Curve Cryptography(ECC); where AES is considered to be simple, reliable and fast encryption algorithm for long plain texts encryption and elliptic curves are used as a digital signature. Although using AES is considered to be fast, key management and digital signature processes are encrypted using elliptic curves which are considered being complex and slow, thus adding extra overhead to the hybrid approach. There is one level of encryption which means the security depends on the stronger of the algorithm in this level. In comparison the proposed system used a hash function (MD5 algorithm) as a digital signature because it is faster and not complex.

The proposed implementation in [8] was evaluated by measuring performance metrics such as security, encryption time, avalanche effect, and throughput and found to provide a good performance but the proposed system in this paper gives better security and performance.

This paper has mentioned that the system model is similar to the one proposed by [7] with an additional security level to solve the integrity problem by saving the hash function, does not use genetic algorithms and there is no need to key exchange."

IX. CONCLUSION AND FUTURE WORK

Multi-level encryption approaches are popular because they combine the strength of many encryption techniques at the same time. In this paper, we proposed a multi-level encryption system that combines the strength of Feistel encryption by using Blowfish algorithm, AES algorithm, and MD5 algorithm. The results show that the proposed system has the lowest running time, highest throughput in comparison with CR6, DES and 3DES algorithms and passes the Avalanche effect criterion. The results showed that the proposed system is promising and encouraging in terms of the security and performance objectives. As a result, the proposed system can be use and run on any machine (PC, laptops or mobile devices) even on limited resources machines because it is so light, your data that stored in cloud will be secure, nobody can know or read the original data except the owner who has the keys, with lowest running time and highest throughput.

As a part of future work, we can use the Twofish algorithm instead of the Blowfish algorithm. Blowfish algorithm has weakness in the decryption process over other algorithms in terms of time consumption and serially in throughput. However, it should be noted that the efficiency of the Twofish algorithm depends on the parameter of the experimental computer memory (RAM) in addition to the used plaintext size.

REFERENCES

1. Verma, Om Prakash, et al. "*Notice of Violation of IEEE Publication Principles: Performance analysis of data encryption algorithms*." 2011 3rd International Conference on Electronics Computer Technology. Vol. 5. IEEE, 2011.
2. Dillon, Tharam, Chen Wu, and Elizabeth Chang. "*Cloud computing: issues and challenges*." *2010 24th IEEE international conference on advanced information networking and applications*. Ieee, 2010.
3. Sen, Jaydip. "*Security and privacy issues in cloud computing.*" *Cloud technology: concepts, methodologies, tools, and applications*. IGI global, 2015. 1585-1630.
4. Chou, Te-Shun. "*Security threats on cloud computing vulnerabilities*." *International Journal of Computer Science & Information Technology* 5.3 (2013): 79.
5. Delfs, Hans, Helmut Knebl, and Helmut Knebl. *Introduction to cryptography*. Vol. 2. Heidelberg: Springer, 2002.
6. Xin, Mingyuan. "*A mixed encryption algorithm used in internet of things security transmission system*." *2015 international conference on cyber-enabled distributed computing and knowledge discovery*. IEEE, 2015.
7. Aljawarneh, Shadi, and Muneer Bani Yassein. "*A resource-efficient encryption algorithm for multimedia big data*." *Multimedia Tools and Applications* 76.21 (2017): 22703-22724.
8. Prasetyo, Kurniawan Nur, Yudha Purwanto, and Denny Darlis. "*An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA*." *2014 2nd international conference on information and communication technology (ICoICT)*. IEEE, 2014.
9. Chatterjee, Swagata Roy, et al. "*FPGA implementation of pipelined blowfish algorithm." 2014 Fifth International Symposium on Electronic System Design*. IEEE, 2014.
10. Li, H. "*Efficient and flexible architecture for AES*." *IEE Proceedings-Circuits, Devices and Systems* 153.6 (2006): 533-538.
11. Gupta, Surbhi, Neha Goyal, and Kirti Aggarwal. "*A review of comparative study of md5 and ssh security algorithm*." *International Journal of Computer Applications* 104.14 (2014).
12. Habboush, Ahmad. "*Multi-level encryption framework." (IJACSA) Int. J. Adv. Comput. Sci. Appl.* 9.4 (2018): 130-134.
13. Aljawarneh, Shadi, and Muneer Bani Yassein. "*A resource-efficient encryption algorithm for multimedia big data.*" *Multimedia Tools and Applications* 76.21 (2017): 22703-22724