Resource Sharing Security in Cloud Computing Environment

Diaa Salama AbdElminaam[1], Yaser Maher Wazery[2]
1Information Systems department, Faculty of Computers and Informatics, Benha University, Egypt
[2]Information Technology department, Faculty of Computers and Informatics, Minia University, Egypt

Abstract: *Although Cloud Computing is a great innovation in the world of computing, there also exist downsides of cloud computing. These most important challenges are Security & Privacy of data on the cloud, check availability of data on the cloud. For these problems, Data storage security refers to the security of data on the storage media. Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. The third party must not be stealing Data so authentication of client becomes a mandatory task. Security is very essential for applications where the sensitive data is transmitted. On the other hand, the encryption methods with minimal key size and minimal computations have to be selected as energy efficiency is also limitation of mobile applications. Therefore, there is a great need of encryption method with high levels of security and with minimal key size. Traditional Symmetric or Asymmetric encryption algorithms can be used for cloud computing to provide three cryptographic primitives, integrity, confidentiality and authentication.*

There are many drawbacks for Symmetric encryption algorithms such as key maintenance is a great problem faced in symmetric encryption methods and less security, level is the problem of asymmetric encryption methods even though key maintenance is easy. And there are many drawbacks of Asymmetric encryption algorithms such as those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. There for, the main target for ensuring security is to developed new hybrid cryptography protocol. This new security protocol using combination of both symmetric and asymmetric cryptographic techniques is proposed by merging both symmetric and asymmetric techniques by a way that avoids the disadvantages of the existing hybrid protocols. We developed Five new hybrid cryptography protocol for achieving security in Mobile Cloud Computing. In proposed protocol the plain text divided into two parties, the first part is encrypted using encryption scheme and the second part encrypted using anther encryption scheme. These two schemes have occurred simultaneously so that the time required making encryption to all plain text is small because two schemes done in parallel way. We can obtain much security with a little time in this proposed protocol. The Proposed protocol has been proposed to achieve the security services such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability. The results show the superiority of NHCP algorithms over other algorithms in terms of the encryption and decryption time, processing time, and throughput

Keywords: *Encryption Algorithms, Cloud Security, Data Security, Information Security, Mobile cloud computing.*

Received August 31, 2017; Accepted November 5, 2017

1. Introduction

The chosen topic areas for this research consist of an overlap of three new growing information technology areas. The First area is cloud Computing (CC), the second area is Smartphone and mobile computing, the third area is cryptography and network security.

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Cloud computing is also called distributed computing over the network i.e. the ability to execute an application or a program on many computers at the same time. Cloud services provides software and hardware which from remote locations which are managed by third party to the individual or businesses [19, 21].

The objectives of cloud computing are to increase capacity and capabilities at runtime without investing in new infrastructure, licensing new software, and training new recruits. The services may be Infrastructure as a Service (IaaS), Data storage as a Service (DaaS), Hardware as a Service (HaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). There are many benefits of cloud computing such as it can be less expensive compared to buying software and hardware, it can be used from any computer or device with an Internet connection, the device does not need as large of an internal storage system, Compatible with most computers and operating systems, Updates occur across the service [3, 8].

On the other side, Data security is becoming a fundamental obstruction in cloud computing. There are some kinds of solution that are providing some security with model, some technology. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard

drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications[1,6].

Also, Mobile devices (e.g., smartphone, tablet pcs, etc.) are increasingly becoming an essential part of human life, Dream of "Information at your fingertips anywhere anytime". These Mobile devices still lack in resources compared to a conventional information-processing device such as PCs and laptops. The solution to overcome of these challenges is Mobile Cloud Computing (MCC). Mobile cloud computing is the cloud infrastructure where the computation and storage are moved away from mobile devices [23, 27].

1.1. Existing Cryptography Algorithms

Developed authentication protocols are based on cryptographic algorithms. Encoding the contents of a message in such a way that hides its content from outsiders is called Encryption. Then encrypted message is called cipher text. The process of retrieving the plain text from the cipher text is called Decryption. Encryption and Decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.
Many encryption algorithms are widely available and used in information security and can be categorized into Symmetric(private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data.

In a symmetric cryptosystem, the encryption and decryption algorithms use the same key and in an asymmetric cryptosystem, the encryption and decryption used two different keys: encryption key and a decryption key.

In an asymmetric cryptosystem, the encryption key is public and decryption key is a private key.

Asymmetric key encryption is used to solve the problem of key distribution where Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA and ECC). Asymmetric key encryption is based on mathematical functions, and is not very efficient for small mobile devices. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power . Strength of Symmetric key encryption depends on the size of the key used. A cryptosystem is a system consisting of two entities: the former contains an Encryption Algorithm and the latter - a Decryption Algorithm.

A cryptosystem can be formalized as five-parameters (P,C,K,E,D) where:

- P is a finite set of plain texts,
- C is a finite set of cipher texts, and K is a finite set of keys.
- E is a set of encryption algorithms;
- D is a set of decryption algorithms.
- For each key k, there is an encryption algorithm and a decryption algorithm.
- The encryption and decryption algorithms are functions ek : p→ C and dk : p→ C with the following
- Property dk (ek (P)) = P for every plaintext P.

Cryptographic techniques enable its users to transmit information in a secure way over insecure communication media. The objectives of the cryptography regarding the security of the information are: confidentiality, authentication, integrity and non-repudiation.

Confidentiality assures the secret of the information. Even if unauthorized users intercept it, the Information is encrypted, so that these users cannot understand the message. Authentication implies entities' identification. The authentication procedures make sure that both the transmitter and the receiver are the right entities. Integrity assures that the message has not suffered any unwanted modification (altered or corrupted). Non-repudiation means that a part of the system cannot deny previously occurred events that triggered the message. Without this property, a receiver might declare that the message was not received.

The most popular secret key algorithms are based on the Feistel Cipher Structure. Encryption schemes like DES, 3DES, AES, Blowfish, and RC6 use different kinds of transformation and rounds to achieve confusion and diffusion. The public key scheme offered an elegant solution to the key distribution and authentication problems while using secret key mechanisms. Public key schemes are asymmetric involving the use of different keys for encryption and decryption process. The popular schemes that use these methods are RSA, ElGamal and ECC respectively.

The remainder of the paper is structured as follows: An overview of related work related to our subject is presented in section number two. In section number three, the materials and methods for the presented developed system are explained. In section number four, results and discussions are produced, before drawing conclusions and future work in section number five and six.

2. Related Work

To give more prospective about the Mobile Cloud Computing, and Security on mobile cloud computing, this section discusses the results obtained from other resources. Much of it investigates the possibility to offload mobile phone functions into the cloud

AlfredO [14] is a middleware platform to automatically distribute different layers of application in smartphones and cloud, respectively, by modeling

applications as a consumption graph, and finding the optimal modules. The test result shows that such platform improves the performance of applications in cloud computing effectively. AlfredO system consists of three bundles (the interface encapsulation on Java classes and services)

It was investigated in [22] the importance of mobile phones in collaboration with cloud computing. The computational power of the mobile phone is stated to be the chief limitation of the mobile phone. This constraint makes it desirable to offload computational tasks to the cloud where the resources are "unlimited". But there are also problems related to the connection between the mobile phone and the cloud in forms of latency, connection interruption and network provider costs that needs to be considered.

It was investigated in [12] which parts of mobile phones are consuming most energy by measuring the different parts of a mobile phone while it was operating. The result shows that data transmission, phone calls and the display are the parts that use most energy. To send and receive data from the cloud is therefore a very energy-consuming task in comparison to other mobile phone related functions.

YFR Security Protocol Architecture

In [10] (YFR Security Protocol Architecture) The plaintext is divided into two blocks. The first n/2 blocks are encrypted using (AES and ECC) . In parallel, the remaining n/2 blocks are encrypted using XOR-DUAL RSA algorithm. Then hashing each two, half-using MD5. In the Decryption Phase: The decryption phases the cipher text is divided into two parts ci blocks and Ci blocks. Hashing is used to identify whether the source node receive the same cipher text or not. In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using AES and ECC algorithms. The remaining n/2 blocks are decrypted using XNOR-DUAL RSA algorithm.

Debabrata et al., [26] systematically explored the security issues, privacy and launch a cryptography-based model for handling multiple request from multiple devices for MCC. Their approach helps to authenticate communication between customers and service providers using encryption, decryption and message digests.

Gill et al., [24] provided the extensive survey on the various energy efficient frameworks available to offload the computation from the mobile to the cloud environment. The principal objective of all these frameworks is energy saving which is most essential requirement of SMDs. The limitations of SMDs like slow execution speed, low processing and less battery life can be addressed by offloading the energy intensive components of mobile applications to the cloud environment. The frameworks are classified based on the offloading decision taken i.e. static or dynamic, the core component used in framework which facilitates offloading, the various parameters which are analyzed before or during offloading and various real-life applications that can run on these frameworks.

Patil et al., [24] presented insignificant Cloud-based storage framework. This framework provided an easy-to-use file navigation service for attribute-based file querying. Simultaneously, it incorporates an effective structure for users to verify their data integrity, which can relieve much load from mobile devices. Experimental simulations show that the proposed framework is effective to provide flexible data sharing in mobile computing environments

Alotaibi et al., [11] investigated the factors related to the selection of SaaS. The research depends on developing an updated model based on the UTAUT. The suggested model offers a complete explanation for software as a services adoption behavior, by making QoS as the main antecedent of BI, according to its role in services held online. Besides, education was included in the model as a moderating factor to fit SaaS context adoption in developing countries. The model was revised to examine using empirical data collected by questionnaire.

Researchers recognized in literature like [9], [4], [15] and [18] evaluated a related analysis of encryption algorithms like DES, AES, Blowfish, RC2, 3DES, and RC6 for data transmission by using the time for encryption, the usages of the memory output byte and power of the battery. The evaluation also studied the performance of chosen symmetric key algorithms. In [28], and [20] developers studied security threats, main common attacks, and many security methods that protect the user from attacks, and intrusions. In [2] devolves new hybrid cryptography algorithm and compare it with different hybrid cryptography algorithms according to power consumption, Encryption time, and throughput.

3. The Proposed Hybrid Cryptography Algorithms

The proposed hybrid cryptography algorithm developed to secure the data and information which is transmitted through the cloud. The aim of the hybrid cryptography algorithm is to efficiently encrypt and secure the transmitted data. Eight encryption algorithms were implemented in the proposed hybrid cryptography algorithm. Five of these algorithms are hybrid and implemented to improve the efficiency of the encryption algorithm time and security. Using the hybrid algorithms improves the security of the encryption algorithms since that the data is encrypted using more than one algorithm and at the same time minimize the time taken by the algorithms that takes much time to encrypt the data. Figure 1 shows structure of the developed system.

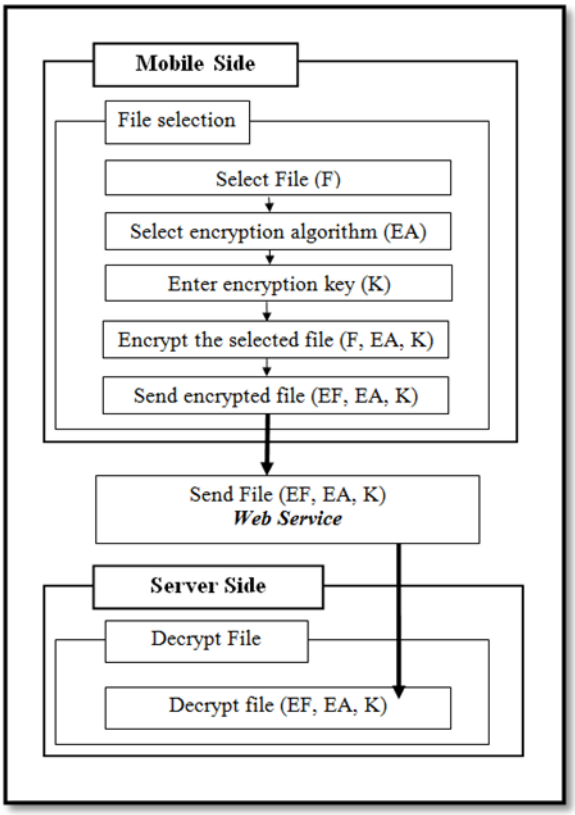

Figure 1. System structure.

The proposed new security protocols using combination of both symmetric and asymmetric cryptographic techniques is proposed. This protocol provides three cryptographic primitives, integrity, confidentiality and authentication. It is a hybrid encryption method where RSA , Krisha , AES , DES , 3DES are combined to provide new cryptography algorithms .

Algorithm for Enryption:

Mobile side

1. Select file (F)
2. Select the encryption algorithm (EA)
3. Enter encryption key (K)
4. Encrypt (F, EA, K)
5. Send encrypted file (EF, EA, K)

Server Side

Data should be store

For Decryption

1. Received encrypted file from server (EF)
2. Select the encryption algorithm (EA)
3. Enter encryption key (K)
4. Encrypt (EF, EA, K)
5. Send encrypted file (F)

The proposed hybrid cryptography algorithm offer set of encryption algorithms:

1. Hybrid encryption algorithm using Krishna and Triple DES algorithms.
2. Hybrid encryption algorithm using Krishna and AES algorithms.
3. Hybrid encryption algorithm using Krishna and Blowfish algorithms.
4. Hybrid encryption algorithm using RSA and Triple DES algorithms.
5. Hybrid encryption algorithm Krishna and AES and Blowfish algorithms.

The aim of the proposed hybrid cryptography algorithm is to determine the fastest and secure encryption algorithm of the previously presented encryption algorithms. It also allows the user to choose the encryption algorithm which is more suitable for the type of his own data. Also, the hybrid cryptography algorithm implements several encryption algorithms and allow the user to use them to encrypt his own data these algorithms are:

1. AES
2. Blowfish

In Krishna algorithm, several steps have to be done to encrypt and decrypt the text. To encrypt the text the algorithm will work as follow:

1. In the Text, each letter is treated as a digit in base 26
2. A block of n letters is considered as a vector of n dimensions.
3. Multiply the vector by a n × n matrix (Key).
4. Get the modulo 26 of the resulted matrix.

In order to decrypt, we turn the cipher-text back into a vector, then simply multiply by the inverse matrix of the key matrix.

3.1. First Hybrid encryption algorithm using (Krishna and Triple DES algorithms).

Figure 2, Figure 3, and Figure 4 show how the system encrypt and decrypt the data using the Krishna encryption algorithm and Triple DES encryption algorithm.

The system allows the user to select the encryption algorithm which is more suitable for the type of his own data. Also, it determines the fastest and secure encryption algorithm of the previous encryption algorithms that help in securing the transmitted data from mobile to cloud with a minimum time.

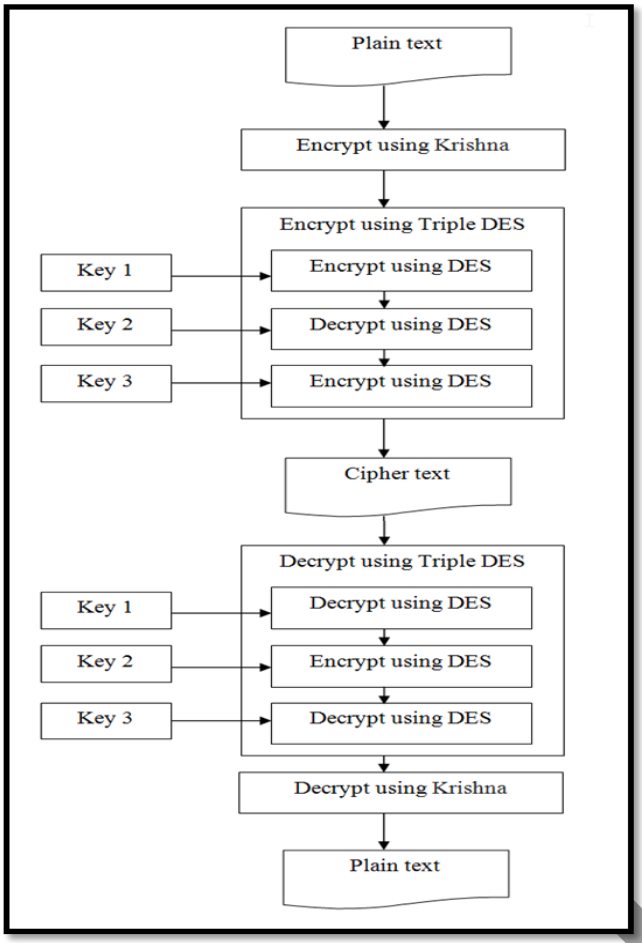

Figure 2. Hybrid encryption algorithm using Krishna and Triple DES algorithms.

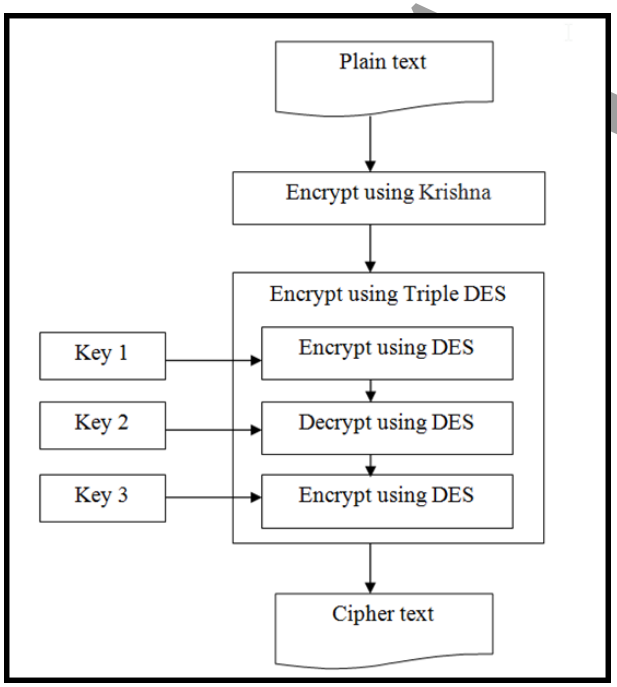

Figure 3. Encryption phase of Hybrid encryption algorithm using Krishna and Triple DES

Algorithm for encryption:

1. plain text file(F)
2. Krishna is used to encrypt a file (F) resulting in (C1k)
3. Triple DES key1 is used to encrypt a (C1k) resulting in (C2ktd1)
4. Triple DES key2 is used to decrypt (C2ktd1) resulting in (C3ktd2)
5. Triple DES key3 is used to encrypt (C3ktd2) resulting in (C4ktd3)

Final Cipher text C4ktd3 is the Cipher text resulting from encryption using Krishna and Triple DES algorithms

Where: C1k is the cipher text resulting from encrypts file (F) using Krishna, C2ktd1 is the second cipher text resulting from encrypting C1k using Triple DES key1, C3ktd2 is the third cipher text resulting from decrypting C2ktd1 using Triple DES key2, and C4ktd3 is the final cipher text resulting from encrypting C3ktd2 using Triple DES key3 and also is the final cipher text resulting from encrypting file (F) using Krishna , and Triple DES algorithms.

Algorithm for decryption:

1. Cipher text (C4ktd3).
2. Triple DES key3 is used to decrypt (C4ktd3) resulting in (C3ktd2)
3. Triple DES key2 is used to encrypt (C3ktd2) resulting in (C2ktd1)
4. Triple DES key1 is used to decrypt (C2ktd1) resulting in (C1k)
5. Krishna is used to decrypt a file (C1k) resulting in (F)
6. F is the Final File.

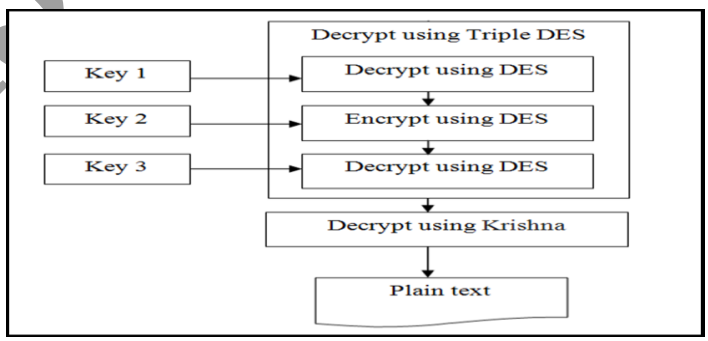

Figure 4. Decryption using Hybrid encryption algorithm using Krishna and Triple DES.

3.2. Second Hybrid Encryption Algorithm Using (Krishna and AES Algorithms)

Figure 5, Figure 6 show how the system encrypts and decrypt the data using the Krishna encryption algorithm and AES encryption algorithm.

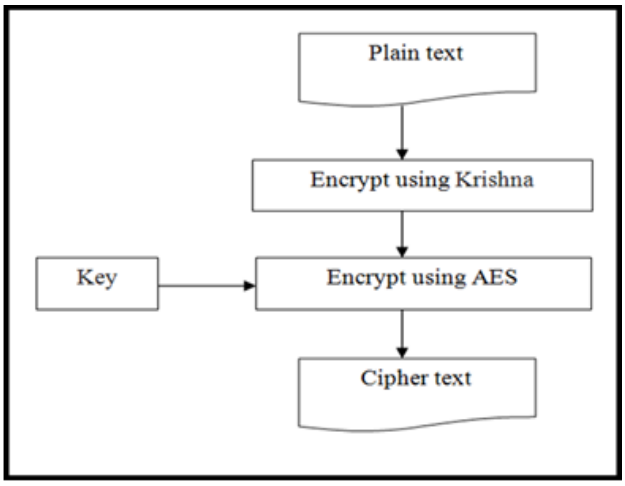

Figure 5. Encryption phase of Hybrid encryption algorithm using Krishna and AES algorithms

Algorithm for encryption:

1. plain text file(F).
2. Krishna is used to encrypt a file (F) resulting in (C1k).
3. AES is used to encrypt (C1k) resulting in (C2kA).
4. C2kA is Final cipher.

Algorithm for decryption:

1. Cipher text (C2kA).
2. AES key is used to decrypt (C2kA) resulting in (C1k)
3. Krishna is used to decrypt (C1k) resulting in (F)
4. F is the Final File.

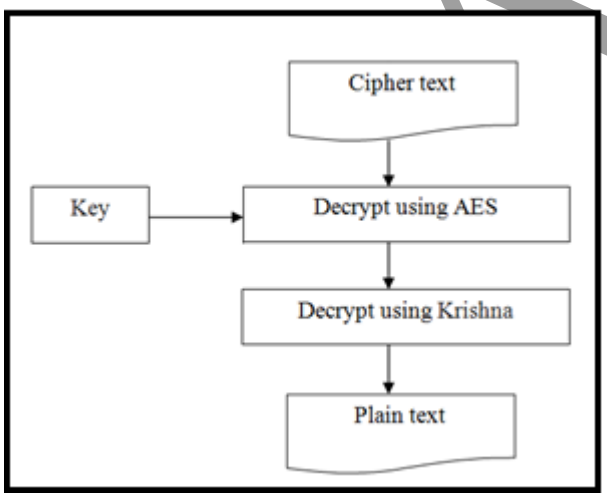

Figure 6. Decryption using Hybrid algorithm Krishna and AES algorithms.

3.3. Third Hybrid encryption algorithm using (Krishna and Blowfish algorithms)

Figure 7, Figure 8 show how the system encrypt and decrypt the data using the Krishna encryption algorithm and Blowfish encryption algorithm

Algorithm for encryption:

1. plain text file(F).
2. Krishna is used to encrypt a file (F) resulting in (C1k).
3. Blowfish is used to encrypt (C1k) resulting in (C2kB).

C2kB is Final cipher.

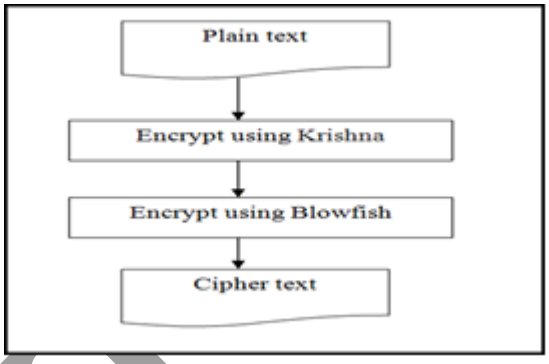

Figure 7. Hybrid encryption algorithm using Krishna and Blowfish algorithms.

Algorithm for decryption:

1. Cipher text (C2kB).
2. Blowfish key is used to decrypt (C2kB) resulting in (C1k)
3. Krishna is used to decrypt (C1k) resulting in (F)
4. F is the Final File.

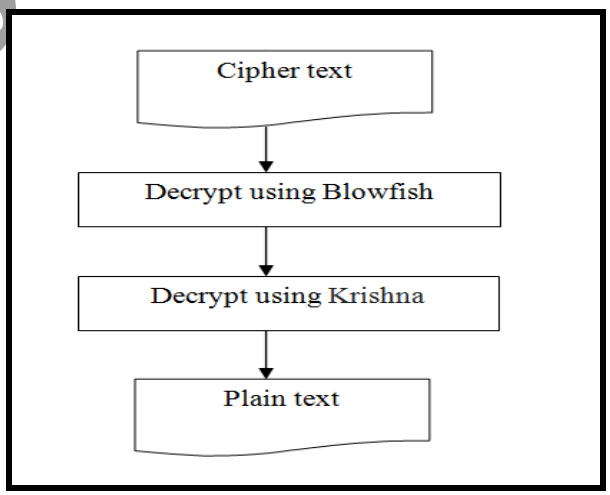

Figure 8. Decryption using Hybrid encryption algorithm using Krishna and Blowfish algorithms.

3.4. Fourth Hybrid encryption algorithm using (using the RSA encryption algorithm and Triple DES encryption algorithm)

Figure 9 and Figure 10 show how the system encrypts and decrypt the data using the RSA encryption algorithm and Triple DES encryption algorithm.

Algorithm for encryption:

1. plain text file(F).
2. Triple DES key1 is used to encrypt a (F) resulting in (C1t).
3. Triple DES key2 is used to decrypt (C1t) resulting in (C2t).
4. Triple DES key3 is used to encrypt (C2t) resulting in (C3t).
5. RSA is used to encrypt (C3t) resulting (C4tR).
6. C4tR is Final cipher.

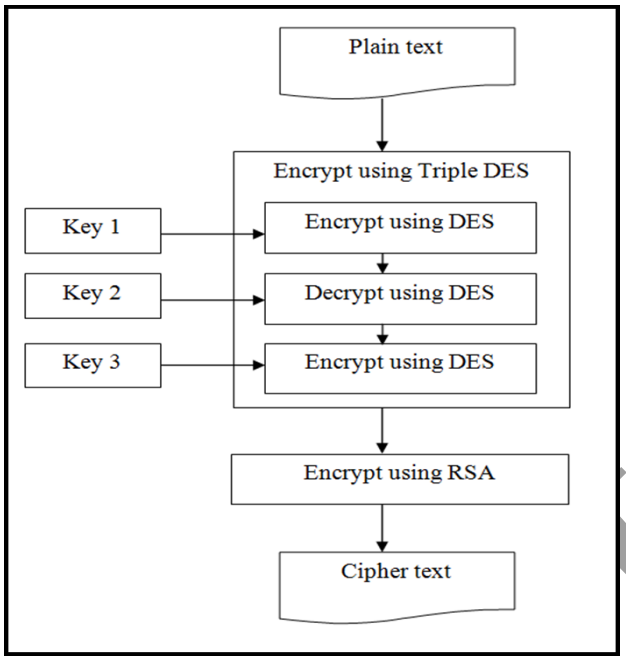

Figure 9. Hybrid encryption algorithm using RSA and Triple DES.

Algorithm for decryption*:*

1. Cipher text (C4tR).
2. RSA is used to decrypt (C4tR) resulting in (C3t).
3. Triple DES key3 is used to decrypt (C3t) resulting in (C2t).
4. Triple DES key2 is used to encrypt (C2t) resulting in (C1t).
5. Triple DES key1 is used to decrypt (C1t) resulting in (F).

F is the Final File

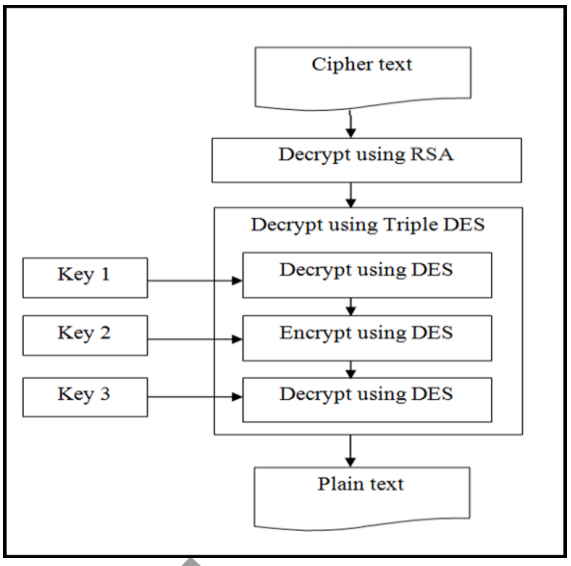

Figure 10. Decryption using Hybrid encryption algorithm RSA and Triple DES

3.5 Fifth Hybrid encryption algorithm

Figure 11, shows how the system encrypts the data using the Krishna encryption algorithm, AES encryption algorithm, and Blowfish encryption algorithm. In this algorithm, the system divides the plain text into two parts. The first part was encrypted and decrypted using Krishna encryption algorithm and AES encryption algorithm. The second part was encrypted and decrypted using Krishna encryption algorithm and Blowfish encryption algorithm.

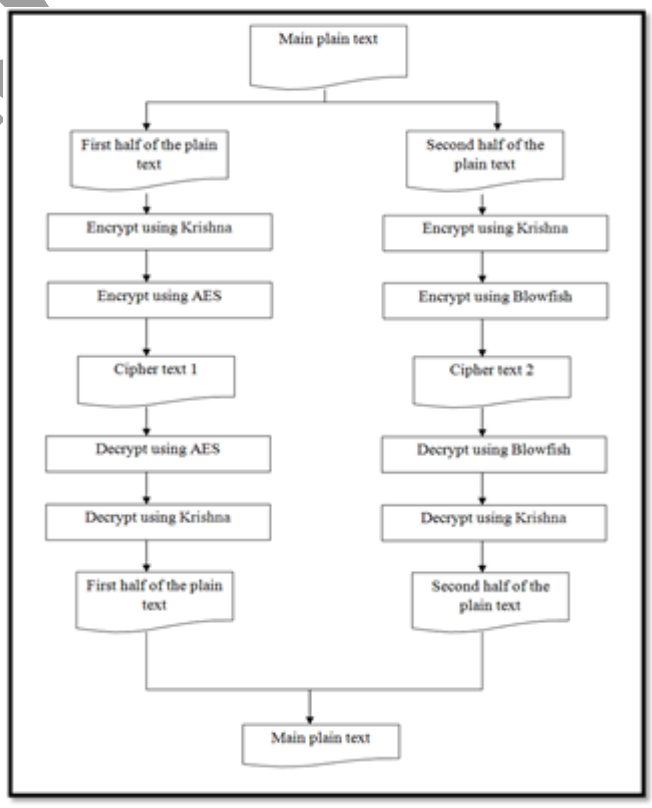

Figure 11. Hybrid encryption algorithm Krishna, AES and Blowfish algorithms.

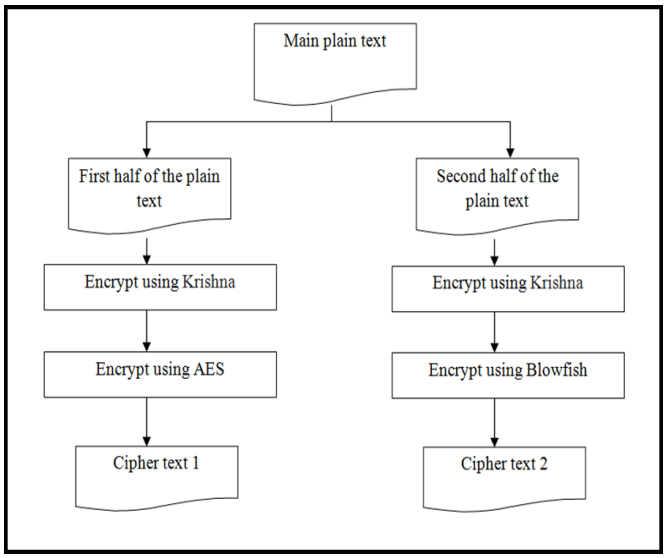

Figure 12. Decryption using Hybrid encryption algorithm Krishna, AES and Blowfish algorithms.

4. Results and discussion

Extensive experiments are preformed to study the efficiency of the implemented hybrid cryptography algorithm encrypt and decrypt data in a minimum time. The hybrid cryptography algorithm was tested on different file sizes. The system runs 50 times for each file size to calculate the average time for each encryption algorithm. Table.1 shows the time consumed in encrypting data using the eight algorithms.

Table 1. The time consumed in encrypting data for each algorithm.

File size / Algorithm	250 KB	500 KB	750 KB	1 MB	1.25 MB	1.5 MB	1.75 MB	2 MB	2.25 MB	2. 5 MB	2.75 MB	3 MB	3.25 MB	3. 5 MB
Triple DES & Krishna	0.7	0.8	2.2	3.1	4.3	5.7	6.4	7.1	9	10.9	12.3	13.4	14.7	15.3
AES & Krishna	.6	1.1	1.7	3.4	4.2	7.1	8.5	12.3	16.8	18.9	20.5	23.7	25.2	29.6
Blowfish & Krishna	2.3	4.9	6.4	9.2	12.3	13.6	15.5	18.6	20.1	23.2	27.8	29.6	32.9	36.7
Triple DES & RSA	2.7	4.5	6.8	8.5	11.3	15.5	19.4	20.8	23.7	25.8	27.4	31.6	33.4	34.4
AES & Blowfish & Krishna	2.8	4.0	4.3	6.9	8.9	10.4	13.1	15.9	17	19.4	22.1	24.9	27.6	30.3
AES	0.6	1.2	1.8	2.4	3.3	4.2	5.8	6.9	7.3	8.7	9.9	11.5	13.6	15.9
Blowfish	2.4	5.1	8.4	11.9	14.2	17.9	21.4	24.3	26.2	29.5	31.8	35.7	39.1	42.4

As shown in Table.1, and Figure.13 the proposed hybrid cryptography algorithm allows the user to encrypt his data with hybrid encryption algorithms that uses two strong encryption algorithms without taking large time in encrypting data. For example, encrypting a file with 1 MB using Blowfish algorithm takes 11.99 seconds and at the same time encrypting the same file using Blowfish and Krishna takes 9,28 seconds. This is because at the second algorithm the plain text was encrypted using Krishna algorithm at the first then the cipher text was re-encrypted using Blowfish algorithm and because that Krishna minimize the size of the plain text in on word the size of the cipher text sent to Blowfish will be small and the algorithm will take minimum time to encrypt it. Table .2 and Figure 14 illustrate the throughput of the algorithms. Throughput was calculated by dividing the size of the file in bytes over the consumed time in seconds. The throughput was calculated using the following equation:

$$\text{Throughput} = \frac{\text{File size}}{\text{Encryption time}} \quad (1)$$

Table 2. The throughput for each algorithm.

File size / Algorithm	250 kb	500 kb	750 kb	1MB
Triple DES & Krishna	328947.36	595238.09	337837.83	327156.54
AES & Krishna	412903.23	435744.68	432919.95	300193.52
Blowfish & Krishna	110678.77	103038.84	11864.66	112968.75
Triple DES & RSA	90252.70	109649.12	112275.44	120046.89
AES & Blowfish & Krishna	89074.46	126482.21	175824.17	150484.50

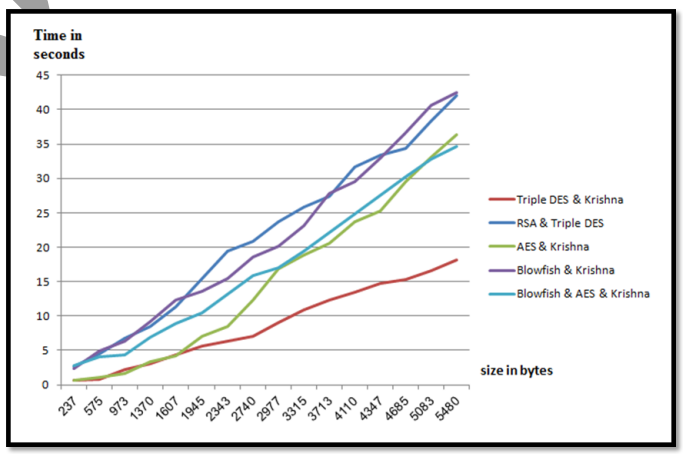

Figure 13. The time consumed in encrypting data for each algorithm.

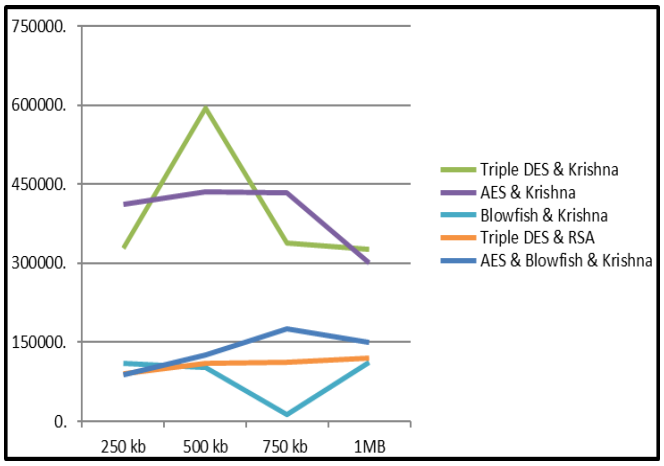

Figure 14. The throughput for each algorithm.

5. Conclusions and Future Works

In this paper, we building a system that encrypts data transferred from the mobile cloud from a mobile phone to a cloud using five hybrid encryption methods. The system presents a variety of different cryptographic algorithms that allow the cloud user to determine which encryption model is proper for his cloud mobile data. The system improves mobile encryption performance of data cloud sent from mobile to cloud since it encrypts data in minimum time and in a secure manner. Also, the system reduces the time it takes to decrypt cloud mobile data in the server. The proposed system allows users to send and receive data between mobile and cloud in a secure manner without facing the problem of data attack. The proposed system demonstrates that the use of hybrid algorithms increases the level of encryption of encrypted mobile data and also reduces the time required for encryption and decryption.

The five a hybrid cryptography algorithm that efficiently encrypt the transmitted data through the cloud. Firstly, our hybrid cryptography algorithm presents a variety of different encrypting algorithms that allow the user to choose the encrypting method which is suitable with his own type of data. Secondly, the hybrid cryptography algorithm improves the performance of the encryption algorithms since it encrypts the data in a minimum time and in a secure way. Thirdly, the proposed hybrid cryptography algorithm allows the users to send and receive data in a secure way without facing the problem of attacking data. Fourthly, the encryption times for encrypting a file with a size 1 MB using difference hybrid algorithms come in the following ascending order: using Triple DES & Krishna hybrid algorithm takes 3.13 seconds, using AES & Krishna hybrid algorithm takes 3.493 seconds, using Triple DES & RSA hybrid algorithm takes 8.53 seconds and using Blowfish and Krishna hybrid algorithm takes 9,28 seconds. Fifthly, the proposed hybrid cryptography algorithm proves that merging the three encrypting algorithms AES, Blowfish and Krishna to have AES & Blowfish & Krishna hybrid algorithm increases the security level and also saves the encryption time, so we can encrypt a file with a size 1 MB using AES & Blowfish & Krishna hybrid algorithm in 6.968 seconds. Sixthly, after calculating the throughput for all hybrid algorithms on a file with a size 1 MB, the Triple DES & Krishna hybrid algorithm shows the largest value for the throughput and on the other side the Blowfish & Krishna hybrid algorithm shows the lowest value for the throughput. Lastly, the proposed hybrid cryptography algorithm proves that using hybrid algorithms increase the level of securing the encrypted transmitted data and also minimize the time taken to encrypt it. As a future work, new hybrid algorithms will be constructed from different existence algorithms to improve the encryption process and compare it with the results of our current work

References

[1] Abdul.Elminaam D., Abdul kader H., Hadhoud M. ,Elslayed S. , "Mobile Cloud Computing Framework for Elastic Partitioned/ Modularized Applications Mobility". International Journal of Electronics and Information Engineering, vol.1, no.2, pp.1-12, 2014

[2] Abdul.Elminaam D., Abdul kader H., Hadhoud M., Elsayed S., "Developing and Evaluation of New Hybrid Encryption Algorithm". *International Journal Of Computers & Technology* , vol.13, no.1, pp. 4038-4052, 2014.

[3] Abdul.Elminaam D., Abdul kader H., Hadhoud M., Elsayed S., "GPS Test Performance: Elastic Execution Applications between Mobile Device and Cloud to Reduce Power Consumption". *International Journal of Computer Science and Network Security*, vol.13, no.12, pp. 6-13, 2013.

[4] Abdul.Elminaam D., Abdul kader H., Hadhoud M.," Wireless Network Security Still Has no Clothes" , *International Arab Journal of e-Technology*, vol. 2, no.2, pp. 112-123, 2011.

[5] Abdul.Elminaam D., Abdul kade H., Hadhoud M., Elsayed S., "Increase the Performance of Mobile Smartphones using Partition and Migration of Mobile Applications to Cloud Computing", *International Journal of Electronics and Information Engineering*, vol.1, no.1, pp..34-44, 2014

[6] Abdul.Elminaam D., Abdul kader H., Hadhoud M., Elsayed S., "Elastic framework for augmenting the performance of mobile applications using cloud computing", *The 9th International Computer Engineering Conference* pp. 134-141, Cairo-Egypt, 2013.

[7] Abolfazli S., Sanaei Z., Ahmed E., Gani A., Rajkumar Buyya, "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies,

and Open Challenges". *IEEE Communications Surveys & Tutorials*. vol. 16, no. 1, pp. 1–32, 2013.

[8] Abolfazli S., Sanaei Z., Gani A., Xia F.., Yang L., "Rich Mobile Applications: Genesis, taxonomy, and open issues". *Journal of Network and Computer Applications*, vol. 40, pp. 345–362, 2014.

[9] Ali M., Dhamotharan R. , Khan E., Khan S., Vasilakos A., Li K., Zomaya A., " SeDaSC: Secure Data Sharing in Clouds " , *IEEE Systems Journal*, vol. 11,no. 2, pp. 395 – 404, 2017.

[10] Alkady Y., Habib M.; Rizk R., "A new security protocol using hybrid cryptography," *In Proceedings of the 9th International Conference Computer Engineering Conference (ICENCO 9th International*, Giza, Egypt, pp. 109-115 , 2013.

[11] Alotaibi, M., "Antecedents of software-as-a-service (SaaS) adoption: a structural equation model." *International Journal of Advanced Computer Research*, vol. 6, no. 25, pp. 114-129, 2016.

[12] Carroll A. and Heiser G. , "An Analysis of Power Consumption in a Smartphone.", *In USENIX Annual Technical Conference*, Boston, MA, pp. 271-285, 2010.

[13] Dinh H., Lee C., Niyato D., Wang P., "A survey of mobile cloud computing: architecture, applications, and approaches". *Wireless Communications and Mobile Computing*, vol. 13, pp. 1587–1611, 2013.

[14] Giurgiu L., Riva O., Juric D., Krivulev I., Alonso G., "Calling the cloud: enabling mobile phones as interfaces to cloud applications," *Middleware*, Springer, pp. 83-102, 2009

[15] Gurjeet Singh, "Security Threats and Maintenance in Mobile ad hoc networks", *IJECT*, vol.2, no. 3, 2011.

[16] Khan A., Othman M., Madan, S., Khan S., "A Survey of Mobile Cloud Computing Application Models", *IEEE Communications Surveys Tutorials*. vol. 16, no. 1, pp 393–413, 2014.

[17] Khan A., Othman M.; Xia F, Khan A., "Context-Aware Mobile Cloud Computing and Its Challenges", *IEEE Cloud Computing*, vol. 2, no. 3, pp. 42–49, 2015.

[18] Li W.and Joshi A., "Security Issues in Mobile Ad hoc Networks - (A Survey)", *The 17 th White House Papers Graduate Research In Informatics at Sussex*, 2004.

[19] Liu F., Shu P., Jin H., Ding L., Yu J., Niu D., Li B., "Gearing Resource-Poor Mobile Devices with Powerful Clouds: Architecture, Challenges and Applications", *IEEE Wireless Communications Magazine*, Special Issue on Mobile Cloud Computing, vol. 20, no. 3, pp.14-22, 2013.

[20] Mandhata S., Patro S., "A Counter Measure to Black hole Attack on AODV Based Mobile Ad hoc Networks", International Journal of Computer & Communication Technology (IJCCT), Vol.2, no. 6, 2011.

[21] Mollah M., Azad A., Vasilakos A., "Security and privacy challenges in mobile cloud computing: Survey and way ahead", *Journal of Network and Computer Applications*, vol. 84, pp. 38-54, 2017.

[22] Palmer N., Kemp, Kielmann T., Ba H.l, "Ibis for mobility: solving challenges of mobile computing using grid techniques," in *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*, , Santa Cruz, California , article no. 17, 2009

[23] Paranjothi, A., Khan, M., Nijim, M., "Survey on Three Components of Mobile Cloud Computing: Offloading, Distribution and Privacy", *Journal of Computer and Communications*, vol. 5, no.6, pp. 1-31, 2017.

[24] Patil, A. Sutar S., "Attribute Based Secured Storage Middleware for Mobile Cloud Computing", *International Journal of aAdvance Technology in Engineering and Science* vol. 4. Special issue 1, 2016.

[25] Sanaei Z., Abolfazli S., Gani A., Buyya R., "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges", *IEEE Communications Surveys & Tutorials*, vol.16, no. 1, pp. 369–392, 2014.

[26] Sarddar D., Nandi E., "An Authenticate Cryptography based security model for handling multiple request from multiple devices for Mobile Cloud Computing", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 1, 2016.

[27] Suo H., Liu Z., Wan J., Zhou K., "Security and privacy in mobile cloud computing". *In Wireless Communications and Mobile Computing Conference* 9th International, Sardinia, Italy ,pp. 655-659, 2013.

[28] Wadhwa D., Panag T., "Performance Comparison of Single and Multipath Routing Protocols in Ad hoc Networks", *Int. J. Comp. Tech. Appl*., vol. 2, no. 5, pp.1486-1496, 2011.

Diaa Salama Abdul-Minaam was born on November 23, 1982 in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009 specializing in Cryptography and network security. He obtained his Ph.D. degree in information system from faculty of computers and

information, menufia university, Egypt. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Benha University, Egypt since 2011. He has worked on a number of research topics. Diaa has contributed more than 20+ technical papers in the areas of wireless networks, wireless network security, Information security and Internet applications, Cloud Computing, Mobile Cloud Computing in international journals, international conferences,local journals and local conferences. He majors in Cryptography, Network Security, IoT, Big Data, Cloud Computing. (Mobile: +20166104747; +201019511000 E-mail: ds_desert@yahoo.com)

Yaser Maher Wazery was born on June 1, 1983 in samalout, Minia, Egypt. He received the B.S from Faculty of Computers &Information, Cairo University, Egypt in 2004 with grade very good with honor, and obtains master degree in information technology from faculty of computers and information, Cairo university, Egypt in 2007 specializing in cryptography. He obtained his Ph.D. degree in information technology from faculty of science port-said university as a joint supervision with CSU, 2014. He is currently a Lecturer in Information technology department, Faculty of Computers and Information, Minia University, Egypt. He has worked on a number of research topics. Yaser has contributed more than 20+ technical papers, graduation projects in the areas of multimedia processing, image processing, wireless networks, wireless network security, Information security and Internet applications, Cloud Computing, in international journals, international conferences, local journals and local conferences. He majors in Cryptography, Image processing , pattern recognition Network Security, IoT, Big Data, Cloud Computing. (Mobile: +201111161981; +201003751772 E-mail: Yaser.wazery@minia.edu.eg)