Journal of Theoretical and Applied Information Technology
15th July 2017. Vol.95. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENSURING AUTHENTICATION IN CLOUD COMPUTING THROUGH HOMOMORPHIC ENCRYPTION

MUTI-UR RASOOL[1], SAMAN IFTIKHAR[2], TANZILA SABA[3*], JARALLAH SALEH AL-GHAMDI[3]

[1] Department of Computer Science Government College University Faisalabad Pakistan
[2] Department of Computer Science Saudi Electronic University Riyadh Saudi Arabia
[3]College of Computer and Information Sciences Prince Sultan University Riyadh, 11586 Saudi Arabia
E-mail: drtsaba@gmail.com (*Contact author)

ABSTRACT

Cloud computing is a relatively new research domain and currently, emphasizes a lot over the whole daily tasks of life. It's significant ownership and utilization is supposed to enhance furthermore, making it an essential ingredient for the future. In this research, data security of cloud computing is aimed to find out exactly how these kinds of problems are resolved. The objective of this particular research is to avoid data contact from an unauthorized user, to recommend a sort of distributed scheme to offer safety of the information in the cloud. We believe as per experimental results that it could be accomplished by utilizing homomorphism encryption along RSA algorithm. Promising results are achieved that are comparable to the state of art.

Keywords: *Cloud computing, Homomorphic encryption, Cloud security, Cloud computing RSA*

1. INTRODUCTION

The knowledge along with data that located on the cloud is essential for people with lethal intention consequently security is significant within cloud environment [1-5]. A considerable way of measuring credibly protected data and particular information on computer systems, and this basic data is presently being put away and replaced by cloud. So realizing this security procedure that the cloud services provider and suppliers use is essential [6-12]. The key thing that really must be handled is the effort to maintain security that the cloud supplier freshly has set up. These efforts to establish security which cloud vendor supply alter from supplier to supplier and around various types of clouds. Generally, there are the following vital security measures connected vulnerabilities in the cloud computing system.

1.1 Data Privacy and Reliability

Within a cloud environment, a similar data center could well comprise info owned by distinct clients within the similar computer. In these cases, info owned by distinct clients is necessary to always be out of the way, which even more lifts the issue of dependability. While process platforms of CSP (Cloud Services Providers) usually are propagated amid distinct clients. For example, harmful software package or infections could well sink into services and additional affect end user environment [13-15].

1.2 Data Integrity

Data ethics is an important issue focused in the most cloud processing environment as it is a high concern of each inner as well as exterior assaults. Deficiency of confidence concerning CSP as well as cloud end user could also improve the difficulty of files ethics. In contrast to classic repository techniques, all its tenant's facts are actually stashed about common files core [16-20].

1.3 Authentication and Authorization

World wide web GUIs have grown to be probably the most sophisticated technologies providing cloud solutions for clients and administrators as well. Nonetheless, there is a shortage of standard aspects of security regarding what's on the actual front-end GUI [32-35].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. BACKGROUND

Security is frequently a zone of sympathy toward both cloud merchants and buyers. Consequently, it seems to be an earnest need in the IT business [20]. As per the overview led by International Data Corporation (IDC), Microsoft [21] and NIST [22], security in a cloud computing model was of essential sympathy toward changed IT administrators [23]. Scientists from MIT accept that "Data innovation's next fabulous test will secure the cloud" [24]. National Institute of Standards and Technology (NIST) [22] likewise focuses "security difficulties of cloud computing presents are impressive". Kui et al. [25] talk about various types of security difficulties for open cloud stages including information protection, trustworthiness, Multi-Tenancy Security and Privacy and Access control. ENISA [26] likewise concentrates on different security challenges that cloud computing is confronting. Albeit different security issues still, exist for cloud computing stages, distinctive non-benefit and government financed association has put a considerable measure of their endeavors to give some security rules. Fundamentally, NIST [22, 27] and CSA [23] propose security rules to be taken after for distributed computing situations.

Considering every one of these certainties, the objective of this examination paper is to plan non-specific and secure structural planning that could amplify the security benefits in any cloud computing stage. Distinctive sort of registering stages exist today, out of which some are exclusive and some are open source. Because of the exclusive business of cloud stages, the extent of this report is constrained to open source (OpenStack) stage. Proposed security expansions are particular and sufficiently granular to be embraced by any cloud stage.

Divya et al [27] the actual proposed design enable end users to audit the cloud storage devices having incredibly light in weight verbal exchanges along with calculation price tag. The actual auditing effect not only guarantees solid cloud storage devices correctness assurance, and also simultaneously defines rapidly data malfunction localization, i.e. the recognition of misbehaving server [28]. For the cloud data are generally powerful within character, the proposed design, even more, helps risk-free along with successful powerful procedures about outsourced data, such as block change, deletion, along with append.

Gayathri et al., [28] discover the problems along with likely safety problems connected with primary extension with thoroughly powerful data messages by before works and demonstrate the way to assemble a stylish proof program with the seamless integration these a couple salient attributes inside our standard protocol layout. Specifically, to accomplish successful data mechanics, improve existing evidence of storage space designs by manipulating the traditional Merkle Hash Tree construction pertaining to stop marking authentication.

Suganya and Damodharan [29] proposed a methodology to check the cloud storage using the really light-weight connection and computation costs too. It supplies durable cloud storage reliability and also provides for more fault position data, that is to say, the proof of identity connected with the misbehaving server. Proposed layout facilitates extended secure and also useful energetic activities, as well as stops change, deletion and also add on.

Kumar et al., [31] proposed the versatile distributed storage devices honesty auditing system, employing homomorphic small along with distributed erasure-coded facts. The actually planned pattern enables people in order to examine your cloud storage devices having quite lightweight verbal exchanges along with working out the cost. The actually planned plan is usually very effective along with robust versus Byzantine failing, detrimental facts change invasion, and in many cases server colluding attacks.

3. PROPOSED METHODOLOGY

The actual RSA public key cryptosystem had been devised in [30]. The actual RSA cryptosystem based upon the particular extraordinary change between large primes along with the issues regarding invoice discounting the item regarding a couple of large prime quantities (the integer

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

factorization problem). This particular section offers a short overview of the particular RSA formula pertaining to encrypting and decrypting announcements.

Utilizing entirely homomorphic encryption, we are able to guarantee files protected for cloud processing [30]. The real key notion is actually that the file is actually encrypted by means of homomorphic encryption and stored in Cloud server, via this specific we are able to obtain the big profit: manage your cipher word right in server and guarantee your data's protection simply because someone else who does not necessarily understand the true secret are unable to decrypt that. We employ homomorphic symmetric encryption to develop the results protected system.

In this algorithm, six prime numbers are used instead of two so that it becomes very difficult to factor *n*. It increases the security of the system as well increases the computation difficulty. To decrease the complication we improved the time taken by the modulo process. Encryption, as well as decryption both in RSA, involves raising an integer to another integer mod *n*. actually, when the exponentiation taken of integer numbers before modulo operation the size of the intermediate results in very big bit integer. Pattern outlines symmetric homomorphic encrypt to enhance data safety measures. Very first, an individual login and the server allocate new key-generation seeds in order to the user; next user generate the trick essential on purchaser employing this seeds, therefore the server don't realize the trick essential by any means. This action could be duplicated next this permits an individual to obtain a similar secret essential anytime. Second of all an individual can use this specific essential in order to encrypt info that your user would like to broadcast and help save this inside the cloud server. Though transmitting in addition different cryptography engineering such as a digital trademark could place on assure the particular strength and non-repudiation. Now, an individual could mail ask in order to cloud server (also encrypted), as well as the server, do the particular functioning also without realizing this article of the functioning. Using this type of scheme, not just the particular located info but additionally, the particular transmitted info is usually encrypted, thus all of us don't bother about the data is usually eavesdropped or thieved. It also offers safe data audit assistance because the third audit party could cope with the particular encrypted data right. Along with the encryption, all of us make use of is usually balance thus we could compute this having a smaller amount MIPS which are usually very necessary for tiny consumers.

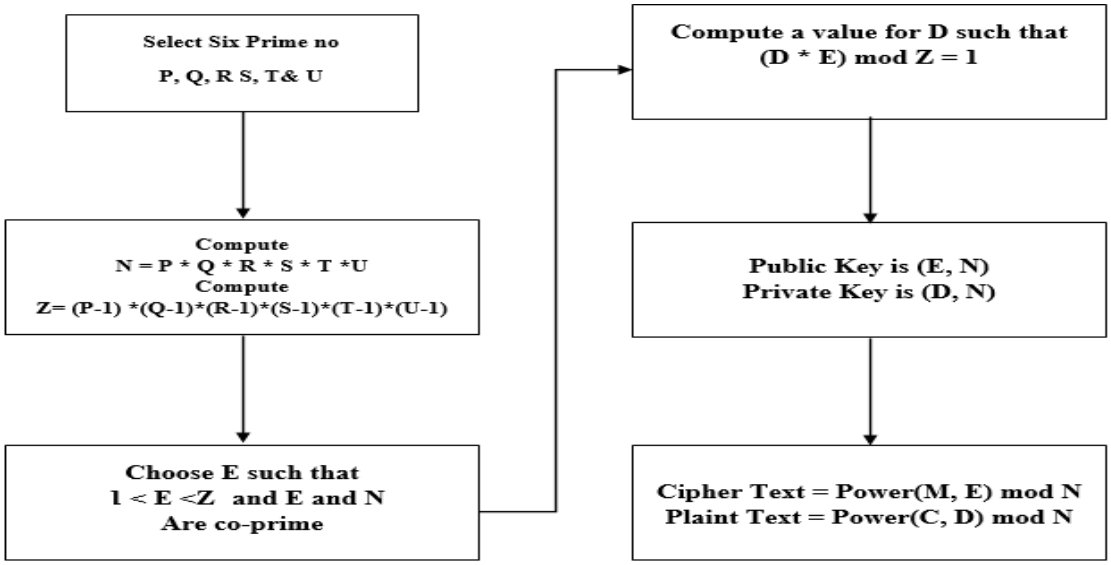

Figure 1: Proposed research layout

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Block Diagram of Proposed Algorithm

In this algorithm first, we have to generate six distinct prime numbers **p, q, r, s, t** and **u**. The product of these numbers is **n** which a component of the public key is. We then produce the encryption key ***e*** for transforming plain text to cipher text which must be relatively prime number to **z = (p – 1) * (q – 1) * (r – 1) * (s – 1) * (t – 1) * (u – 1)**.

After this, we create the decryption key ***d*** for converting cipher text to plain text such that **d * e mod z = 1**. So the public key is **(*n, e*)** and the private key is **(*n, d*)** as shown in fig 1. Then for any certain plain text, cipher text can be computed and vice versa as follows:

Cipher Text: C= power (m, e) mod n.

Plain Text: m= power (C, e) mod n.

3.2 Flow Chart of Proposed Algorithm

The flowchart of the proposed algorithm is exhibited in Figure 2.

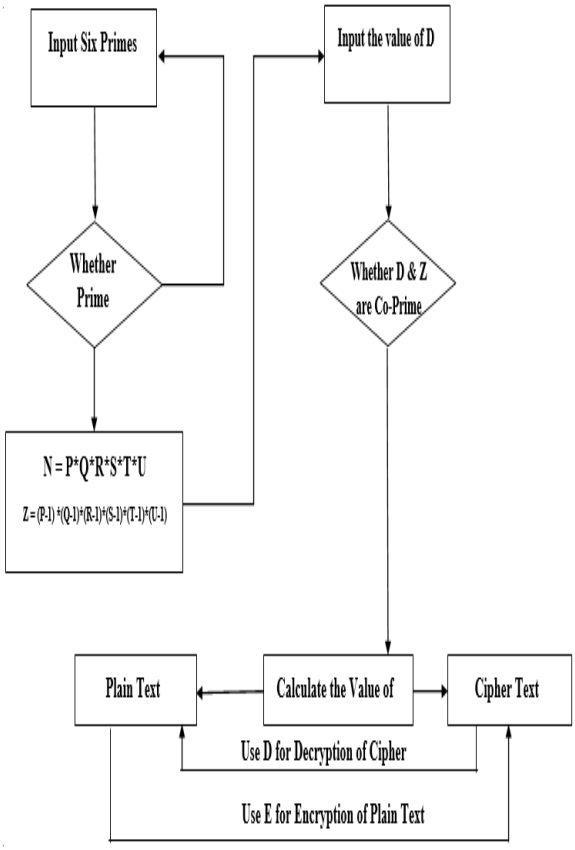

Figure 2: Proposed Research Layout

4. RESULTS ANALYSIS AND DISCUSSION

4.1 Effect of Key Size variation on proposed algorithm

The table 1 displayed below illustrates that if the length of the key bit is 1 then we will recover the key surely after the 10 efforts. If the length of the key is increased to 5 then 100000 efforts are required which takes a lot of time retrieve the key. This means that security keeps on growing as the key size rises but the complexity of the system is also increased. So there is a necessity to uphold adjustments between key length and difficulty of the system.

Table 1: Bit length effect of key on security

S.No.	Length of Key (Bits)	No. of Attempts
1	5	10^5
2	10	10^{10}
3	15	10^{15}
4	20	10^{20}
5	25	10^{25}

The curve in graph 1 demonstrates that if the number of bits of key length grows then the security of system increases. The system is safe for 10^5 attempts in case of 5 bit, during this time data is reached at the destination and at the next time communication, the key is changed. If the time is less and not deliver the full satisfaction of security, then use the 20-bit key length. Depending upon the desired key length, it is increased.

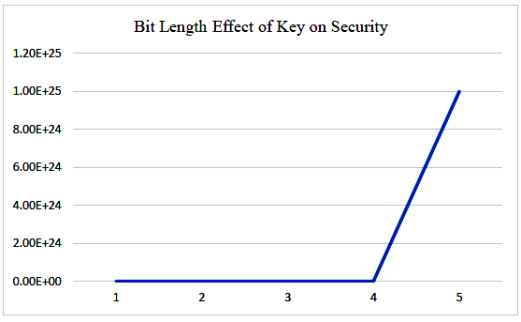

Figure 3. Bit Length Effect Of Key On Security

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Comparison between proposed algorithm and other approaches has been done on the base of throughput for the different file size.

4.1.1 Performance Assessment Limits

A performance assessment criterion is a time taken by the algorithm to do the encryption and decryption of the input text file that is encryption computation time and decryption computation time.

4.1.2 Encryption Computation Period

The encryption computation period is the time which is used by the algorithms to produce the cipher text from the plain text. The encryption time can be taken to calculate the encryption data of the algorithms shown in table 2 respectively.

Table 2: Encryption Computing Time On Files

Input File Size (Kb)	Encryption Completing Time (MSec)						
	RSA	AES	TDES	DES	RC6	RC2	Proposed
59	60	56	54	29	41	60	30
100	93	90	81	49	60	91	42
247	125	112	111	47	77	121	45
321	158	164	167	82	109	168	75
694	222	210	226	144	123	262	135
899	369	258	299	240	162	268	160

For the file of 59 Kb in size, the encryption completing time for above-mentioned algorithms are 60, 56, 54, 29, 41, 60 and 30MSec respectively. For the file size of 899Kb, the encryption completing time are 369, 258, 299, 240, 162, 268 and 160MSec respectively. As it has been revealed that proposed algorithm consume less time for all types of file sizes. With the assistance of the table 2 graph2 has been drawn and it demonstrates that how the encryption completing time depends on the file size.

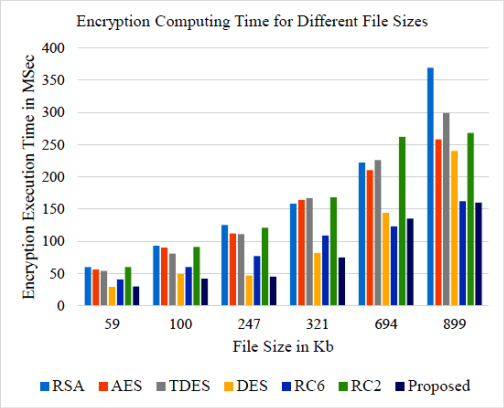

Figure 4: Encryption Computing Time On Files

From the above-computed values of data, it is clear the proposed algorithm provides optimized results in comparison to other encryption algorithm and shown in graph 3

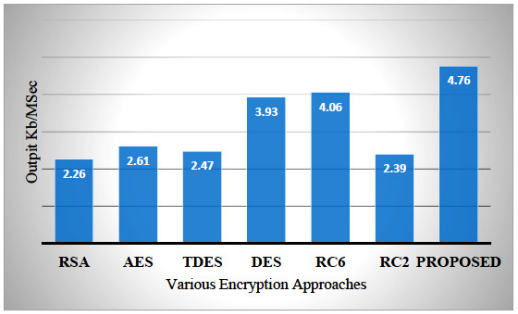

Figure 5: Output Comparison Of Various Encryption Approaches

4.1.3 Time taken during Decryption:

Time taken during decryption is the time taken by the algorithm to convert plain text to cipher text. Time taken during decryption can be used to calculate the decryption of data by the algorithms shown in Table 3.

Table 3: Decryption Computing Time On Files

Input File Size (Kb)	Decryption Completing Time (MSec)						
	RSA	AES	TDES	DES	RC6	RC2	Proposed
59	60	63	53	50	35	65	32
100	76	60	57	57	58	90	53
247	110	76	77	72	66	95	59
321	158	149	87	74	100	161	71
694	171	142	147	120	119	165	134
899	173	171	171	152	150	183	145

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

For the file of 59Kb in the size decryption computing time for RSA, AES, TDES, DES, RC6, RC2 and proposed algorithm are 60, 63, 53, 50, 35, 65 and 32MSec. respectively. For a file size of 899Kb, the decryption computing time is 173, 171, 171, 152, 150, 183 and 145 respectively. Sine it has been revealed the proposed algorithm takes less time for all types of file sizes. Graph 4 has been drawn its shows that how the decryption computing time depends on the file size. Finally, comparison of proposed method with numerous algorithms has been done.

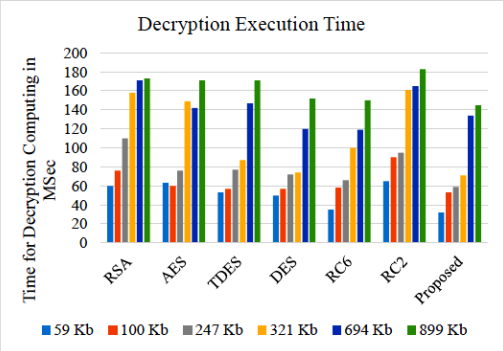

Figure 6: Comparison Of Decryption Execution Time

From the above computing values of data; it is clear the proposed algorithm delivers enhanced results in assessment to other decryption algorithms and shown in graph 5.

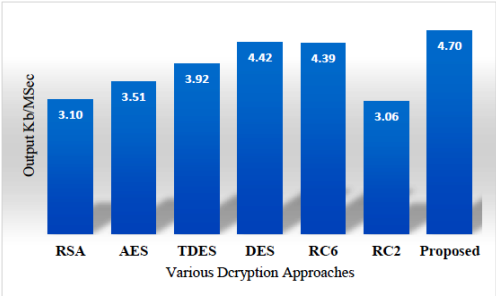

Figure 7: Output Comparison Of Various Decryption Approaches

4.2 Case Study

Simulation results have been provided above. Following example shows the transmission and reception with any length of the string. To implement proposed algorithm we have to focus on three parts which are:

4.2.1 Key Generation

Generate six prime numbers *p, q, r, s, t* and *u*. First, we have to take the input of six large prime numbers and then we compute the value of *d* and *l* which were used to generate public and private keys respectively.

Choose $p = 3$, $q = 5$, $r = 7$, $s = 9$, $t = 11$, $u = 13$

Calculate $n = p * q * r * s * t * u = 135135$

Calculate $z = (p - 1) * (q - 1) * (r - 1) * (s - 1) * (t - 1) * (u - 1). = 46080$

Choose a number relatively prime to *z* called it *e*.

Let $e = 17$

Find d such that $e * d = 1 \bmod z$.

d = 13553

Public Key is (d, n) => (13553, 135135)

Private Key is (e, n) => (17, 135135)

4.2.2 Encryption Process

By the support of public key, we are able to encrypt the value of the plain text. By entering the value of plain text we get the ciphertext.

M = 77

U = 85

T = 73

I = 73

Space = 32

U = 85

R = 82

Space = 32

R = 82

A = 65

S = 83

O = 79

O = 79

L = 76

Compute the cipher text $c = m^e \bmod n$

Cipher text of the message is:

M = 120197

U = 100150

T = 10584

I = 14698

Space = 131042

U = 100150

R = 18847

Space = 131042

R = 18847

A = 66560

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

S = 134824
O = 134824
O = 134824
L = 32416

4.2.3 Decryption Process

By the assistance of the private key, the ciphertext can be transformed to plain text.
Compute $m = c^d \bmod n$ by using the private key.
Decrypted value of the ciphertext is:
120197 = M
100150 = U
10584 = T
14698 = I
131042 = Space
100150 = U
18847 = R
131042 = Space
18847 = R
66560 = A
134824 = S
134824 = O
134824 = O
32416 = L
The decoded message is:
MUTI UR RASOOL
Outcome:
When the ciphertext is decrypted by the assistance of private key same plane text has been observed. This shows that the correctness of proposed algorithm is good.

5. CONCLUSION AND FUTURE WORK

The purpose of the cryptography is to avoid data from hackers. Study of several encryption algorithms has been effectively done. The strength of the proposed algorithm depends on the key length. The length of the key is directly proportional to safety and vice versa to performance. As the length of key grows the security of the algorithm is increased too but indirectly the performance degrades and; length of the key has been optimized. After critically examining RSA; it is found that some flaws are in it and to overcome these defects a new algorithm has been designed, implemented and evaluated. The proposed algorithm has been associated with other approaches, and it is found that output of proposed algorithm is better than other encryption approaches. The work could be extended to reduce the difficulty of proposed algorithm.

REFERENCES

[1] Jadooki, S. Mohamad, D., Saba, T., Almazyad,A.S. Rehman, A. "Fused features mining for depth-based hand gesture recognition to classify blind human communication", *Neural Computing and Applications*, pp. 1-10, doi. 10.1007/s00521-016-2244-5, 2016.

[2] Fadhil, MS. Alkawaz, MH., Rehman, A., Saba, T. "Writers identification based on multiple windows features mining", *3D Research*, vol. 7 (1), pp. 1-6, doi.10.1007/s13319-016-0087-6, 2016

[3] Waheed, SR., Alkawaz, MH., Rehman, A., Almazyad,AS., Saba, T. "Multifocus watermarking approach based on discrete cosine transform", *Microscopy Research and Technique*, vol. 79 (5), pp. 431-437, doi. 10.1002/jemt.22646, 2016.

[4] Alkawaz, M.H., Sulong, G., Saba, T. Rehman, A . "Detection of copy-move image forgery based on discrete cosine transform, *Neural Computing and Application*. doi:10.1007/s00521-016-2663-3", 2016.

[5] Bashardoost, M., Mohd Rahim, M.S., Saba, T. Rehman, A. "Replacement Attack: A New Zero Text Watermarking Attack", *3D Research*, vol. 8(8), doi.10.1007/s13319-017-0118-y, 2016.

[6] Neamah, K. Mohamad, D. Saba, T. Rehman, A. "Discriminative features mining for offline handwritten signature verification", *3D Research* vol. 5(2), doi. 10.1007/s13319-013-0002-3, 2014.

[7] Al-Turkistani, H. and Saba, T. "Collective Intelligence for Digital Marketing", *Journal of Business and Technovation*,vol.3(3), pp: 194-203, 2015.

[8] Mundher, M. Muhamad, D. Rehman, A. Saba, T. Kausar, F. "Digital watermarking for images security using discrete slantlet transform", *Applied Mathematics and Information Sciences*, vol. 8(6), pp. 2823-2830, doi.10.12785/amis/080618, 2014.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] Norouzi, A. Rahim, MSM, Altameem, A. Saba, T. Rada, A.E. Rehman, A. and Uddin, M. "Medical image segmentation methods, algorithms, and applications" *IETE Technical Review*, vol.31(3), pp. 199-213, doi. 10.1080/02564602.2014.906861, 2014.

[10] Rehman, A. Kurniawan, F. Saba, T. "An automatic approach for line detection and removal without smash-up characters", *The Imaging Science Journal*, vol. 59(3), pp. 177-182, doi. 10.1179/136821910X12863758415649, 2011.

[11] Ming, J.,Ping, J. and Chiun, R. "Provably Secure Password-based Threeparty Key Exchange Protocol with Computation Efficiency", *Journal of Business and Technovation,* vol.2(2),pp-117-126, 2014.

[12] Arafat, S. and Saba, T. Social Media Marketing Vs Social Media Commerce: A Study on Social Media's Effectiveness on Increasing Businesses' Sales, *Journal of Business and Technovation*, vol. 4(3), pp. 134-147, 2016.

[13] Joudaki, S. Mohamad, D. Saba, T. Rehman, A. Al-Rodhaan, M. Al-Dhelaan, A. Vision-based sign language classification: a directional Review, *IETE Technical Review*, vol.31(5), pp.383-391, doi. 10.1080/02564602.2014.961576, 2014.

[14] Jun,S. Mii, S. and Kao, C. New CMT-SCTP With Increased Speed of Data Transmission Using Fuzzy Logic, *Journal of Business and Technovation* , vol. 4(2), pp. 66-74, 2016.

[15] Rehman, A. Alqahtani, S. Altameem, A. Saba, T. "Virtual machine security challenges: case studies", *International Journal of Machine Learning and Cybernetics* vol. 5(5), pp. 729-742, doi. 10.1007/s13042-013-0166-4, 2014.

[16] Lung, JWJ , Salam, MSH, Rehman, A. Rahim,MSM, Saba, T. "Fuzzy phoneme classification using multi-speaker vocal tract length normalization", *IETE Technical Review*, vol. 31 (2), pp. 128-136, doi. 10.1080/02564602.2014.892669, 2014.

[17] Younus, Z.S. Mohamad, D. Saba, T. Alkawaz,M.H. Rehman, A. Al-Rodhaan, M. Al-Dhelaan, A. "Content-based image retrieval using PSO and k-means clustering algorithm", *Arabian Journal of Geosciences*, vol. 8(8) , pp. 6211-6224, doi. 10.1007/s12517-014-1584-7, 2015.

[18] Elsayed, H.A.G., Alharbi, A.N. AlNamlah, H. Saba, T. "Role of Agile Methodology in Project Management and Leading Management Tools", *Journal of Business and Technovation*, vol.3(3),pp. 188-193, 2015.

[19] Zendehdel, M. and Paim, L.H "Online Sales and Purchase of Products: Security and Privacy Issues", *Journal of Business and Technovation*, vol. 2(2), pp.142-146

[20] Sosinsky B. Cloud Computing Bible. 1st ed. Wiley, 2011.

[21] Jay Chou. PC Leaders Continue Growth and Share Gains as Market Remains Slow, http://www.idc.com/getdoc.jsp?containerId=prUS25372415.

[22] Wayne Jasen & Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standard and Technology, US Department of Commerce, Special Publication 800-144, 2011.

[23] IDC Enterprise Panel, 2015, http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg

[24] Talbot, D. "Security in the Ether. Technology Review", pp. 36–42, 2010

[25] Ren Kui, Cong Wang, and Qian Wang. Security challenges for the public cloud, *Internet Computing, Institute of Electrical and Electronics Engineers*, vol.16(1), pp. 69-73, 2012.

[26] Cattedduand Daniele, "Cloud Computing Benefits, Risks and recommendation for information security", *European Network and Information Security Agency*, 2012.

[27] Divya, K. Navya Sri,P. and Tejavath Charan Singh, "Data Storage Transparent Security in Cloud Computing", *International Journal of Ethics in Engineering and Management Education*, vol. 1(9), pp. 232-240, 2014.

[28] Gayathri, K. Umamaheswari,P. and Senthilkumar,P. "Enabling Efficiency in Data Dynamics for Storage Security in Cloud Computing", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2(12), pp. 4624-4629, 2013.

[29] Saba, T. Rehman, A. Sulong, G. "Cursive script segmentation with neural confidence, International *Journal of Innovative Computing and Information Control (IJICIC)*, vol. 7(7), pp. 1-10, 2011.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[30] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *ACM Commun*, vol. 21(2), pp. 120-126, 1978.

[31] Kumar, BA., Prasad, K. H. and Chandra, C. S. "Homomorphic Token and Distributed Erasure-Code for cloud", *International Journal of Research in Computer and Communication Technology*, vol. 2(10), pp. 1069-1075, 2013

[32] Ahmad, AM., Sulong, G., Rehman, A., Alkawaz,MH., Saba, T. "Data Hiding Based on Improved Exploiting Modification Direction Method and Huffman Coding", *Journal of Intelligent Systems*, vol. 23 (4), pp. 451-459, doi. 10.1515/jisys-2014-0007, 2014.

[33] Khodamoradi, M. Bozorgmanesh, M. and Ghorbani, E. "Usage of Data and Correspondence Advancements (ICT) In Instruction", *Journal of Business and Technovation*, vol.2(2), pp.131-135, 2014.

[34] M.S. Amin and A. Noori. "Mechanism For Farm Mechanization and Careful Planning Using Geographic Information System (GIS)", *Journal of Business and Technovation*, vol.4(1), pp. 23-28, 2016.

[35] Rehman, A. and Saba, T. "Evaluation of artificial intelligent techniques to secure information in enterprises", *Artificial Intelligence Review*, vol. 42(4), pp. 1029-1044, doi. 10.1007/s10462-012-9372-9, 2014.