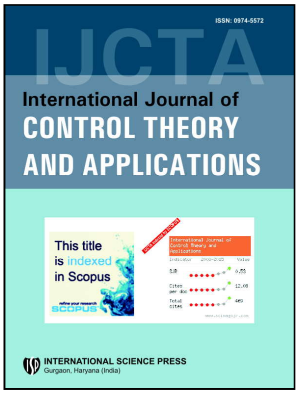

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 15 • 2017

Design and Implementation of Encryption based Data Security Algorithm for Cloud Environments

Pawan Kumar[1], Sawtantar Singh[2] and Surender Jangra[3]

[1] Ph.D Research Scholar, Department of Computer Science & Engineering IKG Punjab Technical University, Jalandhar Punjab, India, Email: pawanspp@gmail.com
[2] Professor, Department of Computer Science, BMSCE Mukatsar Punjab, India, Email: sawatantar@gmail.com
[3] Assistant Professor, Department of Computer Applications Guru Tegh Bahadur College, Bhawanigarh, Sangrur, Punjab, India, Email: jangra.surender@gmail.com

Abstract: cloud computing is growing more and more mature from initial concept building to current actual deployment. Now days many organizations, especially Small and Medium Business (SMB) enterprises, are increasingly realizing the benefits by putting their applications and data into the cloud. The adoption of cloud computing may lead to gains in efficiency and effectiveness in developing and deployment and save the cost in purchasing and maintaining the infrastructure. Objective of proposed work is to study various encryption algorithms used for data security in cloud environment. This paper describes the design of a new XOR based encryption algorithm to enhance data security. The implementation of the proposed approach is done and Compare the performance of proposed algorithm with RSA, AES, MD5 based on parameters - file size and average response time.

Keywords: cloud computing, RSA, AES, MD5

1. INTRODUCTION

Regarding definition of cloud computing model, the most widely used one is made by NIST as "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models". The cloud computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are : Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS) [1].

Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution [2], [13]. This viewpoint is shared by many distinct groups, including academia researchers [3], business decision makers and government organizations [4] and Improved Load Management In Cloud

Environment Using MHT Algorithm [12]. The many similarities in these perspectives indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and reputation fate sharing.

2. PROPOSED ALGORITHM

2.1. Problem Formulation

Data protection is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. To build the trust for the growth of cloud computing, cloud providers must protect the user data from unauthorized access and disclosure. One technique could be encrypting the data on client side before storing it in cloud storage.

2.2. Research Problem

Encrypting data on client machine and then storing the information to public cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more difficult for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. In proposed work we will use various encryption description algorithms like Advanced Encryption Standard (AES), Ron Rivest, Adi Shamir and Len Adleman (RSA) etc. to compare with proposed approach.

2.3. Research Methodology

There are various simulators are used for simulating the above algorithms. The appropriate simulator will be used for simulating the proposed algorithm and comparison with other algorithms. In proposed work graphical comparisons will be done to compare various parameters for result discussion. Time monitoring of the whole process will be done to ensure it’s feasible in real-time environment of a network.

2.4. Algorithmic Approach

Step 1: Initialize & Activate Cloud Virtual Machine Packet P_i at Cloud Environment Source End S_i for transmission to Cloud Environment Destination D_i

Step 2: Cloud Virtual Machine Packet Encryption Module PE_k based on Dynamic Key k Generation, once the Cloud Virtual Machine Packet moves from Cloud Environment Source End S_i

$$C_{i\,:} = PE_k\,(P_i) \tag{1}$$

Step 3: Transmission of Encrypted Cloud Virtual Machine Packet C_i using specified Path/Route R_i

$$C_i \rightarrow D_i\,[R_i] \tag{2}$$

Step 4: Cloud Virtual Machine Packet Authentication on Decryption

IF ($C_i = PD_k\,(C_i)$ // Cloud Virtual Machine Packet Decryption Module PD_k
to decrypt the Cloud Virtual Machine Packet at Cloud Environment Destination (3)

BEGIN

```
          (a)  DEST [i] := $PD_k$ ($C_i$)                                                   (4)
          (b)  Successful Delivery of Cloud Virtual Machine Packet
          (c)  ACK sent to Cloud Environment Source End $S_i$     // Acknowledgement ACK is delivered
               to Cloud Environment Source End in case of Success
      END
      ELSE
      BEGIN
          (a)  A record will be inserted in the Forensic Database. The Interception Table will consist of the
               Structure (Id, Interception Type, Timestamp of Interception).  // Acknowledgement ACK is
               sent to Forensic Database in case of Failure Attempt
          (b)  Cloud Environment Source End $S_i$ senses the Forensic Database.
               Select All Records from Forensic Database
               IF (true)Then
               print "Failure Delivery, Retransmit the Cloud Virtual Machine Packet"
          (c)  GOTO Step 1
          (d)  Update Forensic Analyzer Database for taking remedial actions.
      END
Step 5:   Forensic Analyzer
          (a)  Retrieve Records for analysis of interceptions.
          (b)  Analyze the type $T_i$ of Intercept
          (c)  Perform remedial stroke for avoiding the stored interception type
```

The proposed architecture consists of various phases which will include algorithms for encryption and decryption of data Cloud Virtual Machine Packet along with the technique to analyze the overall interception patterns.

2.5. PHASE - 1

```
Step 1:   Activate and Initialize the Cloud Virtual Machine Packet $P_i$
Step 2:   Generate a Random Key $K_R$ by analyzing number of 1s in Cloud Virtual Machine Packet.
      (a)  Develop a routine to count bits in the Data Cloud Virtual Machine Packet
      (b)  Set N := Count($P_i$) // Count Number of 1's in the Data Cloud Virtual Machine Packet.   (5)
      (c)  Set $K_R$ :=N // Store N in Random Number $K_R$                                          (6)
Step 3:   Apply XOR (Exclusive-OR) Operation
      (a)  Set $E_{K\,:}= P_i \oplus K_R$                                                          (7)
      (b)  The Encrypted Cloud Virtual Machine Packet $E_K$ is generated using XOR Operation.
      (c)  Set $PE_K$ :=$E_K$ // Utilize $E_K$ as Encrypted Cloud Virtual Machine Packet            (8)
```

```
Step 4:  Cloud Virtual Machine Packet equipped for Transmission
```

2.6. PHASE - 2

```
Step 1:  Receive the Encrypted Cloud Virtual Machine Packet $PE_K$
Step 2:  Check the Front $PF_i$ and Rear End $PR_i$ of Cloud Virtual Machine Packet
         if ($PF_i = PR_i$)                                    (9)
         Accept PFi                                            (10)
         Set $K_R := PF_i$                                     (11)
         else
         goto Step 5
Step 3:  Generate the Binary Equivalent of $K_R$
         $PB_i = Binary(K_R)$                                  (12)
Step 4:  Perform XOR Operation
         if ($PB_i = PE_K$)                                    (13)
             Decryption Successful
             Accept the Cloud Virtual Machine Packet
         else
             goto step 5
Step 5:  Insert the Record of Corrupt Cloud Virtual Machine Packet in Forensic Database
```

3. EXPERIMENT AND RESULT

To analyze the performance of proposed algorithm with RSA, AES, MD5 based on parameters - file size and average response time.

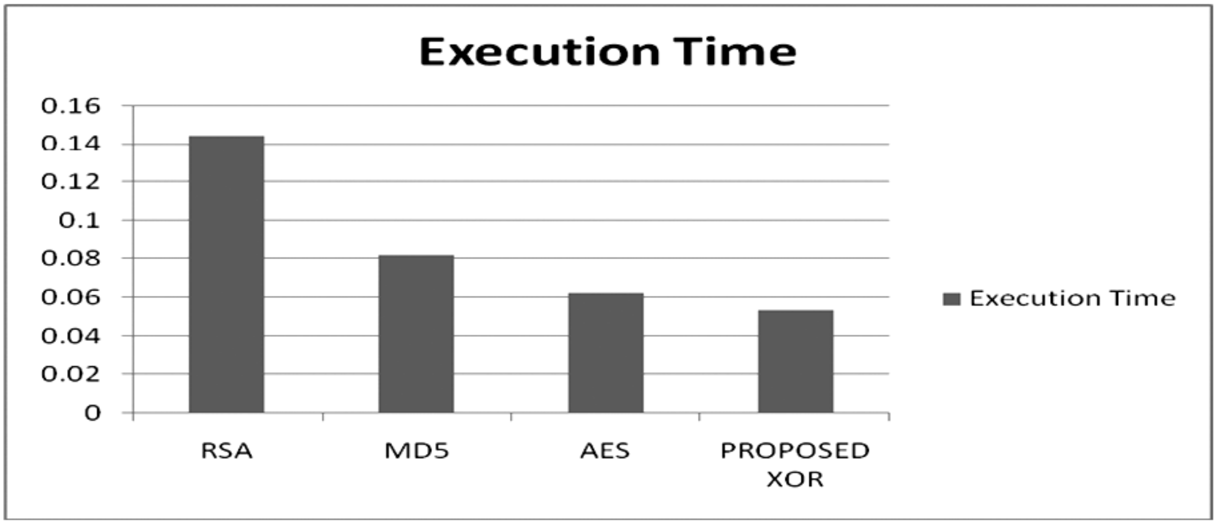

Figure 1: Comparative Analysis of Time Factor

Fig. 1 depicts that the proposed approach is relatively better than the other approaches as shown in the results. The proposed XOR based approach is effectual and giving enhanced results in terms of lesser execution time.

Fig. 2 based line graph depicts that the proposed approach is relatively better than the other approaches as shown in the results. The proposed XOR based approach is effectual and giving enhanced results in terms of lesser execution time.

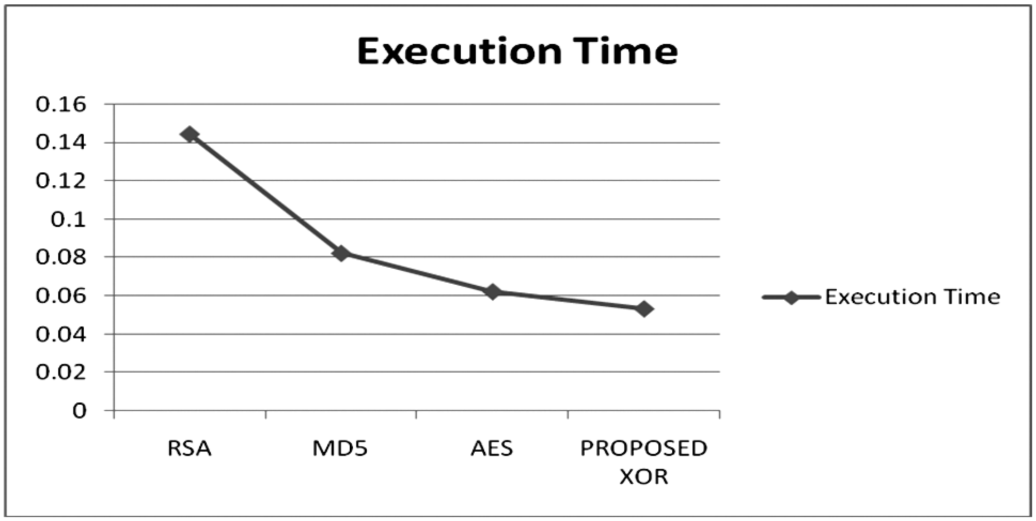

Figure 2: Comparative Analysis of Time Factor

Table 1
Parameter Based Evaluation of Algorithms

	RSA	MD5	AES	PROPOSED XOR
Execution Time	0.14432	0.08234	0.062383	0.0534858
Complexity	72.16	41.17	31.1916	26.7429
Cost Factor	87	68	48	30
Performance	64	72	82	92

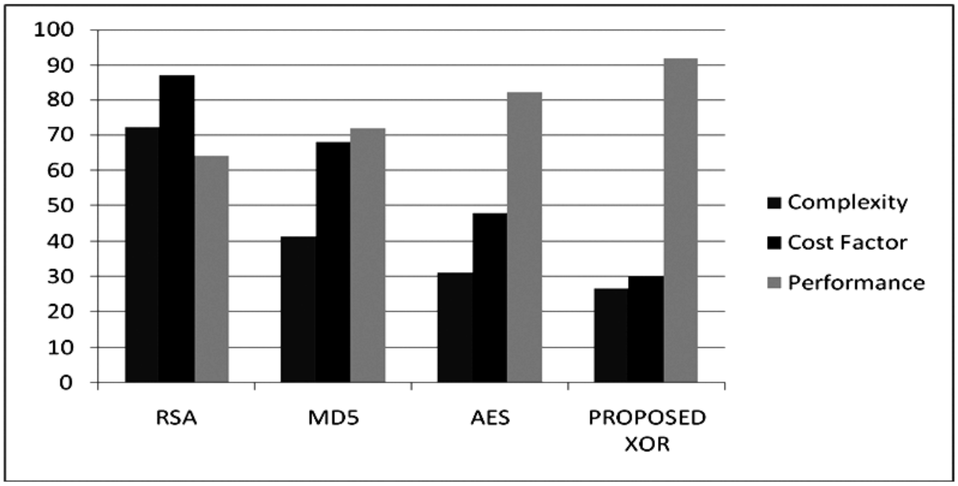

Figure 3: Comparative Analysis of Assorted Parameters

Fig. 3 bar graph based results depicts that the proposed approach is relatively better on multiple parameters and effective than the other approaches as shown in the results. The proposed XOR based approach is effectual and giving enhanced results on multiple parameters.

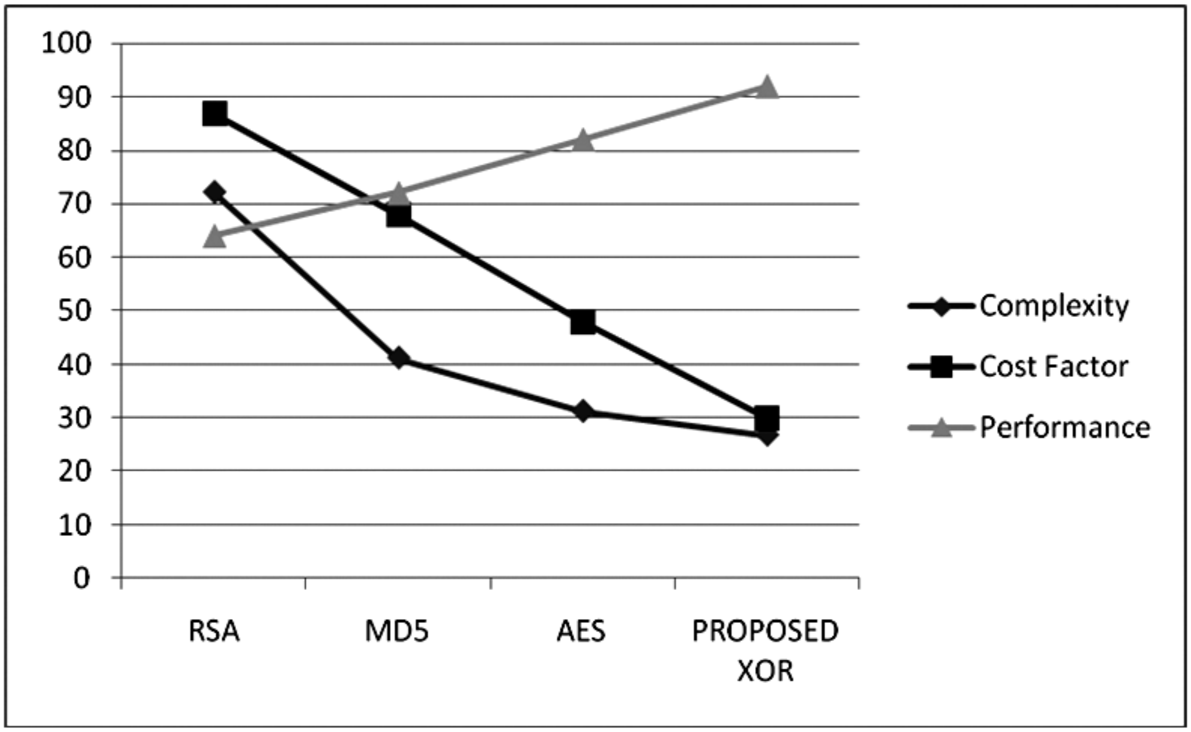

Figure 4: Comparative Analysis of Assorted Parameters

Fig. 4 line graph based results depicts that the proposed approach is relatively better on multiple parameters and effective than the other approaches as shown in the results. The proposed XOR based approach is effectual and giving enhanced results on multiple parameters.

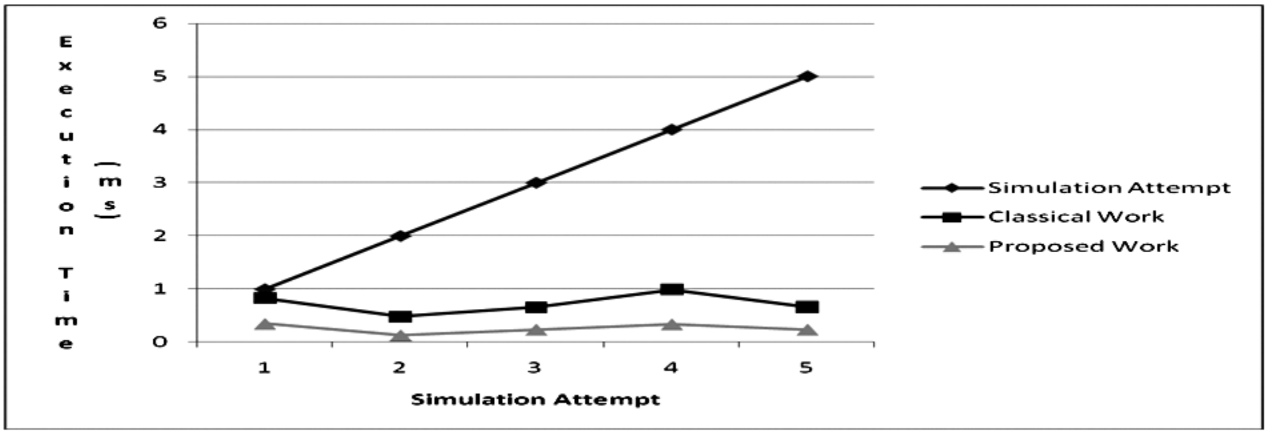

Figure 5: Line Graph Analysis of the Classical and Proposed Approach

Fig. 5 line graphical representation depicts that the proposed approach is relatively better than the other approach as shown in the results. The proposed XOR based approach is effectual and giving enhanced results in terms of lesser execution time.

Table 3
Comparative Analysis based on Cost Factor

Simulation Attempt	*Cost Factor - Classical Work*	*Cost Factor - Proposed Work*
1	89	70
2	78	60
3	67	59
4	76	40
5	49	20

Table 4
Comparative Analysis based on Security Factor

Simulation Attempt	*Security Factor - Classical Work*	*Security Factor - Proposed Work*
1	67	85
2	47	86
3	69	89
4	47	97
5	64	98

Fig. 6 line graphical representation depicts that the proposed approach is relatively better than the other approach as shown in the results. The proposed XOR based approach is effectual and giving enhanced results in terms of higher security factor and optimization.

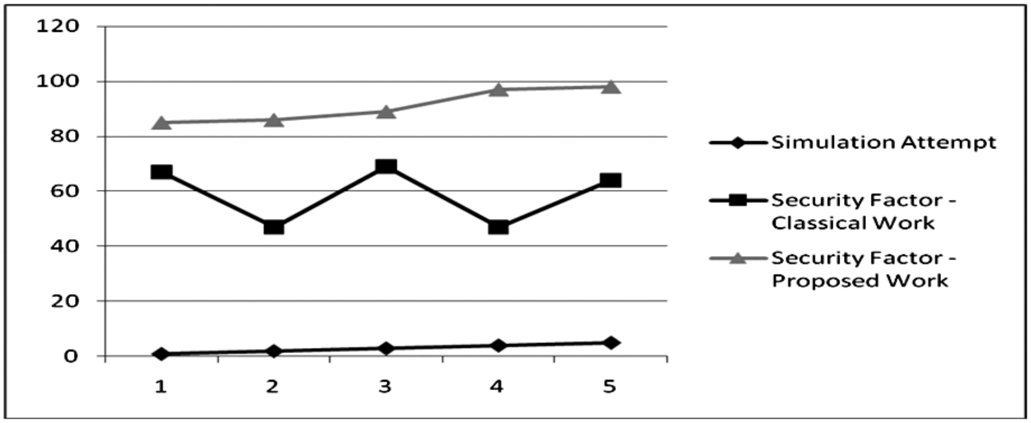

Figure 6: Line Graph Analysis of the Classical and Proposed Approach (Security Factor)

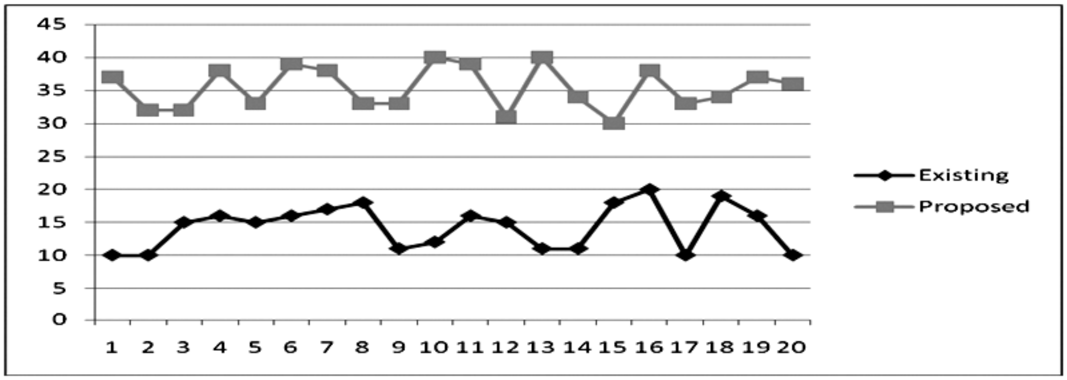

Figure 7: Line Graph Comparison between Existing and Proposed Approach

Fig. 7 line graphical representation depicts that the proposed approach is relatively better than the other approach as shown in the results. The proposed XOR based approach is effectual and giving enhanced results in terms of higher security factor and optimization.

4. CONCLUSION & FUTURE SCOPE

4.1. Conclusion

A new and innovative algorithm for cloud environment is proposed in this thesis which combines the three security solutions - cryptographic solution (system solutions), trust-based solution (behavioural solutions) and authentication (hybrid solutions). The main objective of this algorithm is to store, process and access the data according to their sensitivity or privacy need and data owner is able to control and manage the privacy mechanisms required to maintain the security of sensitive data which is achieved with the help of three different security schemes where each security scheme is different from each other in the manners of privacy aspects followed to store, process and access the privacy categorized data.

- The proposed algorithm is also analysed in terms of their security performance and computational efficiency.
- A data owner centric three- tier privacy aware cloud computing model is also proposed to implement the algorithm in real-time cloud environment. For implementation purpose this thesis takes the advantage of ‘pay-as-you-grow’ feature and ‘platform-as-a-service’ facility provided by cloud.
- The implementation of three-tier privacy aware cloud computing model is done in real-time cloud environment which is created using a website hosting platform. The cloud service provider offers the website hosting platform according to pay-per- use strategy by using the platform as a service model. Finally the results evaluated in the form of Query Execution Time. But these results are not enough and there are several directions in which this investigation can go in.

4.2. Future Scope

The cryptographic techniques are essential, but not the only one, method to protect private data against partially trustworthy cloud server. Therefore, future work of this research might include the tolerance power of proposed model may be checked by implementing and penetrating various attacks. After the tolerance test we may come to a conclusion about its robustness in terms of confidentiality, integrity and authenticity. The combination of access control techniques and cryptographic techniques may be used to maintain more privacy and security of data within the cloud.

REFERENCES

[1] Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. Future Generation computer systems, 28(3), pp.583-592.

[2] A. Kumar, Surender and Rajiv Mahajan, “A Modified Heuristic-Block Protocol Model for Privacy and Concurrency in Cloud”, Published in International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6, No. 9, 2015, Pg. 179-184.

[3] Xu, J., Jiang, D., Wang, B., Yang, D. and Reiff-Marganiec, S., 2015, June. Local reputation management in cloud computing. In Services (SERVICES), 2015 IEEE World Congress on (pp. 261-267). IEEE.

[4] Tian, L.Q., Lin, C. and Ni, Y., 2010, October. Evaluation of user behavior trust in cloud computing. In Computer Application and System Modeling (ICCASM), 2010 International Conference on (Vol. 7, pp. V7-567). IEEE.

[5] Padhy, R.P., Patra, M.R. and Satapathy, S.C., 2011. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), pp.136-146.

[6] Manuel, P.D., Selvi, S.T. and Abd-El Barr, M.I., 2009, December. Trust management system for grid and cloud resources. In Advanced Computing, 2009. ICAC 2009. First International Conference on (pp. 176-181). IEEE.

[7] Reddy, V.K. and Reddy, L.S.S., 2011. Security architecture of cloud computing. International Journal of Engineering Science and Technology (IJEST), 3(9), pp.7149-7155.

[8] Bendale, Y. and Shah, S., 2013. User Level Trust Evaluation in Cloud Computing. International Journal of Computer Applications, 69(24).

[9] Gambhir, S., Rawat, A. and Sushil, R., 2013. Cloud Auditing: Privacy Preserving using Fully Homomorphic Encryption in TPA. International Journal of Computer Applications, 80(14).

[10] Li, X., Ma, H., Zhou, F. and Yao, W., 2015. T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services. IEEE Transactions on Information Forensics and Security, 10(7), pp.1402-1415.

[11] Noor, T.H., Sheng, Q.Z., Ngu, A.H., Alfazi, A. and Law, J., 2013, October. Cloud armor: a platform for credibility-based trust management of cloud services. In Proceedings of the 22nd ACM international conference on Conference on information & knowledge management (pp. 2509-2512). ACM.

[12] Akhilesh Kumar Bhardwaj, Rajiv Mahajan and Surinder, "Improved Load Management In Cloud Environment Using MHT Algorithm", published in, "Int'l J. of Control Theory and Applications" Vol. 9(22), 2016, pg. 301-305.

[13] A. K. Bhardwaj, Rajiv Mahajan and Surender, "TTP based Vivid Protocol Design for Authentication and Security for Cloud", published in IEEE Xplore; Pg. 3275-3278 (2016).

[14] Rabi Prasad Padhy, ManasRanjanPatra and Suresh Chandra Satapathy, "Cloud Computing : Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.

[15] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN : 1084-8045.

[16] V. Krishna Reddy, B. ThirumalRao, Dr. L.S.S. Reddy, P.SaiKiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[17] Nelson Gonzalez, Charles Miers, Fernando Red´ygolo and Mats N¨aslund, "A quantitative analysis of current securityconcerns and solutions for cloud computing", SPRINGER, 2012.

[18] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", IEEE, PP. 647-651, Dec. 2012.

[19] Pinal V Chauhan, "Cloud Computing In Distributed System", IJERT, ISSN : 2278-0181, Vol. 1, Issue 10, December, 2012.

[20] Priyanka V. Mogre, GirishAgarwal and PragatiPatil, "Data Security And Its Techniques In Cloud Storage – A Review", IJERT, Vol 1, Issue 10, December 2012.

[21] K. Srilaxmi and M.Madhavi, "A Review on Cloud Computing", IJERT, Vol 1, Issue 10, December 2012.

[22] Pankaj Arora, RubalChaudhryWadhawan and Er. Satinder Pal Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service", IJARCSSE, Vol. 2, Issue 1, 1 January, 2012.