Reliable Cyber Security And Improvement In E-Learning System

Aman Kumar[1], Dr. Anil Pandit[2], Dr. Sumanjeet Singh[3]

[1]*Research Scholar, GNA University, Phagwara, Punjab & Assistant Professor, NIFT Kangra, Himachal Pradesh*
[2]*Assistant Professor, GNA University, Phagwara Punjab, India*
[3]*Associate Professor, Ramjas College, University of Delhi*

Abstracts. Some of the cloud-based education solutions for distance learning that have been previously offered have a lack of security. Researchers have decided to strengthen security rather than reduce it, but this raises the question of performance, as it takes a long time to safeguard the data. Consideration of performance and security challenges in a cloud-based education system for remote learning is the topic of this research article. It is necessary to have a system in place that can protect educational materials while not impairing student learning. An online education system based on the cloud and its approach and constraints is discussed in this study. To ensure both security and performance, new research is needed, and the breadth of such a system is described. E-learning system security and performance have been the topic of an academic study in the field of cyber-security. Simulated results are compared against RSA-based results.

Keywords: Cyber security, Cloud Environment, Performance, Security, E-learning

Introduction. E-Learning security concerns include preventing data modification, user authentication fraud, and confidentiality breaches. Interoperability for apps, learning environments, and heterogeneous systems is becoming increasingly important in the current e-Learning landscape. For example, Graf (2002) claims that the employment of information communication technology in online learning might lead to several security problems such as unauthorized access to essential data as well as vandalism of public information services.

Main Cyber Security Threats

1. Ransomware – Attackers encrypt an organization’s data, and they demand cash to decrypt it.
2. Cryptojacking – When fraudsters exploit a victim's computer to mine bitcoin without their knowledge.
3. Threats against data – Breach of data.

1.3.1 Security Factors

In a cloud system, viruses and external assaults have resulted in Security Treats. As a result, instructional information on a network might be compromised. Hackers are responsible to get unauthenticated access to data. Crackers are on the other side, responsible for breaking the encryption. Security measures like encryption and firewalls are commonly employed. The following assaults, however, have the potential to compromise security attacks:

1. Brute Force
2. Trojan Horse
3. Man in Middle
4. Denial of Service
5. SQL Injection

1.3.2 Performance Factors

Increasing the system's security requires the adoption of time-consuming encryption techniques that also impact the system's performance. Numerous variables can affect how well a cloud environment performs.

1. **Transmission media:** The performance of the system is affected by the type of transmission media used, whether wired or wireless. Compared to a wired connection speed, wireless media typically lags behind. Furthermore, wireless and wired systems are subdivided into other subcategories.

2. **Bandwidth:** In computing, bandwidth refers to the amount of data that can be transmitted in a given amount of time. Faster transmission of bigger volumes of data is made possible by increased bandwidth.

3. **The protocol used for high-speed transmission:** On the network, protocols govern how information flows. Compared to the transmission control protocol, a connection-less protocol, like the user datagram protocol (UDP) that does not require acknowledgement, is more efficient.

4. **Security mechanism:** Because it takes so long to verify whether or not a communication is genuine, the security mechanism used on the cloud network can sometimes slow down the network's activities.

5. **Distance:** Transmission quality is influenced by transmission distance. Increasing the distance increases the transmission time, and performance slows. Because of this, a shorter distance results in better performance.

6. **Compression mechanism:** Compression can be used to lower the file size of the content used in the online learning system. The problem of data loss remains, despite the existence of numerous compression algorithms. In a replacement table, words with a high frequency of occurrence must be replaced by smaller-sized alternatives. Switching from long to short words can reduce the size of a packet. Because of this, the packet's transmission time is shaved off of it. In addition, packets of a smaller size go over the network more quickly, reducing the risk of packet loss. As a result, an online learning system that uses this compression approach may benefit from faster packet transfer.

[2] MOTIVATION

The integration of Electronic Learning into the cloud computing environment has resulted in a wide range of studies [1]. Several scholars are debating whether cloud computing [2] should be used in schools. For distant learning, web technologies [3] access to information and resources has been found to be facilitated. It is also possible to share information and applications using a dynamic web system, which has been shown to be the newest technology. A nation's financial development is aided by education, according to extant studies [4]. Poverty may be eliminated in a country via education. Many obstacles have arisen due to the quick development objectives and constantly changing technologies. Higher education institutions in the contemporary period have concentrated on the most cutting-edge technology and resources to study learning. The Internet and a multitude of educational materials have combined to create a worldwide phenomenon. A word processor and a spreadsheet are only two examples of software that can assist in processing academic material. The distribution of educational resources among countries has been shown to be unequal. Developing nations require affordable online education for impoverished pupils. The use of the cloud as a platform for new teaching practices is becoming increasingly common. In order to build teaching materials and manage the teaching, a supportive environment must be created. According to previous studies, there are a number of security models [5]. In order to protect the cloud-based material DNA, AES, DES, RSA security, and various security procedures have been discussed. These studies have prompted the development of cloud-based educational content security measures. Only a small number of studies have looked at how well clouds perform. Consequently, it is necessary to increase the pace at which instructional information is transmitted securely through the cloud.

[3] LITERATURE REVIEW

Distance learning has been the subject of a wide range of studies. Several studies have looked at how to increase the scalability and diversity of educational content in a cloud-based distance learning system. E-learning for remote education using cloud computing has been discussed in this area. Also included in the presentation is a research paper that provides cloud application security and compresses material via the cloud. These topics include cloud-based e-learning, data compression, and cloud security in this portion of the article.

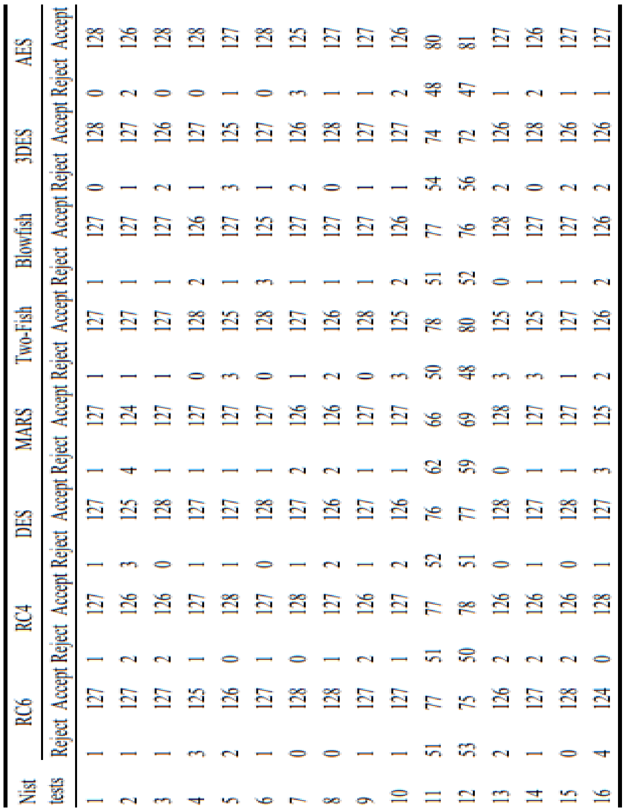
In 2016, Dr. Pranav Patil et al. [1] did a study on distance education using electronic means. When practising, they employ Cloud Computing technology. A current E-Learning system has been examined in their work. They came up with a concept for using cloud computing in online teaching. The integration of Electronic Learning has been used to describe the architecture of a cloud computing system.

In 2014, Asgarali Bouyer et al. [2] represented the need for cloud computing in online education. Dynamic scalability of cloud computing has been discovered throughout their research. This device can provide a web-enabled service. Because of technological advancements, virtual technologies are becoming increasingly significant in online learning. Researchers have outlined the benefits of online training. There has been a focus on both the qualitative and quantitative aspects of online education in the research conducted. Both educational institutions and students of technical science and engineering benefit from research. The focus of the study was on the use of a cloud computing-based online education system.

In 2016, Agah Tugrul et al. [3] represented the characteristics and features of cloud computing systems that were employed in online education. Data utilized in education is becoming more diverse and important, according to the findings of the study. This is primarily due to advances in technology. Web technologies and their contributions to a distance learning system were examined in a study. Additionally, mobile systems, a popular and extensively used technology in distance education, were considered in the study. It has made web-based technology more accessible. Individuals may now access info on the web regardless of where they are or how much time has passed. Furthermore, it has been found that both students and teachers benefit greatly from the ability to save and retrieve instructional data and resources. This study examined the use of cloud services in education. They looked into the benefits of cloud computing services. The survey approach was used in this study.

In 2019, Ananthi Claral Mary et al. [4] presented cloud computing implications and problems for academics. Several advantages have been brought about by cloud computing in the academic arena. It is possible to have security concerns if you use the cloud to store and process confidential data. Cloud computing security flaws have been outlined in this study, as well as a way to avoid attacks on the cloud environment.

In 2013, Meslhy [5] presented data security models that were necessary to secure cloud applications. Using a single default gateway, this research study proposes a data security approach that protects sensitive user information across various public and private cloud services. This gateway platform encrypts critical data before it is sent to cloud storage, preventing cloud apps from being crashed during the transmission process. With the help of this research, a fast encryption technique with file integrity has been developed. Additionally, it provides anti-malware, firewall, and tokenization capabilities. Due to malware detection and firewall restrictions, and slowdowns, this security strategy has lowered performance by 7%.



Nist	RC6		RC4		DES		MARS		Two-Fish		Blowfish		3DES		AES	
tests	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept	Reject	Accept
1	1	127	1	127	1	127	1	127	1	127	1	127	0	128	0	128
2	1	127	2	126	3	125	4	124	1	127	1	127	1	127	2	126
3	1	127	2	126	0	128	1	127	1	127	1	127	2	126	0	128
4	3	125	1	127	1	127	1	127	0	128	2	126	1	127	0	128
5	2	126	0	128	1	127	1	127	3	125	1	127	3	125	1	127
6	1	127	1	127	0	128	1	127	0	128	3	125	1	127	0	128
7	0	128	0	128	1	127	2	126	1	127	1	127	2	126	3	125
8	0	128	1	127	2	126	2	126	2	126	1	127	0	128	1	127
9	1	127	2	126	1	127	1	127	0	128	1	127	1	127	1	127
10	1	127	1	127	2	126	1	127	3	125	2	126	1	127	2	126
11	51	77	51	77	52	76	62	66	50	78	51	77	54	74	48	80
12	53	75	50	78	51	77	59	69	48	80	52	76	56	72	47	81
13	2	126	2	126	0	128	0	128	3	125	0	128	2	126	1	127
14	1	127	2	126	1	127	1	127	3	125	1	127	0	128	2	126
15	0	128	2	126	0	128	1	127	1	127	1	127	2	126	1	127
16	4	124	0	128	1	127	3	125	2	126	2	126	2	126	1	127

Fig. 1. Amazon EC2 rejection rate for modern encryption algorithms

[Ref: Yadav, et.al. (2020). Design and Implementation Technique for Cloud Computing

Security Improvement]

In 2016, Osman, Saife [6] presented virtual learning Environment Systems that require performance analysis of cloud-dependent online services. Cloud-based web services may be used in diverse contexts, according to a study. Soap and REST might be used to implement these services. Some excellent services are being offered by protocols. The performance study's findings helped optimize the overloud web services environment. Response time and throughput during cloud access to quiz web services have been studied in detail. Security precautions have resulted in a 5% increase in response time.

In 2019, Pandey, G. P. [7] implemented using DNA Cryptography; the cloud application was kept safe. The Huffman Algorithm has been utilized for compression in research. The author employed socket programming to facilitate transfer between sender and recipient programmers. Mechanisms for securing compressed data in the cloud have been developed via research. The system's performance has been impacted by 13 per cent due to the mechanism.

In 2016, P. Suresh [8] presented RSA ALGORITHM was being used to conduct research on cloud security. Algorithms like AES, DES, RSA, and others have been studied for their encryption and decryption capabilities. An asymmetric key algorithm was used to implement RSA in this study. It has been encrypted and decrypted using different key sizes. Security mechanisms, on the other hand, reduce system performance by 20%.

Table 1. Comparison of DES, AES and RSA considering contributor, key length , block size and security rate

Factors	**DES**	**AES**	**RSA**
Contributor	IBM 75	Rijman Joan	Rivest Shamir 78
Key length	56- Bits	128,192 and 256	Based on No. of bit in N=A*B
Block size	64 Bits	128 bits	variant
Security rate	Not Enough	Medium	Good

In 2016, Singh, S. K [9] The RSA method was used in a study on cloud application data security. It has been determined that RSA Algorithm's performance depends on three factors, which the author has investigated. Throughput, Space Complexity and Timing Completion are the three main factors to consider. A method called RSA has been employed in this study to encrypt data so that only legitimate users may access it. Before being uploaded to the cloud, all data was encrypted. When a user requests data, the Cloud provider verifies their identity & authorizes the transfer of that data. 15% of the performance has been lost due to the time it takes to encrypt data.

Table 2. Time Complexity

Private key length(bits)	**Time in (ms)**
64	86.00
128	91.33
256	110.33
512	142.67
1024	363.67
2048	2748.67

Table 3. Space complexity

Private key length(bits)	**Run Time Memory**
128	345128
256	347224
512	347320
1024	348040
2048	348608
4096	349488
8192	351048

Table 4. Throughput

	Throughput for different Private Key Length				
Data Bits	**128 bits key length**	**256 bits key length**	**512 bits key length**	**1024 bits key length**	**2048 bits key length**

32	205.13	186.04	136.75	102.56	48.854
64	457.14	372.09	256	205.13	71.99
128	914.28	684.49	514.056	315.27	182.33
256	1641.02	1361.70	1094.02	684.49	443.67

In 2014, Bandara, [10] presented the e-learning education system needs cyber security. The term "cybersecurity" refers to a set of regulations for protecting the Internet. In an e-learning environment, security concerns are increasing at an alarming rate. The author has demonstrated a method for monitoring and controlling cyber security in e-Learning systems in this research.

In 2011, Kumar, G. [11] presented cloud-based e-learning security challenges and solutions. Theoretical and empirical investigations were incorporated into the research. E-learning solution suppliers' cloud-based websites have been surveyed for empirical evidence.

In 2015, Arshad Ali et al. [12] published e-Learning in Distance Education's utilization of Cloud Computing. A review of existing e-learning elements was conducted in this study. Scientists have also studied the notion of cloud computing. This research has described in depth the architecture of cloud computing platforms for integrating E-Learning elements. Using cloud computing in online education is the topic of this study.

In 2014, Sudhir Kumar Sharma et al. [13] explained technologies for a distance learning environment. They talked about cloud computing and e-learning systems. E-learning aids e-learners by leveraging cloud computing services, according to research. Cloud computing is also being used in e-learning research.

In 2014, Yinghui Shi et al. [14] presented trends in Educational Cloud Computing. There are five main areas of attention in this study. This is a combination of pedagogical and conceptual work, educational software development, and processing of data and resources Cloud computing advantages and drawbacks in education, as well as DBMS integration to cloud-based services.

In 2015, Sanjay Karak et al. [15] authored an article about cloud computing as a paradigm for distant education. This study chose to give an affordable web-based solution anywhere, anytime, on any device. Cloud-based distant education systems are often the subject of this study.

In 2019, Jyoti Prakash Mishra et al. [16] looked at a new perspective on educational cloud computing. A service that uses cloud computing, the author looked at how it is being used in education. Findings from this research indicate the necessity for specific corrective activities to ensure that it can be properly utilized as a service.

In 2016, Awatef Balobaid et al. [17] proposed the idea of a Cloud-Based Distance Learning paradigm is innovative. This study aims to make cloud-based online education available to students in developing nations who would otherwise be unable to afford it.

In 2103, Xu Zhihong et al. [18] extended via the development of a cloud-based education system. In order to create instructional resources, the author created an educational cloud computing platform. Teaching management may be done in this context. Innovative practice teaching can be accomplished through research.

[4] PROBLEM STATEMENT

For teachers, staff and students in the education sector, cloud computing has been examined by researchers [1, 2, 3, 4]. Researchers have also looked into safety and security concerns, risk classifications and levels. Potential impact of Cloud computing on education is examined. One of the most pressing issues in education in developing nations is safety and security management. Intruders' hacking and cracking operations are a security concern. 24-hour availability is also a concern. Students today need to be able to access necessary information from any location, at any time, via the cloud [5]. Researchers looked into ways to cut down on the expense of remote education. It is difficult to provide online cloud-based education to impoverished kids & youngsters in a developing country. The cloud system, however, has already been protected by RSA, DNA Cryptography, and other protocols [10, 11]. However, there's still the matter of quality. Existing studies that have given security have decreased overall performance by 7-20%. Packet size, encryption time, firewall filtering time, and malware detection time are just a few elements that affect cloud performance. As a result, a new technique is needed that may improve both security and speed.

[5] PROPOSED WORK

It has been shown that the new method is both safer and more effective than the old one. Integration to improve the security of Steganography has overcome the problems with conventional research. Designing a secure encoding and decoding technique would allow users to transport data over the network without delay or data loss, thereby improving system protection. An important aspect of cryptography is the creation of secret codes, either written or generated. Data is encrypted such that it cannot be decoded by anybody other than the intended recipient, making it impossible for the data to be intercepted in transit. Several degrees of cryptography is employed to achieve information security. During transmission and storage, the information is secure. The use of cryptography also helps to ensure that no one can deny the validity of a transaction. It's possible to determine who sent an email and when it was delivered, thanks to this feature.

The employment of the XOR operator has improved security on the network.. In comparison to the old approach, the XOR key would be more efficient in encrypting data. The XOR key would be used to encode and decode data.

Working

The xor method will be taught step-by-step.

1. Faster data transfer can be achieved using the proposed method.
2. There is minimal possibility that the intended work will be hacked.
3. In the suggested method, a graphical user interface is used to create an interactive interface.
4. Due to this user-defined port, we were could not send the unauthentic message.
5. In the suggested method, a session-level has been included.

IP Filter

Decryption requests from legitimate IP addresses would be allowed in a centralized database of IP addresses. Decryption is not permitted if the IP address has not been detected in the database or if its status is 0.

FLOW CHART OF PROPOSED XOR MECHANISM

By incorporating an IP filter, we are going to increase the security of steganography by rejecting unauthenticated transmissions from the server to client.

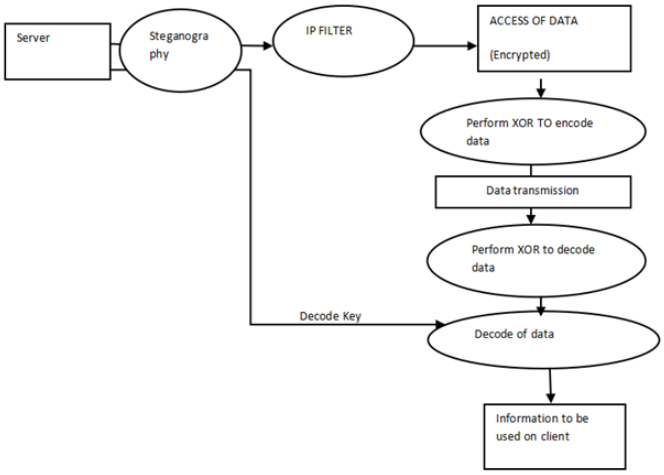


Fig. 2. XOR Based Model

We use XOR to customize an existing steganography technique to increase network security. The research aims to find and fix current security flaws while also enhancing network security using steganography. We would write an authenticated socket server and the client to protect data during transmission. We would provide a user interface to facilitate communication between clients and servers. As compared to traditional stenography, this method would be far more efficient [23].

[6] RESULT AND DISCUSSION

The proposed methodology is more secure than the traditional method, which relies on brute force and timing attacks. The following diagram illustrates the main differences between the suggested and traditional methods.

Table 5. Comparison between traditional RSA and proposed XOR techniques

Parameter	**Tradition RSA Technique**	**Proposed XOR Technique**
Brute force attack	Attack is possible	Attack is not possible

Timing attack	Possible of timing attack	No possibility of timing attack
Port	Predefined	User defined
Security	brute force and timing attacks make the system less secure. –	Because brute force and timing attacks are impossible, the system is more secure.
IP Validation	No	Yes
Multilevel encryption	No	Yes

The accompanying table demonstrates that the traditional method is less secure than the one presented. The comparison is based on several distinct factors. Conventional strategies are vulnerable to brute force and timing assaults, but the XOR methods suggested in this paper protect against these. Tradition dictates that a port is already established. When using XOR methods, the port can be set by the user. In addition to these features, XOR's suggested implementation includes IP validation and multilevel encryption, which the traditional approach, does not [21].

COMPARISON OF TRADITIONAL & PROPOSED TECHNIQUES IN CASE OF BRUTE FORCE ATTACK

The following graph compares the proposed work to typical RSA work and shows how strong it is. Brute-force attacks are more likely when using traditional RSA, as seen in the accompanying table. The risk of brute force attacks rises as the number of packets grows. However, when the number of packets rises, the threat from brute force attacks decreases in proportion to the previous method.

Even in the case of a brute force assault, the standard RSA method would only get 6 packets affected, compared to just 1 packet in the suggested approach. During transmission, the number of impacted packets rises in lockstep with the overall packet count. While less packets are affected by the proposed techniques, compared to traditional methods, more packets are affected by traditional methods.

Table 6. Analysis of brute force attacks on RSA and XOR in the context of the suggested XOR algorithm.

No of packetsx100	**Previous model**	**Proposed model**
1	5	2
2	7	3
3	13	3
4	16	5
5	23	8
6	30	14
7	41	19
8	50	24
9	63	27
10	71	33

The number of packets affected by a brute force assault using traditional RSA and the proposed XOR method is shown in the table above. The number of packets affected by the suggested XOR approach is lower than with traditional RSA, as shown in the table. As a result, it may be stated that the Proposed XOR is more resistant to brute-force attacks than standard RSA.

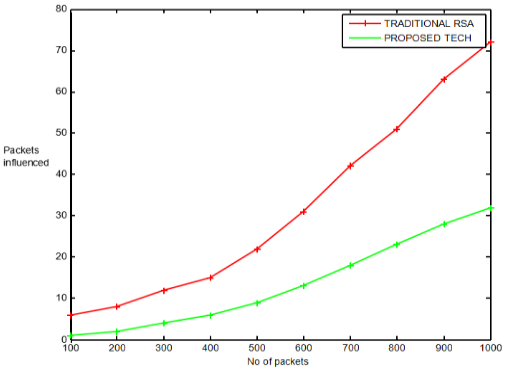


Fig. 3. Comparison of traditional & proposed techniques in case of Brute force attack

A brute force attack on a normal RSA and a proposed XOR approach is shown in the right-hand figure. The graph (Fig. 3) shows that the recommended XOR technique affects fewer packets than Traditional RSA. Brute force attacks are predicted to be less effective against the proposed XOR algorithm than the traditional RSA algorithm at all times.

COMPARISON IN CASE OF TIMING ATTACK

The following graph compares the proposed work to typical RSA work and shows how strong it is. The following table shows that traditional RSA is more vulnerable to a timing attack than modern RSA. The likelihood of a timing attack grows as the number of packets increases. However, when the number of packets rises, the threat from the Timing attack in the suggested approach decreases.

Table 7. Timing attack comparison

No of Packets x100	Previous model	Proposed model
1	7	2
2	10	4
3	15	5
4	21	8
5	29	10
6	39	14
7	49	19
8	62	25
9	72	30
10	83	35

RSA would receive 7 packets affected in the case of a timed attack if 100 packets were sent, but the suggested method would only obtain 2 packets. During transmission, the number of impacted packets rises in lockstep with the overall packet count. However, in the event of a timing attack, the suggested strategies impact fewer packets relative to standard techniques [22].

The amount of packets affected by a timing attack using traditional RSA and the proposed XOR method are shown in the table above. The number of packets affected by the suggested XOR approach are lesser than with traditional RSA, as shown in the table. As a result, the suggested XOR method is found to be more resistant to a timing attack than regular RSA (Fig. 4).

Time-based attack scenarios: comparison of old RSA with the newer suggested XOR approach

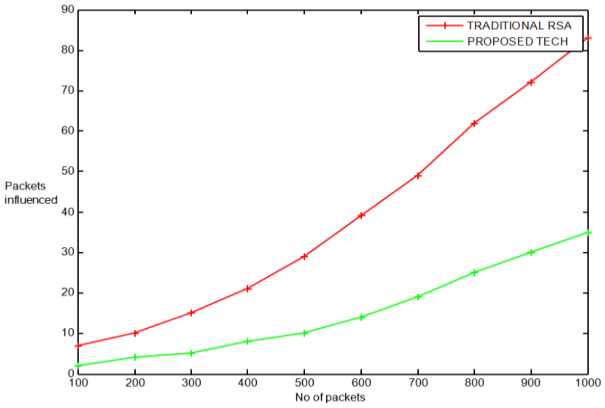


Fig. 4. COMPARISON OF TRADITIONAL & PROPOSED TECHNOLOGY IN CASE OF TIMING ATTACK

Traditional RSA and Proposed XOR are shown in the image above, with the amount of packets affected by timing attacks. Proposed XOR has a lower amount of packets affected than Traditional RSA, according to this graph. XOR is more vulnerable to a timing attack than the standard RSA provided in this paper.

[7] CONCLUSION

In comparison to the classic RSA technique, the XOR approach has been found to provide greater cyber security with high performance. A combination of user-defined ports, IP validation, and layered encryption were employed in the study. The proposed work would mitigate a brute force assault or a timed attack in this way.

[8] SCOPE OF RESEARCH

Cloud computing and e-learning is hot topics right now. It has a significant impact on the education and learning process. These are aiding smart phone users in implementing their operations more efficiently and at a lower cost. Many different cloud service providers are supplying cloud-dependent apps for these platforms. Research in the future should be able to supply crucial technologies for the security of cloud applications for remote learning. Additional requirements include improving service quality and being qualified for instructional resource management. Intelligent service management is another goal for future study.

REFERENCES

1. Dr. Pranav Patil, "A Study of E-Learning in Distance Education using Cloud Computing" International Journal of Computer Science

and Mobile Computing, IJCSMC, Vol. 5, Issue. 8, August 2016, pg.110 – 113.

2. Asgarali Bouyer, Bahman Arasteh "The Necessity of Using Cloud Computing In Educational System" CY-ICER 2014, 1877-0428 © 2014 Elsevier.

3. Agah Tugrul Korucu, Handan Atun "The Cloud Systems Used in Education: Properties and Overview " World Academy of Science, Engineering and Technology International Journal of Educational and Pedagogical Sciences Vol:10, No:4, 2016.

4. Ananthi Claral Mary.T, Dr.Arul Leena Rose. P.J (2019) "Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art" International Journal of Scientific & Technology Research, Volume 8, Issue 12.

5. Meslhy, Eman & Abd Elkader, Hatem & Eletriby, Sherif. (2013). Data Security Model for Cloud Computing. Journal of Communication and Computer 10 (2013) 1047-1062. 10. 1047-1062.

6. Osman, Saife & Eltahir Abdelhag, Mohammed & Abdelrahman, Saad. (2016). Performance Analysis of Cloud-based Web Services for Virtual Learning Environment Systems Integration. International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 4, April 2016.

7. Pandey, G. P. (2019). Implementation of DNA Cryptography in Cloud Computing and Using Huffman Algorithm, Socket Programming, and New Approach to Secure Cloud Data. Socket Programming and New Approach to Secure Cloud Data (August 7, 2019).

8. P.suresh(2016) SECURE CLOUD ENVIRONMENT USING RSA ALGORITHM. 2016, IRJET.

9. Singh, S. K., Manjhi, P. K., & Tiwari, R. K. (2016). Data Security Using RSA Algorithm in Cloud Computing. International Journal of Advanced Research in Computer and Communication Engineering, 5(8), 11-16.

10. Bandara, I., Ioras, F., & Maher, K. (2014). Cybersecurity concerns in e-learning education.

11. Kumar, G., & Chelikani, A. (2011). Analysis of security issues in cloud-based e-learning. University of Borås/School of Business and IT.

12. Arshad Ali, Amit Bajpeye, Amit Kumar Srivastava" E-learning in Distance Education using Cloud Computing" International Journal of Computer Techniques -– Volume 2 Issue 3, May – June 2015.

13. Sudhir Kumar Sharma, Nidhi Goyal, Monisha Singh" Distance Education Technologies: Using E-learning System and Cloud Computing" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1451-1454.

14. Yinghui Shi, Harrison Hao Yang, Zongkai Yang, and Di Wu" Trends of Cloud Computing in Education" S.K.S. Cheung et al. (Eds.): ICHL 2014, LNCS 8595, pp. 116–128, 2014. © Springer International Publishing Switzerland 2014.

15. Sanjay Karak, Basudeb Adhikary "CLOUD COMPUTING AS A MODEL FOR DISTANCE LEARNING" International Journal of Information Sources and Services, Vol.2: July-Aug 2015, Issue 4.

16. Jyoti Prakash Mishra, Snigdha Rani Panda, Bibudhendu Pati, Sambit Kumar Mishra" A Novel Observation on Cloud Computing in Education" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019.

17. Awatef Balobaid, Debatosh Debnath" A Novel Proposal for a Cloud-Based Distance Education Model" International Journal for e-Learning Security (IJeLS), Volume 6, Issue 2, September 2016.

18. Xu Zhihong, Gu Junhua, Dong yongfeng, Zhang Jun, Li-yan "Expand distance education connotation by the construction of a general education cloud "International

Conference on Advanced Information and Communication Technology for Education (ICAICTE 2013).

19. Jyoti Prakash Mishra, Snigdha Rani Panda, BibudhenduPati, Sambit Kumar Mishra (2019) " A Novel Observation on Cloud Computing in Education" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3.

20. Pandey, G. P. (2019). Implementation of DNA Cryptography in Cloud Computing and Using Huffman Algorithm, Socket Programming, and New Approach to Secure Cloud Data. Socket Programming and New Approach to Secure Cloud.

21. Jyoti Prakash Mishra, Snigdha Rani Panda, BibudhenduPati, Sambit Kumar Mishra (2019) " A Novel Observation on Cloud Computing in Education" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3.

22. V. R. Niveditha, T. V. Ananthan , S. , Amudha Dahlia Sam and S. Srinidhi (2020), Detect and Classify Zero Day Malware Efficiently In Big Data Platform.

23. Abdulbaset Salem Albaour, Yousof Abdulrahman Aburawe (2021). Big Data: Review Paper.

24. Cunha W, Mangaravite V, Gomes C, Canuto S, Resende E, Nascimento C, et al. (2020, may). On the cost-effectiveness of neural and non-neural approaches and representations for text classification: A comprehensive comparative study. Inf Process Manage;58(3):102481.