TELKOMNIKA, Vol.17, No.6, December 2019, pp.2818~2825
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i6.13201

Modified RSA-based algorithm: a double secure approach

Israa Al_Barazanchi*[1], Shihab A. Shawkat[2], Moayed H. Hameed[3], Khalid Saeed Lateef Al-badri[4]
[1]Baghdad College of Economic Sciences University, Baghdad, Iraq
[2]Directorate of Education, Salah Al-Din, Iraq
[3]Department of Accounting, The faculty of managerial and financial sciences, University of Imam Jaafar Alsadiq, Iraq
[4]Department of Physics, College of Education, University of Samarra, Samarra, Iraq
*Corresponding author, e-mail: israa44444@gmail.com[1], shahab84ahmed@gmail.com[2], moayed_hamad@yahoo.com[3], saaedkhalid@gmail.com[4]

Abstract

Security algorithms like RSA are becoming increasingly important for communications to provide companies, organizations, and users around the world, secure applications who rely heavily on them in their daily work. Security algorithms use different acquaintances among companies which might belong to various countries or even cities. Such data should essentially be encrypted to make sure that there is security in transportation. Thus, the current research paper leads to the novel system of security for the safe transfer of data. This paper examines the general principles of encryption and focuses on the development of RSA and the complexity of the encryption key so that it becomes more secure in the applications used. In this project, we will work on the RSA algorithm by adding some complexity to the 3keys (3k). This addition will increase the security and complexity of the algorithm's speed while maintaining encryption and decryption time. The paper also presents an approach by means of public key encryption to enhance cryptographic security. Moreover, double security is provided by the algorithm of RSA. This novel RSA algorithm was investigated in MATLAB. Numerical results for the various parameters such as Mean Square Error (MSE), correlation and Bit Error Ratio (BER) were implemented for the encryption of the message. The experimental results demonstrated that the proposed algorithm for 3 keys has small error rate in the retrieval of the encoded text

Keywords: *decryption, encryption, RSA algorithm, RSA2k, RSA3k*

1. Introduction

Security in digital systems describes the act of maintaining information confidential and protecting it from unauthorized access and users. In security, confidentiality alludes to the process of keeping data safe whereas integrity describes the process of preventing modification of the data. Further, availability means that the data is accessible by the authorized users when needed. These three security goals can be achieved via cryptography. The public key cryptography is made of a set of approaches that are utilized in the encryption of sensitive message to make it readable to the authorized personnel. Providing security for data transfer and support for the most reliable and secure way to handle sensitive data in connection is one of the most critical requirements for secure applications that meet user requirements, the most important practical aspects of communications and applications [1]. The harmless communication of data remains an essential part of life. Thus, it is crucial to shield the data from any exploitation. Data can be transformed into a cryptosystem by way of encryption and decryption. The conversion of the plain text into the encrypted one is termed as encryption. Or the data which has to be conversed to yield the ciphertext by utilizing encryption key is known as encrypted data. Whereas, the decryption key used for the transformation of the ciphertext to the plain/ original text is termed as decryption. Symmetric cryptography represents the sameness of encryption or decryption key or derivative of each other. Such type of cryptosystem can be a subject to wreckage if unauthorized personnel gain access to the decrypt or encrypt key. Martin Hellman and Whitfield from Stanford University presented a mechanism to escalate the protection with the help of Public key cryptosystem [2]. This mechanism uses a pair of correlated decryption and encryption keys.

Received May 23, 2019; Revised June 30, 2019; Accepted July 18, 2019

Out of these two, one private key retains undisclosed, whereas the public key gets revealed. Moreover, the encrypted message is generated through public key whereas decrypted with the help of a private key, and this protects decryption via a public key. This is what made communication security conceivable. The best prevalent algorithm for public key is RSA, which was named after authors such as Rivest-Shamir-Adleman.

The processing competencies, security measures, and shortage of secure data are the most emphasized features for safer communication. Normally four steps are required for secure communication involving encoding-sending-receiving-decoding. However, this can be breached into two phases, i.e., the first phase includes the interception of encoded data such as its transfer to the receiver from the sender. While the second phase signifies the data decoding [1]. A regular power of computation can assist in reverse engineering of the cryptographic algorithm after the obsolescence of a secure system of communication. The cryptographic algorithmic security is straightforwardly associated with the mathematical operations' complexity, which also describes the essentials of an ending procedure. Another research work indicated a comparatively small lifecycle of each cryptographic algorithm with hardware-assisted reverse engineering while evolving the power of computation [3]. Thus, the reliability of a safer communication system depends upon the reliability of a cryptographic algorithm. The growth of e-commerce and computer technology has provided an extensive space for RSA technology application. RSA software is suitable for an individual's usage out of library software, hardware, or product kernel. The IC technology is established enough in case of 'hardware' as it is being used in electronic devices of all types. While it is mostly utilized in case of software for internet digital certification, encryption correction, and digital connection. But with an increasing volume of improving the needs of people as well as data each year, RSA is subject to different challenges. These include advanced persistent threats (APTs), application/data security, service rejection attacks, privacy, mobile, and algorithm security. However, advancements have been projected in a few years. The problem of mathematical factorization is being relied upon in this case. It suggests that in a huge quantity of numbers, finding two prime numbers with a given product number is not possible. Because with an increased number, the factoring possibility declines, thus, requiring a worthy public cryptosystem key in a large quantity. This system makes breaching more difficult as one essentially first identify the carrier that holds the secret data before trying to extract and decipher it [4]. This study presents a modified RSA algorithm that is based on a set of unique prime numbers which uses double encryption and decryption process. This proposed system seeks to solve the shortcomings associated with RSA algorithm which traditionally employs two prime numbers, same key for encryption and signing and a small encryption exponent. The proposed solution utilizes "n" distinct prime number instead of the conventional two prime numbers increasing the pool for the selection of a bigger encryption exponent leading to enhanced security. This modified RSA has an increased factoring due to the increased prime numbers and the big encryption exponent. The process of double encryption and decryption significantly increase the security of the RSA algorithm.

Cryptography

The Greek word 'Cryptography' means 'hidden secret' which gives secure communication in the company of adversaries. Usually, it works by overpowering the influence of adversaries/ third parties. Hence, facilitating in investigation and assemblage practices of information security data, for instance, data integrity, non-repudiation, authentication, and data confidentiality. Modern cryptography intersects different disciplines like computer sciences, electrical engineering, and mathematics. Furthermore, its applications comprise computer passwords, electronic commerce, and ATM cards [5]. Former modern age cryptography was considered to be efficiently identical to encryption whose primary focus was converting the readable information into seeming boloney. The history indicated that the instigator of an encrypted message shared the practice of decoding to the anticipated recipients only. Thus, preventing undesirable persons from decoding for original data. By the time of World War, I as well as the computer arrival, operating cryptology became intricate and prevalent [6]. As modern cryptology is centered upon computer science and mathematical theories.

Therefore, computational rigidity assumptions are used to design cryptographic algorithms which make algorithms unbreakable as a result of any adversary intrusion. Theoretically, this system is breakable; however, not possible with familiar practical ways. Such schemes are designated as computationally protected. Fast computing technology and

theoretical advances need persistently modified solutions. Theoretically safer schemes are indestructible by infinite computing power such as a one-time pad. However, such schemes' implementation is more problematic than that of computationally safer and theoretically destructible procedures. The situation of encryption and decryption entitled as cryptosystem is presented in Figure 1.

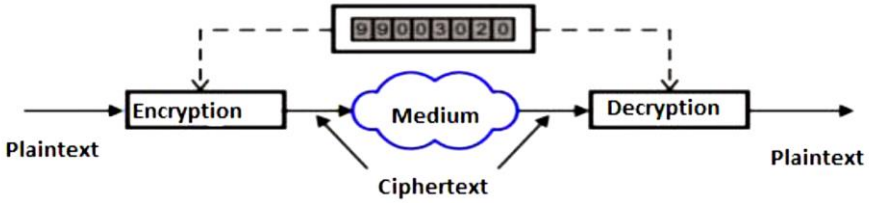

Figure 1. A system of encryption and decryption is called a cryptosystem [7]

RSA algorithm

The associates of Massachusetts Institute of Technology (MIT) founded public key as RSA and the origin as asymmetric cipher. RSA had designated because of its reputation and broad analysis. Being commercial, an algorithm of a public key is broadly promoted and utilized in the personal and business communication sector. Recent applications of RSA are more beneficial because of its flexible range of key size, which is 2 to 2048 bit. Algorithm's safety relies upon the chosen key size by programmer or user. With the length of 1024-bit size key is used along with this algorithm. Though the key size of 512 bits is still utilized for many applications [8].

The secret/private key encryption frequently designated as a symmetric key. Overall, a solo key is used to 'encrypt' / 'decrypt' the messages in this grouping of algorithms. Because of the key, all the communication among intricate parties will be confidential. To make the security ideal, every communicator should have a discrete key. Thus, both correspondents should make sure to preserve the discretion of the operator key [9]. RSA algorithms present the key generation as an initial step. Moreover, every customer needs to create a pair of the public-private key [10]. The top acknowledged and extensively used scheme of public key formation trails the subsequent steps. The algorithm of key generation has the following particulars:

a. Two great prime number are chosen. Suppose they are "p" and "q". Both p and q are in any case 512 bits in size. Thus these are represented as p!=q
b. Computation of system modulus is done which is N=p*q, here, ϕ (N)= (p-I) 1(q-1)
c. Calculate "n" to find n through n= p*q
d. A minor odd integer "e" is selected which is comparatively major to ϕ (N) & not to the 1. Here, 1 is less than others like 1 <e<g< N. thus, represented as gcd (e, ϕ (N)=1
e. Further, "d" is calculated to become the multiplicative inverse of "e" modulo "ϕ (N)". at this time, e.d=1 mod ϕ (N) & 0 <d<N
f. Thus, the encryption key which is the RSA public key of ordered pair (e, n). This key is going to be published.
g. Whereas, decryption key is the RSA private key which is ordered pair of (d, n). This key should be kept in secret.
h. Not to compromise your cryptosystem's security, annihilation of "p" & "q" must be assured.

RSA Encryption

The public key of a recipient (KU= {e, N}) is attained firstly by sender for encryption of message M through RSA. The encrypted message is computed according to (1) after receiving the public key from the recipient [11].

$$C=M^e \bmod N \quad (1)$$

where 0≤ M< N

Hence, C represents the message which is encrypted and given to the recipient through a public setup. Message M cannot be obtained by any user other than the recipient through decryption of C. The two public and private keys are important in RSA encryption. Private one is

kept in reserve by the receiver while public one is broadcasted publically. Therefore, public key is used by sender to provide encryption although, through private key decryption is provided [12]. Keys are less in number but less effective for longer messages. This condition is represented in Figure 2.

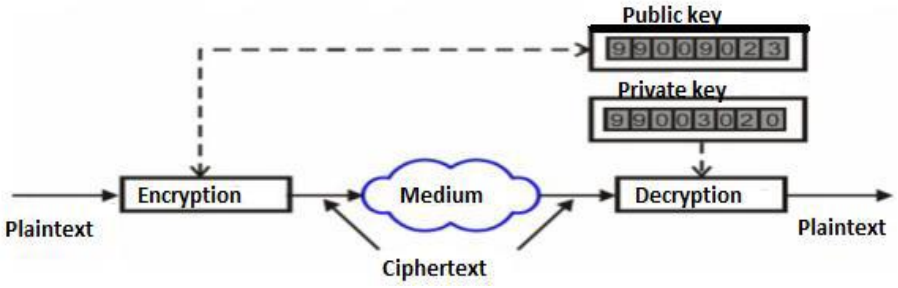

Figure 2. A simple asymmetric key cryptography model [7]

2. Related Work

Lately, the safety levels of computing communication applications are demonstrated by various security means. This is the developed process for the sustenance of used information/data. Competent algorithm of security progression permits the users to reach their data more flexibly. This offers huge storage competence at less costs. It emboldens the customers to shift between applications in their own storage [13]. The study [14] used general RSA algorithm with three keys but the study still needs prove the security level to solve the problem in upload data from server. The author [15] proposed Dual RSA security framework but Dual RSA can't be used in all application because the algorithms of key formation has improved in complication.

3. Implementation of Proposed System

The usage of more than 2 keys by the suggested system upsurges the RSA algorithm security. Thus, making the algorithm further intricate for the one who try to access data by decoding. Digital signatures and key exchange both can use the RSA algorithm. RSA practices conventionally accelerative mathematics while using numbers with hundreds of digits. RSA based private and public key is created by subsequent steps:

a. Two of the prime numbers are chosen including 'p, q" & r. Modulus by sub 2 can be calculated using these numbers such as n=p*q*2.
b. While being the public exponent, the 3rd number 'e' which cannot divide equally is selected. It shows prime relevancy to product of (p–1), (q–1), (r–1).
c. The integer "d" is a private exponent which can be calculated from quotient $\frac{(ed-1)}{(p-1)(q-1)(r-1)}$.
d. The 'n' and 'e' are number pair of public keys. Though these are publically acknowledged values but incompetent for the determination of "d" from 'e' and 'n' even when q and p are great enough.
e. The cipher text 'C' is produced through a public key for the creation of encrypted message 'M'. For this purpose, equation $C = M^e$ Mod n is used.
f. The desired cipher text is decrypted by receiver while utilizing private key and equation $M = C^d$ Mod n.

3.1. The Keys for Encryption Step

Presume a situation in which a sender 'A' desires to direct a message to the receiver 'B'. For this, the sender has to follow some subsequent steps.

a. Sender has to attain the public key "e & n" of the recipient B.
b. Signify the plain message by the way of a positive figure 'M'.
c. Computation of cipher text is performed using $C = M^e$ Mod n
d. Sending the C cipher text to the person B.

Figure 3 symbolizes the flow chart of algorithm encryption.

3.2. The Keys for Decryption Step

After the sent message the recipient 'B' will trail the steps given below:

a. Private key d and n is used for the computation M= C^d Mod n
b. The integer descriptive M is extracted for plain text.

there presents the essentially minimum value of modulus n and RSA algorithm works for it. Decryption processes are illustrated well in Figure 4.

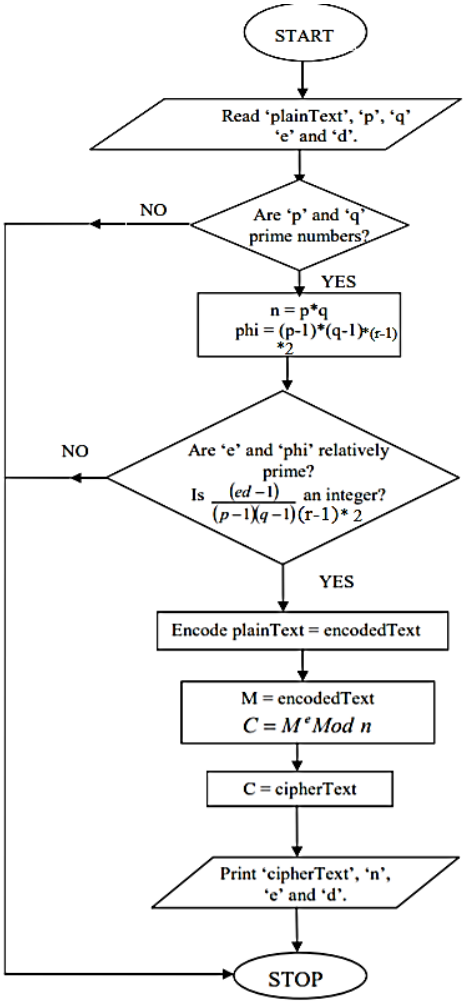

Figure 3. A flow chart illustrating the RSA decryption algorithm

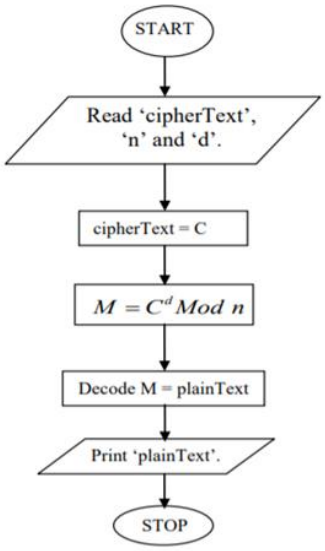

Figure 4. A flow Chart to Illustrate the decryption algorithm

This study eradicates the privacy concerns of data via algorithms of cryptographs. While boosting up the algorithm of security according to the perception of customers in applications. This work recommended a multilevel system for decryption and encryption for the provision of more security to storage information. For exclusion of the security concerns from personal algorithms of safe storage, three various keys for security were projected. RSA has been used as an asymmetric algorithm for keys in this study, which involves the usage of several keys for the purpose of encryption and decryption. However, it is intended for the maintenance of text files security. Our anticipated system strategy emphasizes on following objects for the increase of storage data safety.

a. Text files' encryption
b. Plain text display to the consumer.

Verification of stored data is mandatory for the establishment of well protected communication for linked and circulated possessions. The drawback with secure algorithm is

the security challenges since the data in the applications are managed by third party. Steganography and cryptography are some of the security measures applied in the applications to secure user data. Where it was Encryption be combined with a secure algorithm to increase security and data be sent to the software after encryption to increase security and this research paper, uses cryptographic algorithm to eliminate the privacy concerns of data. This improves communication security according to the different point of view of software clients.

4. Experimental Setting

MATLAB version R2016a software suite was used for instigation of these methods. The software was run on a private computer with an operating system having 2.27 GHz Intel (R) Core (TM) i5 CPU with Windows 10 and 4GB RAM.

4.1. Evaluation Parameters

Numerical parameters that evaluated the proposed system's quality for the encryption message were four in number. The description of these parameters is specified below [16-19].

4.1.1. Mean Square Error (MSE)

Among the encrypted text and the original data, the average error magnitude is estimated by MSE. A square is taken of the perceived values amongst text and original encryption for the calculation of an average [20]. In case of the existence of huge error, RMSE is used, which can further provide high relevancy weight to the errors. However, for the calculation of MSE equation is used as follows:

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

4.1.2. Bit Error Ratio (BER)

The amount of the received error bits, when divided with a total transferred bit, is called bit error ratio. The estimation of BER is done with the help of incorrectly gained bit (because of noise) probability calculation [21]. Being a meek conception, BER can be determined from (3).

$$\mathrm{BER} = \text{Errors/Total Number of Bits} \tag{3}$$

4.1.3. Correlation

The two signals become alike when correlation stretches to the maximum. The multiplication of the signal's intricate conjugate related to spectrum frequency with other spectrum rates defines to be corresponding the correlation [22-25]. More, the closely related data sets of vectors / two signals are determined for their relatedness or dissimilarities in their stage and size. The range of linear coefficient of correlation (r) amid 1 and -1 can be estimated with the help of (4). Correlation

$$= \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2 \sum(Y_i - \bar{Y})^2}} \tag{4}$$

4.2. Experimental Results

Table 1 represents the results attained from the execution of anticipated RSA (2k, 3k) algorithm proceeding test profaning for various sizes of text. Further observation showed the zero value for correlation and BER, whereas, one for all sizes of text. Thus, it designated the zero-error received by bits number.

It is evident that the proposed algorithm with 3keys has a very small error rate in the retrieval of encoded text. A clear difference is the variation from the standard 2key algorithm, but there is one negative, the time of encryption, which is a small difference compared to the first algorithm, and this is calculated to the proposed method as having a strong advantage and has an excellent effect in the rate of error and the timing of encryption. And that Cryptography is a

good way to increase the data security. RSA 2key is better than RSA 3key because time taken for encrypting and decrypting data using RSA 2key is much smaller than RSA 3key.

Table 1. Results from Implementing the Proposed RSA Algorithm (2k, 3k)

No.	Algorithm	Input text size (in byte)	MSE	BER	Correlation	Execution in Time (in Sec)
1	RSA 2k	10	0.0627	0	1	0.040637
	RSA 3k		0.0608	0	1	0.051207
2	RSA 2k	20	0.0571	0	1	0.026459
	RSA 3k		0.0500	0	1	0.041997
3	RSA 2k	30	0.0518	0	1	0.030554
	RSA 3k		0.0498	0	1	0.035163
4	RSA 2k	40	0.0468	0	1	0.032963
	RSA 3k		0.0452	0	1	0.036704
5	RSA 2k	50	0.0422	0	1	0.033964
	RSA 3k		0.0408	0	1	0.035192
6	RSA 2k	60	0.0391	0	1	0.030636
	RSA 3k		0.0363	0	1	0.033958
7	RSA 2k	70	0.0349	0	1	0.028010
	RSA 3k		0.0322	0	1	0.030544
8	RSA 2k	80	0.0295	0	1	0.027097
	RSA 3k		0.0282	0	1	0.029125
9	RSA 2k	90	0.0258	0	1	0.027128
	RSA 3k		0.0247	0	1	0.028191
10	RSA 2k	100	0.0236	0	1	0.034315
	RSA 3k		0.0213	0	1	0.035638

5. Conclusions

Generally, the current project achieved a significant milestone because the implementation of the programs met all the objectives set at the start. As well as all test runs have proved the robustness of the new approach. The creation of the longer keys would provide a security for some years such as factoring them is not feasible. A test was being run for this scheme on dissimilar input text types with altered RSA keys and text sizes. Then, all the time, an upright quality secret text was recovered successfully. The comparison of a traditional RSA and three keys RSA showed the relatively high security and alterations in equation formation for 3k RSA algorithm. All the case observations concluded that any imposter might get successful to acquire encrypted shares of the networks. But that person won't be able to recover secret text while lacking a private key accessibility.

Our forthcoming plan includes more improvement in contemporary design, primarily. Its execution on a bigger scale will simulate the multiple covers and normal collaborative parties. We will introduce a sequence of listeners in the middle of sender and receiver communication path which will also include most of the set of art stag analysis filters. We will further analyze the system for its placement maintenance on a bigger scale with attacking parties and higher magnitudes safer data. Following all the figures based on the previous implementation, our plot is to categorize ultimate liabilities and remove them. The generated keys may perhaps be used by open pretty good privacy (PGP) for the encryption and decryption algorithms' executions. Further, it may be used to emphasize Add 4 primary key of the algorithm. Additionally, it can advance the bit encryption standard (128 bit or 256 bit) or block size with an influential encryption RSA and DES techniques.

References

[1] Abdulshaheed HR, Binti SA, Sadiq II. A Review on Smart Solutions based on Cloud Computing and Wireless Sensing. *International Journal of Pure and Applied Mathematics*. 2018; 119(18): 461–486.

[2] Dey H, Islam R, Arif H. *An Integrated Model to Make Cloud Authentication and Multi-Tenancy More Secure*. In 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST). 2019: 502-506.

[3] Gautam P, Ansari MD, Sharma SK. Enhanced Security for Electronic Health Care Information Using Obfuscation and RSA Algorithm in Cloud Computing. *International Journal of Information Security and Privacy (IJISP).* 2019; 13(1): 59-69.

[4] Srivastava S, Srivastava A. Integration of RSA and Waterfall Framework: Aggrandize Security in Cloud Computing using Integration of Rivest–Shamir–Adleman (Encryption Algorithm) and Waterfall Model. *Journal of Microcontroller Engineering and Applications*. 2018; 4(3): 1-8.
[5] El Makkaoui K, Beni-Hssane A, Ezzati A. Speedy Cloud-RSA homomorphic scheme for preserving data confidentiality in cloud computing. *Journal of Ambient Intelligence and Humanized Computin.* 2018: 1-12.
[6] Yang LT, Huang G, Feng J, Xu L. Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing. *Information Sciences*. 2017; 387: 254-265.
[7] Bisht N, Singh S. A comparative study of some symmetric and asymmetric key cryptography algorithms. *International Journal of Innovative Research in Science, Engineering and Technology*. 2015; 4(3): 1028-1031.
[8] Yu Y, Xue L, Au MH, Susilo W, Ni J, Zhang Y, Shen J. Cloud data integrity checking with an identity-based auditing mechanism from RSA. *Future Generation Computer Systems*. 2016; 62: 85-91.
[9] Thirumalai C, Kar H. *Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices*. In 2017 Innovations in Power and Advanced Computing Technologies (i-PACT). 2017: 1-6.
[10] Pancholi VR, Patel BP. Enhancement of cloud computing security with secure data storage using AES. *International Journal for Innovative Research in Science and Technology*. 2016; 2(9): 18-21.
[11] El Makkaoui K, Beni-Hssane A, Ezzati A, El-Ansari A. Fast cloud-RSA scheme for promoting data confidentiality in the cloud computing. *Procedia Computer Science.* 2017; 113: 33-40.
[12] Prema G, Natarajan S. *An enhanced security algorithm for wireless application using RSA and genetic approach*. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). 2013: 1-5.
[13] El Makkaoui K, Beni-Hssane A, Ezzati A. Cloud-ElGamal and Fast Cloud-RSA Homomorphic Schemes for Protecting Data Confidentiality in Cloud Computing. *International Journal of Digital Crime and Forensics (IJDCF)*. 2019; 11(3): 90-102**.**
[14] Stergiou C, Psannis KE, Kim BG, Gupta B. Secure integration of IoT and cloud computing. *Future Generation Computer Systems*. 2018; 78: 964-975.
[15] Abdulshaheed HR, Binti SA, Sadiq II. Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing. *International Journal of Pure and Applied Mathematics*. 2018; 119(18): 427–449.
[16] Dahiya N, Rani, S. Cloud Computing Security: A Review. *IJEDR.* 2017; 5 (3): 11–16.
[17] Dubey A. Cloud Computing and Its Security Issues. *International Journal of Advance Research in Computer Science and Management Studies*. 2016; 4(7): 29–33.
[18] Bhavani SD. International Journal of Advanced Research in Data Storage Security in Cloud Computing: A Survey. *International Journal of Advanced Research in Computer Science and Software Engineering.* 2017; 7(1): 52–57.
[19] Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access*. 2018; 6: 20596-20608.
[20] Chai T, Draxler R. Root mean square error (RMSE) or mean absolute error (MAE)? Arguments against avoiding RMSE in the literature. *Geoscientific Model Development*. 2014; 7(3): 1247-1250.
[21] Islam M, Islam M, Islam N, Shabnam B. A Modified and Secured RSA Public Key Cryptosystem Based on “n” Prime Numbers. *Journal of Computer and Communications.* 2018; 6(3): 78-90.
[22] Kamardan M, Aminudin N, Che-Him N, Sufahani S, Khalid K, Roslan R. Modified Multi Prime RSA Cryptosystem. *Journal of Physics: Conference Series*. 2018; 995: 012030.
[23] Saxena S, Kapoor B. State of the art parallel approaches for RSA public key-based cryptosystem. arXiv preprint arXiv. 2015; 1503: 03593.
[24] Lone AH, Khalique A. Generalized RSA using 2k prime numbers with secure key generation. *Security and Communication Networks.* 2016; 9(17): 4443-4450.
[25] Zhao T, Ran Q, Yuan L, Chi Y, Ma J. Key Distribution and Changing Key Cryptosystem Based on Phase Retrieval Algorithm and RSA Public-Key Algorithm. *Mathematical Problems in Engineering.* 2015; 2015(7): 12.