Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Exclusive OR (XOR) based Enhanced Data Security Algorithm for Cloud Environment

Pawan Kumar
Ph.D Research Scholar, Department of Computer Science and Engineering
IKG Punjab Technical University, Jalandhar Punjab, India

Surender Jangra
Assistant Professor, Department of Computer Applications
Guru Tegh Bahadur College, Bhawanigarh, Sangrur, Punjab, India

Sawtantar Singh
Professor, Department of Computer Science,
BMSCE, Mukatsar Punjab, India

Abstract: With the advent and adoption of cloud services in assorted segments, the vulnerability and security issues are escalating very rapidly and therefore there is the increasing need to work out the specialized and highly secured environments so that overall trust and effectiveness of cloud based services can be setup. A number of algorithms and approaches are devised so far by number of researchers and practitioners; still there is huge scope and thrust of the novel algorithms so that the cloud services can be adopted without any security predicament. The key objective and goal in this research work is to deeply investigate the diverse algorithms of security which are used in the cloud environment. This research manuscript underlines and proposes a new Exclusive OR (XOR) based encryption algorithm to enhance the data security to greater degree. The implementation of the projected novel approach is done and compared with the parameters associated with RSA, AES, MD5 based on parameters - file size and average response time.

Keywords – Cloud Computing, Cloud Security, Encryption Approaches, Performance of Cryptography on Cloud

I. INTRODUCTION

Cloud Computing [1], [8-11] is one of the exhortations in the current era of distributed and high performance computing. Most of the computing services are now delivered using cloud environment from number of cloud service providers. The cloud computing can be used for any type of automation and computing services which includes infrastructure, memory or software. In traditional perspectives, these are known as Infrastructure as a Service (IaaS) [2], Storage as a Service, Platform as a Service (PaaS) [3], Testing as a Service and Software as a Service (SaaS) [4].

There is a diversified set of cloud service providers which are engaged in delivering the cloud services with higher performance and trust factors.

II. PROPOSED RESEARCH WORK

2.1 Problem Formulation

As there are number of security issues in cloud services, it is required to devise and implement the security aware algorithms for cloud computing [6]. As per the reports, the distributed denial of service (DDoS) and Sybil were most common attacks in year 2016-17 [7]. The vulnerabilities because of malware and key intrusion is very frequent and therefore this research work is having the key focus on key based security so that the overall performance and efficiency can be improved.

2.2 Research Problem

The classical approaches and algorithms are in implementation from a long time which needs to be updated with new and effective modules so that the multilayered security can be imposed with higher intensity of cloud defense.

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

The novel projected architecture is having a set of multiple layers which function in association with each other so that the higher degree of security and integrity can be maintained.

ALGORITHMIC APPROACH

Layer 1: Initialize & Stimulate Cloudlet P_i at CloudSource (CS) S_i for transmission to Cloud Destination (CD) CD_i
Layer 2: Cloudlet Encryption Phase PE_k Cloudlet enlisted CloudSource (CS)
$EC_{i:} = CPE_k (P_i)$
Layer 3: Transmission of Enciphered Cloudlet EC_i using specified Path/Route R_i
$EC_i \rightarrow CD_i [R_i]$
Layer 4: ***Cloudlet Authentication on Decryption***
IF ($EC_i = CPD_k (EC_i)$
BEGIN
(a) *CloudDest [i] :=* $CPD_k (EC_i)$
(b) *Successful Delivery of Cloudlet*
(c) *ACK sent to CloudSource (CS)* CS_i

END
ELSE

BEGIN

(a) *A log inserted with Forensic Database*

(b) *CloudSource (CS) CS_i deeply learn the forensic database FD*

List Records FD

While not False

print "Malfunction Attempt, ReAttempt for Cloudlet"

(c) *GOTO Layer 1*

(d) *FD Updated*

END

Layer 5: ***Deep Learning of Cloudlets and Predictive Analyzer***

(a) *Fetch List of intrusions.*

(b) *Analyze the type T_i of interrupt*

(c) *Implementation of Avoidance Approach*

CLOUDLET ENCRYPTION ALGORITHM

At the initial stage, the Cloudlet will be transmitted from CloudSource (CS) to Cloud Destination (CD) over transmission media using efficient cryptographic algorithm to encrypt the entire Cloudlet.

ENCRYPTION OR ENCIPHER APPROACH

Layer 1: Stimulate the Cloudlet P_i

Layer 2: Spawn a indiscriminate Cloud Key CK_R

(a) Build-Up module for encryption

(b) Activate CCN := Count(CCP_i)

(c) Activate CCK_R :=CCN

Layer 3: Integrate Exclusive-OR (XOR)

(a) Activate CCE_K := $CP_{i\ op.C}CK_R$

(b) The Enciphered Cloudlet CCE_K Spawnd

(c) Assign CPE_K :=CE_K

Layer 4: Cloudlet equipped for Transmission

ON-CLOUD DECIPHER AND INTERCEPT DETECTION ALGORITHM

ALGORITHM

Layer 1: Fetch the Enciphered Cloudlet PE_K

Layer 2: Analyze the Front CPF_i and Rear End CPR_i of Cloudlet

if (CPF_i = CPR_i)

Fetch and Log CPFi

Activate CK_R := CPF_i

else

goto Layer 5

Layer 3: Generation of the Binary Equivalent of K_R

CPB_i = Binary(CK_R)

Layer 4: Execute XOR

if (CPB_i =CPE_K)

On-cloud decipher Successful

Fetch and Log the Cloudlet

else

goto Layer 5

Layer 5: Insert the Log of Corrupt Cloudlet in Back-End Forensic Database

III. EXPERIMENT AND RESULT

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

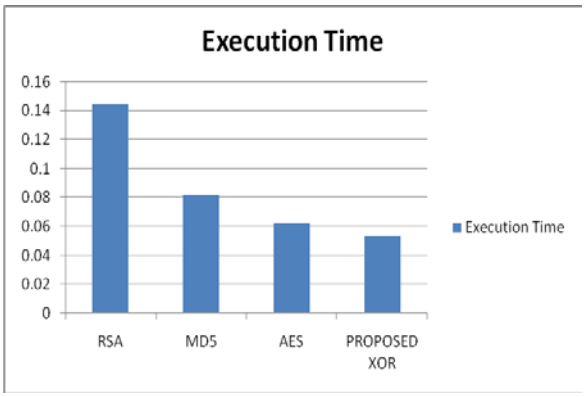

Figure 1: Comparative Analysis of Time Factor

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.

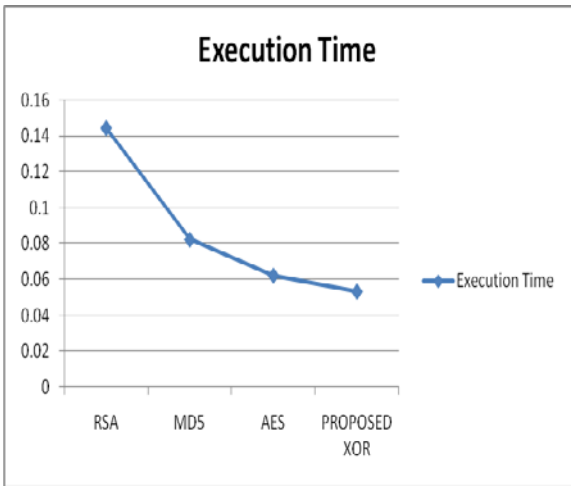

Figure 2 – Evaluation of algorithms based on the factor of Execution Time

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.

Table 1: Evaluation of algorithms based on the assorted factors and parameters

	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

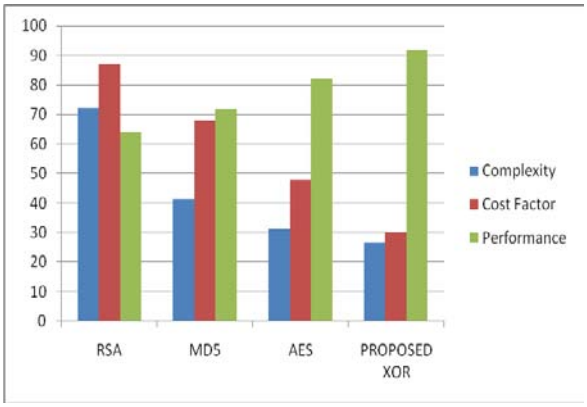

Figure 3: Evaluation of algorithms based on the factors of Complexity, Cost and Performance

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.

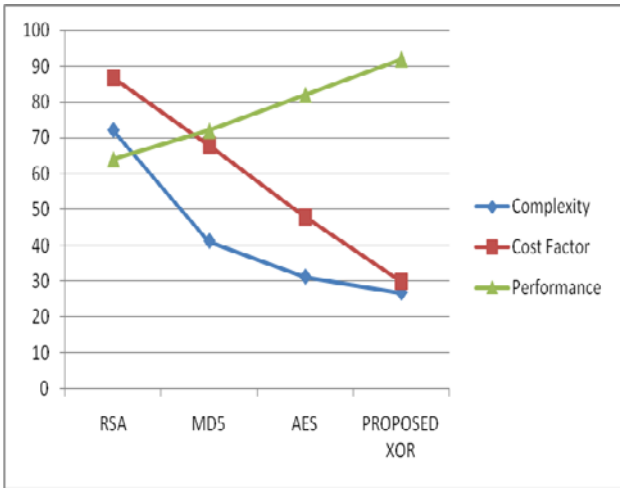

Figure 4: Evaluation of algorithms based on the factors of Complexity, Cost and Performance

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.

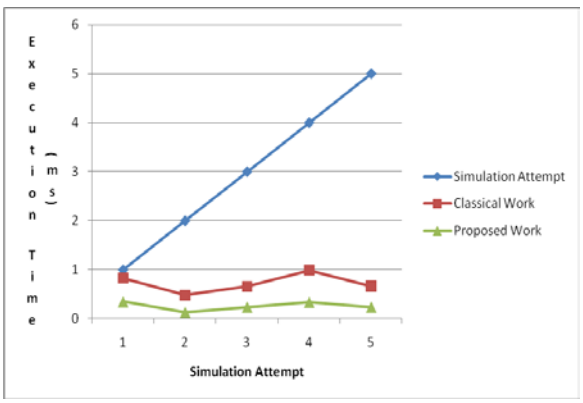

Figure 5: Evaluation of traditional and projected algorithm

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

Table 2 – 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 3 – 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

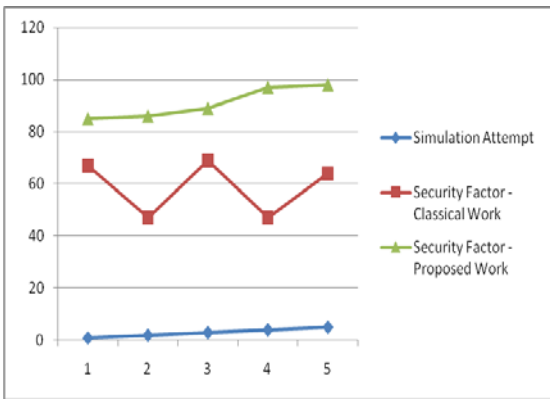

Figure 6: Evaluation on Security Parameter in the traditional and novel implemented algorithm

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

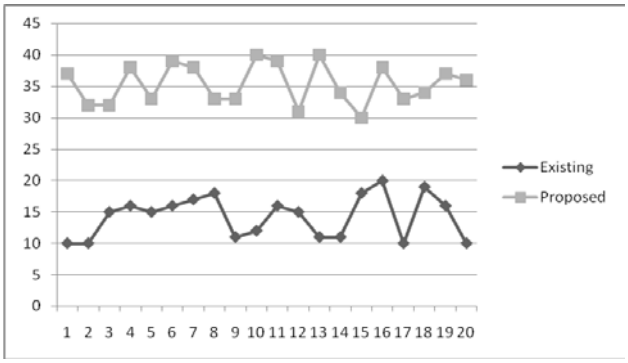

Figure 7: Evaluation of traditional and projected approach in form of line graph

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

IV. CONCLUSION

This proposed work is proposed to give the effective results to minimize the error rate and high effectiveness in receiving the higher probability factor of more security still this work can be more enhanced using other optimization approaches. There exist another approach hyper-heuristic that can be integrated for deep learning of cloud vulnerabilities and predictive analysis.

For the scope of future work, the integration of metaheuristic and soft computing approaches can be used for higher degree of performance and efficiency on multi dimensional perspectives. The soft computing and metaheuristic approaches which are highly optimized by the nature include Ant Colony Optimization, Bat Algorithm, Bayesian Network, Bees Algorithm, Cuckoo Search, Lion Algorithm, Elephant Approach, Evolutionary Approaches, Firefly Algorithm, Flower Pollination Algorithm, Fuzzy Logic, Metaheuristics, Nature Inspired Algorithms, Particle Swarm Optimization, River Formation Dynamics, Simulated Annealing, Support Vector Machines, Swarm Intelligence and many others.

REFERENCES

[1] Mell, P., & Grance, T., "The NIST definition of cloud computing (2011)".

[2] Zhang, Q., Cheng, L., & Boutaba, R., "Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications, 1(1), pp. 7-18 (2010).

[3] Boniface, M., Nasser, B., Papay, J., Phillips, S. C., Servin, A., Yang, X., ... & Kousiouris, G., " Platform-as-a-service architecture for real-time quality of service management in clouds", In Internet and Web Applications and Services (ICIW), IEEE 2010 Fifth International Conference on (pp. 155-160).

[4] Godse, M., & Mulik, S., "An approach for selecting software-as-a-service (SaaS) product", In Cloud Computing, CLOUD'09, IEEE International Conference on , pp. 155-158, (2009).

[5] Dillon, T., Wu, C., & Chang, E., "Cloud computing: issues and challenges", In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on (pp. 27-33).

[6] Tebaa, M., El Hajji, S., & El Ghazi, A., " Homomorphic encryption applied to the cloud computing security", In Proceedings of the World Congress on Engineering , Vol. 1, pp. 4-6 (2012).

[7] Sood, R., Garg, S., & Palta, P., " A Novel Approach to Data Filtration against Packet Flooded Attacks in Cloud Service", Journal of Network Communications and Emerging Technologies (JNCET), Vol. 6(5), (2016).

[8] A. K. Bhardwaj, R. 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), pp. 301-305 (2016)

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

[10] P. Kumar, S. Singh and Surender Jangra, "Design and Implementation of Encryption based Data Security Algorithm for Cloud Environments ", Published in, "*Int'l J. of Control Theory and Applications"*, Vol. 10, Issue No. 15, Pg. 163-171, (2017).

[11] A. Kumar, Surender and R. 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, Pg. 179-184, (2015).