SECURE AND HIGH PERFORMANCE HYBRID SOCKET BASED APPROACH FOR CLOUD ENVIRONMENT BY INTEGRATION OF MACHINE LEARING APPROACH

[1]Radhika Garg and [2]Dr. Kavita Mittal

[1]Research Scholar and [2]Associate Professor, Jagannath University, NCR, Haryana

ABSTRACT

Applications are that utilize the cloud are becoming more and more common, and cloud services are rapidly being used to move digital files between different places. The risk of unauthorized access to digital information does not go away even after it has been transferred. Adding security measures to cloud systems has been found to have a negative impact on performance. An extensive investigation was carried out by researchers in an effort to improve cloud security and performance. The proposed strategy should increase safety without sacrificing performance. It is being evaluated to determine whether any of the published research have any restrictions in terms of cloud-based software security issues. Cloud system and socket-based high-performance mechanisms' transmission latency, error probability, and packet loss probability may be improved using an encrypted hybrid technique. The suggested model is being compared to existing techniques in the field in terms of security, performance, and dependability. This study is meant to investigate the proposed initiative's need, inspiration, and challenges. This research will examine how the intended work will be carried out in the actual world after examining the problem description. The Endeavour's algorithm and mechanism would describe the tools and procedures used in study. The simulation's results would be presented, along with an explanation of why this study is superior to previous studies. There are a variety of approaches you may take to this research, which we'll go over in more depth below. Exploratory studies may yield out new topics. Providing answers to a problem through doing research. Research work considered machine learning approach in order to classify different by of attacks in order to improve the security of hybrid socket based approach.

Keywords: Cloud computing, Distance learning, security, performance, machine learning.

DOI Number: 10.48047/NQ.2022.20.15.NQ88613 **NeuroQuantology2022;20(15): 6116-6131**

[1] INTRODUCTION

Cloud-based applications and cloud services are becoming more popular as a means of transmitting digital data from one location to another. There is still a hazard in transferring digital content. It's also been proved that cloud systems' performance suffers when security features are included. The goal of these investigations is to make the cloud more secure and efficient. The purpose of the proposed method is to increase security without losing speed.

1.1 CLOUD COMPUTING

With cloud computing, computer system resources, such as data storage (cloud storage) and processing power, are made available on-demand and without human involvement. When it comes to large clouds, functions are often spread among numerous data centres, each of which serves as its own data centre. If you don't know what you're getting yourself into with cloud computing, you may end up paying more than you bargained for if you don't know what you're getting yourself into with cloud computing. The purpose of cloud computing is to enable consumers to benefit from all of these technologies, without the requirement for extensive knowledge or skill with any one of them. In an effort to save money, the cloud enables customers to concentrate on their main business rather than being stymied by IT issues. Virtualization is the primary technology that enables cloud computing. Using virtualization software, a single physical computer equipment may be divided into a number of smaller, more manageable "virtual" machines. Idle computer resources may be more effectively allocated and used thanks to the virtualization of operating systems at the system level. By increasing the utilisation of infrastructure, virtualization allows for greater agility in IT operations and lower costs. On-demand resource provisioning is made possible by autonomous computing, which automates the provisioning process. Automation speeds up the process, lowers labour expenses, and decreases the likelihood of human mistake. Automation. The measurements provided by cloud computing are based on notions from utility computing.

Cloud Computing Shares Characteristics With

- Any distributed programme that differentiates between service providers (servers) and service seekers (clients) is referred to as a client-server model (clients). [45]
- The term "computer bureau" refers to a company that specialised in computer services throughout the 1960s through the 1980s.
- Distributed and Parallel Computing (DPC): A kind of distributed and parallel computing in which a cluster of networked, loosely connected computers operate in unison to complete extremely large jobs.
- Data, computation, storage, and application services are provided closer to the client or near-user edge devices (such as network routers) via fog computing, a distributed computing paradigm. As a result, fog computing processes data at the network level, on smart devices, and on the end user's client-side (e.g., mobile devices).
- Computable resources, such processing and storage, are packaged into a metered service comparable to a standard public utility.
- No central coordination is required in a peer-to-peer system. Participant organisations provide and consume resources in a two-way fashion (in contrast to the traditional client-server model).
- Sandbox in the cloud — A computer environment where programmes, codes, and files may execute without harming the application in which they are running.

1.2 Challenges to Cloud Computing

The benefits of a cloud-based education system outweigh the negatives, which include installation, performance, and security issues. Here are a few of the issues that need to be addressed:

1. Because of their complexity and intricacy, cloud services are tough to manage. Many personnel with extensive expertise are needed to build a cloud-based remote learning system.
2. Every aspect of how a cloud system works has an effect on how well it performs for its users.
3. Low network performance may sometimes prohibit instructional resources from being distributed over the network. These difficulties may be attributed to a lack of bandwidth and storage space.
4. Another challenge that arises with a cloud-based learning system is the management of enormous amounts of instructional data. It may be difficult to move big amounts of data from one location to another.
5. A fifth worry is the security of educational data, which is vulnerable to network attacks and hacking. Some of the safeguards that may be put in place to protect a cloud-based education system may have an adverse effect on its performance.

1.3 SECURITY FACTORS

In the past, cloud security has been breached by viruses and other attacks. There is a possibility of instructional information being hacked through the internet as a result of this. Hackers are to blame for data breaches that occur due to a lack of effective authentication. Crackers, on the other hand, are the ones who are in charge of eroding the security of the system. Encryption and firewalls are often employed to keep data secure.

1.4 PERFORMANCE FACTORS

Encryption methods that require a long time to deploy and have an impact on the system's performance must be used in order to increase the system's security. Several variables affect the performance of the cloud environment, including:

1. Wired or wireless transmission media has an impact on the performance of the system. Wireless media might lag behind when compared to a wired connection. There are divisions for both wireless and wired systems.
2. Bandwidth refers to the amount of data that may be transmitted in a given amount of time. More data can be transmitted in less time with more bandwidth.
3. For data transmission, protocols are sets of rules that govern how data is sent through a computer network. An acknowledgment-free protocol like the User Datagram Protocol (UDP) is more efficient than the Transmission Control Protocol (TCP).
4. Security mechanisms: The cloud network's performance may be severely affected since it takes a long time to check whether or not a transmission is legitimate.
5. Performance may be impacted by the distance between the transmitter and receiver in the network. Transmission time and efficiency degrade as distance is increased. As the distance decreases, so does the amount of time it takes to send a message.
6. When a signal goes from one area to another, it experiences attenuation. Distance and medium of transmission affect attenuation. A signal regenerator is the sole solution to attenuation-related issues.
7. In this section, a compression methodology for online learning content has been discussed. There are several ways to compress data, but there is always a risk of data loss. Replace the large words with smaller ones in another table. Using smaller words in place of longer ones reduces the overall size of a packet. The packet's transmission time was shortened by 80% as a result. A smaller packet also moves faster across the network, lowering the chance of a packet being lost in transit. In a cloud-based online learning system, packet transmission time could be reduced by using a compression algorithm.

1.5 Role of machine learning in enhancement of performance and accuracy

Machine learning is mechanism that allows smart decision making. Considering machine learning approach, classification is made after training neural network. In proposed research machine learning mechanism would be applied in order to classify the attacks on the bases of previous experience in order to make system more reliable and efficient. Present research is considering different types of attack and making classification after

[2] LITERATURE REVIEW

Numerous research have been undertaken to improve cloud storage security and speed.

In 2011, Kumar, G. [2] conducted research on cloud-based e-learning. The study drew on both theoretical and empirical approaches. The cloud-based websites of e-learning solution providers have been examined for empirical proof. Research on cloud security has led to a theoretical conclusion. For the purpose of comparing actual data with theoretical predictions, scholars have developed a variety of comparative methodologies. For cloud applications, Meslhy [6] created a data security model in 2013. This research report recommends using a single default gateway to protect sensitive user information across many public and private cloud applications. It is feasible to encrypt sensitive data before transferring it to the cloud using this gateway platform and not cause a cloud app to break. Research has led to the development of a quick encryption method and the integrity of files. In addition, it has anti-malware, firewall, and tokenization functions. capabilities. As a consequence of numerous application threads being slowed down by the firewall and malware detection, the security method has reduced performance by 7%.

In 2014, Asgarali Bouyer et al. [11] emphasised the importance of cloud computing for online education. During the course of their inquiry, they learned that cloud computing is a dynamically scalable technology. The provision of web-based services is an option. Due to recent technical developments, virtual technologies are becoming increasingly important in online education. Academics have found great value in online learning. Both quantitative and qualitative improvements are being made in online education. Both educational institutions and students in the sciences and technologies benefit from research. The study's main emphasis was on the usage of an online education system based on cloud computing.

On the utilisation of the RSA technique to safeguard cloud data in 2016, Singh, S. K. provided findings [13]. According to the author's research, the RSA Algorithm's performance is influenced by three factors: Time Complexity, Space Complexity and Throughput are the three main factors to consider. According to the results, authentic people could only access the data once it was encrypted using the RSA technique. All data is encrypted before uploading to the cloud. When a user asks for data from a Cloud provider, the provider verifies the user's identity and gives them permission to provide it. It has taken 15 percent longer than expected to encrypt data, which has affected speed.

P.suresh [30] employed RSA ALGORITHM in his 2016 research to secure the cloud. The encryption and decryption capabilities of algorithms like AES, DES, RSA, and others have been researched. This work used an asymmetric key algorithm to implement RSA. Encryption and decryption required the use of various key sizes. In contrast, security procedures slow down the system by 20%.

An investigation of the performance of cloud-based web services necessary for virtual Learning Environment Systems was conducted by Osman and Saife in 2016 [31]. Web services delivered through cloud environments have been proved to be useful in a variety of scenarios, opening the door to new kinds of applications. These services may be accessed via a variety of protocols, including SOAP and REST. Protocols provide several high-quality services. The study's results provide a way to enhance the cloud's web services environment. Cloud-based access to quiz services has been researched in terms of performance characteristics, such as response time and throughput. Security measures have increased response times by 5%.

In 2016, Agah Tugrul et al. [32] studied the features and properties of cloud platforms for online education. Data used in education is becoming more diverse and valuable as a result of technological advancements. The importance of web technology to a remote education system has been shown in several studies. The study also looked at mobile systems, which are widely utilised in distance education. It has made the internet more accessible. Web technology has made it possible for anyone across the world to access information on the internet regardless of location or time. Both the storage and acquisition of educational data and resources has been shown to be crucial.

Until 2019, Pandey, G. P. [34] used DNA Cryptography to secure the cloud application. A data compression algorithm known as the Huffman Algorithm has been employed in academic study for some time. Socket programming was employed to permit transmission for both the sender and the recipient applications by the author. Compressed data has been safely stored in the cloud for research purposes. An additional 13% has been lost due to this process. This research focused on how schools are making use of cloud-based services. It's a study of the various cloud computing choices. This research used a survey technique.

When Ananthi Claral Mary et al. [35] examined the implications and issues of Cloud Computing in 2019, it was reported. It is beneficial to use cloud computing in academics for a variety of reasons. If you utilise the cloud to store and handle sensitive data, you may have security worries. Cloud computing security issues have been exposed in this research, as well as the measures in place to prevent an attack from spreading throughout the cloud ecosystem.

Table 5: Literature Review

Sno	Author/ year	Objective of research	Mechanism	Benefits	Limitations
1.	G Kumar [2] / 2011	Security concerns in cloud-based e-learning	Security protocols	The security of a cloud-based e-learning system has been examined by researchers.	Work has ignored the data compression concept
2.	Meslhy, Eman [6] / 2013	Data Security Model for Cloud Computing	Cloud computing	A cloud security paradigm has been presented by researchers.	Work is generalized and did not focus on performance
3.	Bandara, I [8] / 2014	Cybersecurity concerns in e-learning education	Security protocols	A new security system has been discovered.	Research has provided limited security solution and ignored the cloud performance.
4.	Asgarali Bouyer [10] /2014	Affirming that cloud computing in education is a must	Cloud computing	Cloud computing in education was examined in this study.	The research did not propose a mechanism for security and performance
5.	Singh, S. K. [28] / 2016	Cloud Computing Data Security using RSA Algorithm	RSA algorithm	RSA mechanism is enabling data security of cloud	Research ignored the performance factors.
6.	P.suresh [29] / 2016	Secure cloud environment using RSA algorithm	RSA algorithm	Researchers have proposed an RSA algorithm for the security of cloud data	No mechanism has been proposed to reduce the size of the packet to improve the performance of the cloud.
7.	Osman, Saife [30] / 2016	Integration of Virtual Learning Environment Systems Based on Performance Analysis of Cloud-based Web Services	Cloud computing	Work has considered the performance factors that are influencing cloud	Research has ignored security features.
8.	Agah Tugrul Korucu, [31] / 2016	Overview and Specifications of Educational Cloud Computing Platforms	Cloud computing	Research reviewed the role of the cloud in education	The security of the cloud has been ignored.
9.	Pandey, G.	Implementation of DNA	DNA	The research	The research did not

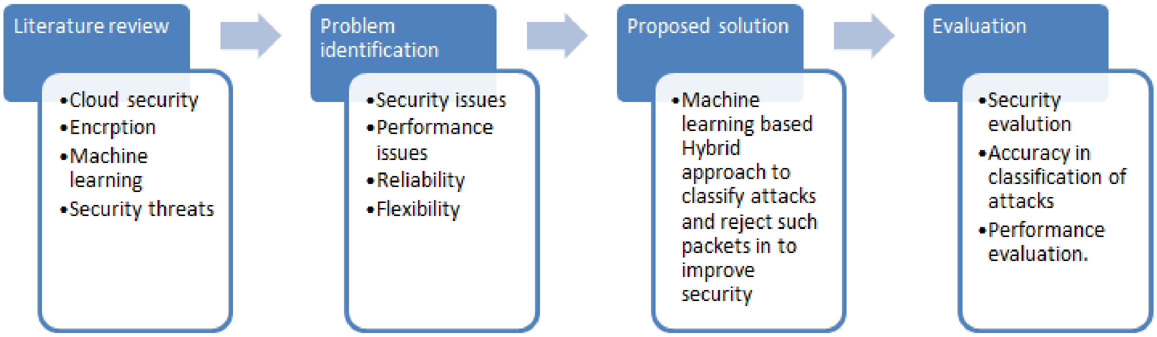
	P. [33] / 2019	Cryptography in Cloud Computing and Using Huffman Algorithm, Socket Programming and New Approach to Secure Cloud Data	cryptography	proposed DNA based security to secure the content of cloud	provide a solution to improve the performance of the cloud.
10.	Ananthi Claral [34] / 2019	Using Cloud Computing in the Academic Environment – A State-of-the-Art	Cloud computing	Risk and challenges to cloud application are considered	The research did not provide any solution for security risks

[3] Problem Statement

Multiple findings in cloud computing security research, yet the security techniques used invariably resulted in reduced performance for the cloud in question. In addition, earlier research has concentrated on a small portion of the data. It's worth noting that past experiments had minimal throughput due to weak speeds and severe packet loss. Text and graphics must be safeguarded without losing any of their effectiveness. Moreover there is lack of smart approaches that should eliminate the packets considering previous experience. Proposed work is supposed to provide security solution for cloud service where attacks such as man in middle , brute force, denial of service are detected considering trained model.

[4] Proposed Research Methodology

There has been several research related to cloud security. Present research considering security of textual as well as graphical contents. In order to improve the security of machine learning approach has been integrated. Such mechanism allows filtering of data packet and restricts transmission of invalid information over network. Proposed research work considers the issues of performance along with security and reliability. Considering factors that influences security and performance of cloud, proposed work is focusing on machine learning approach that would be capable to classify type of attacks. These attacks might be man in middle, brute force and denial of service attack.



The flowchart below illustrates the suggested model's use of machine learning. Graphs and text are both protected in the current research. The machine learning approach has been implemented in order to improve the level of security it provides. Filtering of data packets ensures that inaccurate information cannot be sent over the network. The proposed research effort aims to address the issues of performance, security, and reliability together. The proposed research focuses on machine learning techniques that are capable of classifying different types of attacks in light of factors affecting cloud security and performance. A man in the middle, brute force, or a denial of service attack might be used in these attacks.

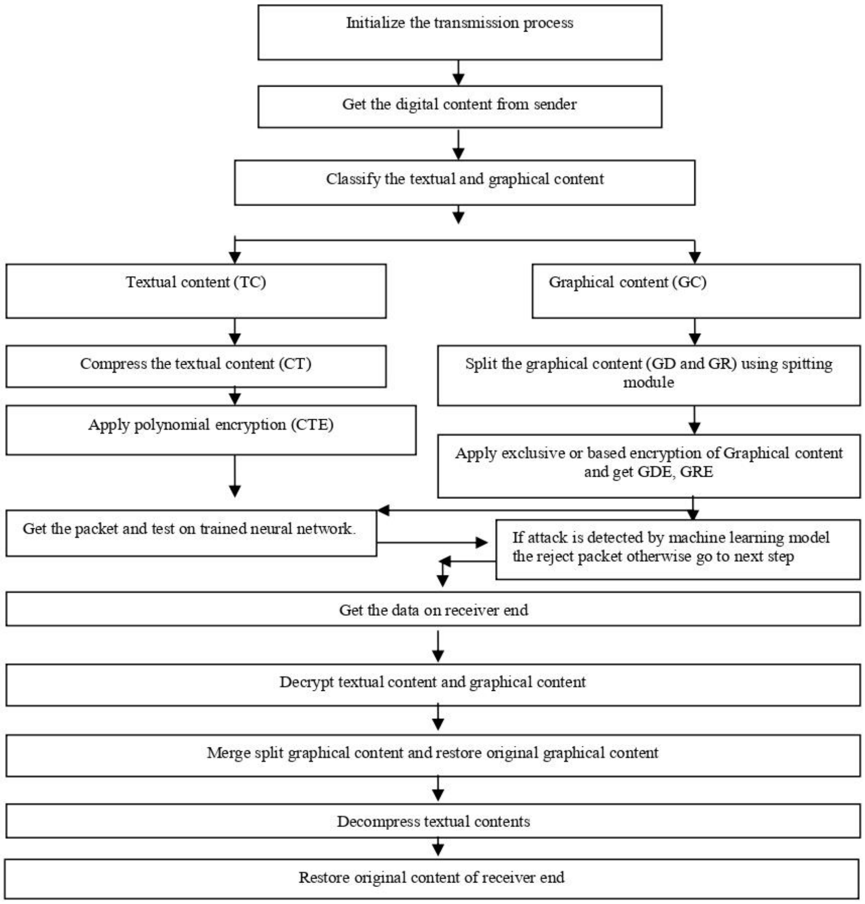

Initialize the transmission process
Get the digital content from sender
Classify the textual and graphical content
Textual content (TC)
Graphical content (GC)
Compress the textual content (CT)
Split the graphical content (GD and GR) using spitting module
Apply polynomial encryption (CTE)
Apply exclusive or based encryption of Graphical content and get GDE, GRE
Get the packet and test on trained neural network.
If attack is detected by machine learning model the reject packet otherwise go to next step
Get the data on receiver end
Decrypt textual content and graphical content
Merge split graphical content and restore original graphical content
Decompress textual contents
Restore original content of receiver end

Fig 2 Process flow of Proposed Work

[5] RESULT AND DISCUSSION

5.1 Platform Used to implement the proposed Model

In order to construct the transmitter and receiver module, Java was used as a programming language on the Netbean platform. Packets are used to measure the amount of time it takes to complete past and planned tasks during a simulation. MATLAB has been used for the simulation work.

5.2 Simulation for time/error/packet size

The amount of time it takes for a data packet to travel between the sender and receiver modules is taken into account.

5.2.1 Time consumption

Simulated time in contrast to existing RSA, DES, and AES cryptography-based research for the proposed system is shown in figure 3. The data has been compressed and encrypted using exclusive order in the proposed work. However, prior studies used the RSA and AES encryption mechanisms, which took longer to encrypt data. In addition, prior studies did not compress data before it was sent. As a result of the smaller data packets, the processing time is significantly reduced.

Table 6: Comparative analysis of Time consumption

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	0.95	0.93	0.88	0.82	0.36
20	1.67	1.59	1.51	1.22	1.07
30	2.32	2.29	2.2	1.67	1.49
40	3.09	2.99	2.87	2.35	1.47
50	3.91	3.57	2.93	2.65	1.99
60	4.62	4.58	4.35	3.42	2.72

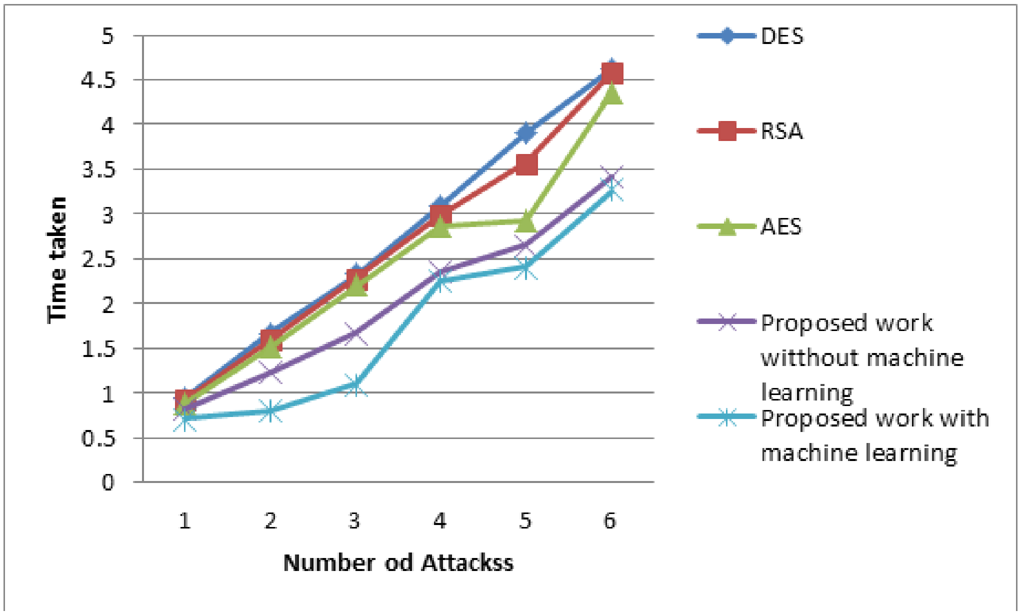


Fig 3: Comparison of time taken

5.2.2 ERROR RATE

Errors may still occur during the transfer of data. A lower amount of data in a smaller packet also reduces the chance that it may be mistaken for a spam message. Because the string size is lowered utilising a replacement process, there are less possibilities of a mistake. There has been no reduction in the size of packets using the RSA and AES cryptographic mechanisms that were employed in prior study. As a result, the current study's error rate may be minimised. Comparative comparison of error rates between proposed work and prior work is shown in Figure 4 (RSA, DES, and AES).

Table 7: Comparative analysis of Error rate

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	0.83	0.78	0.67	0.59	0.54
20	1.36	1.29	1.16	0.89	0.46
30	2.33	2.3	2.2	1.69	1.26
40	2.55	2.35	2.24	1.82	1.15
50	3.94	3.53	3	2.46	1.83
60	4.2	3.92	3.76	3.51	2.90

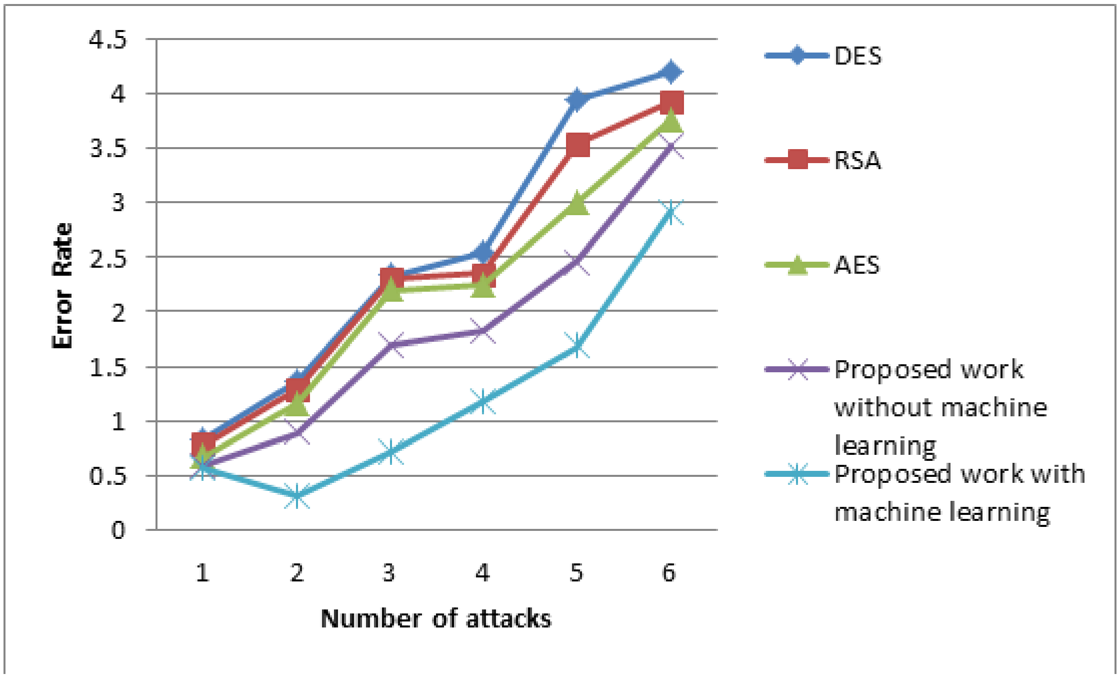


Fig 4 Comparison of error rates

5.3 MATLAB SIMULATION FOR COMPARATIVE ANALYSIS OF SECURITY

In this section, we'll look at the impact on security of the proposed modifications. As the number of assaults grows, the number of packets impacted decreases. AES encryption has been determined to be superior than RSA and DES in prior studies. The suggested approach, on the other hand, outperforms AES in terms of security. According to the accompanying graphs, the number of impacted packets is lower when using the suggested method rather than RSA or AES-based encryption.

5.3.1 MAN-IN-THE-MIDDLE

Its impact on the packet in the case of RSA, DES and AES cryptography and proposed work with and without machine learning in case of these attacks are shown below.

Table 8: Comparative analysis of Man in middle attack

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	9	8	7	4	2
20	13	11	9	6	3
30	20	13	11	9	5
40	25	17	15	11	6
50	29	25	19	14	7
60	32	31	27	17	9

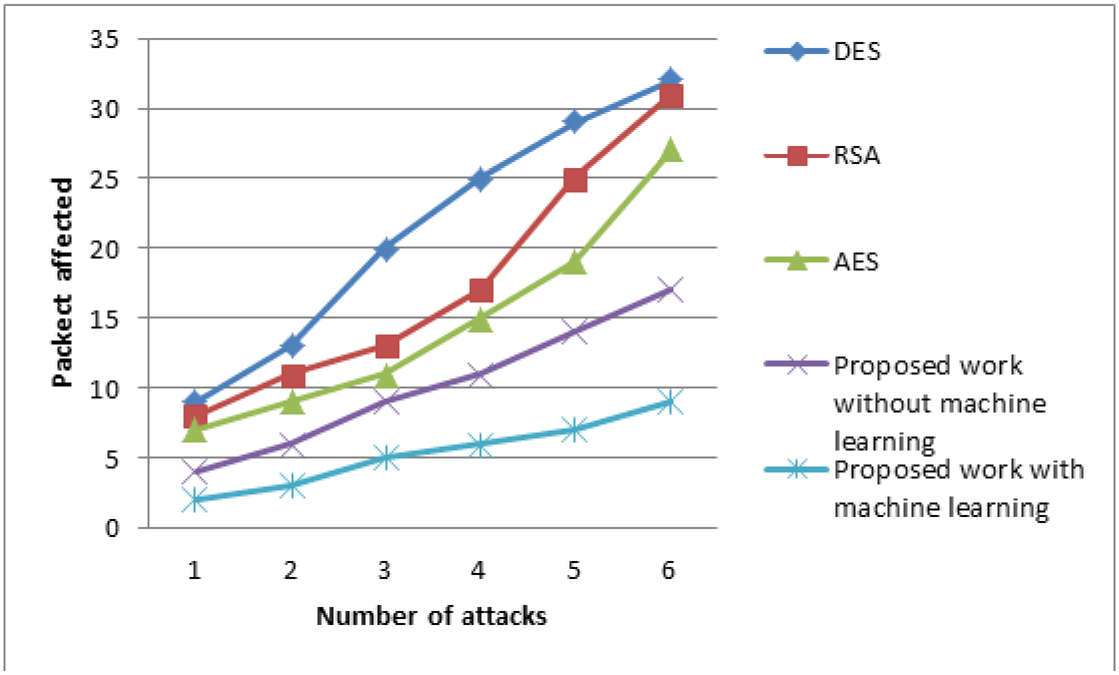


Fig 5: Comparative analysis in case of attack Man-In-The-Middle

5.3.2 BRUTE FORCE ATTACK

A brute force assault uses trial and error to try to figure out a user's login details. Encryption keys and a hidden web page are also used. Comparative analysis of this attack is shown below.

Table 9: Comparative analysis of Brute force attack

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	8	7	6	3	1
20	12	10	8	5	3
30	20	15	11	7	5
40	26	15	13	10	8
50	31	24	19	14	11
60	33	32	27	21	15

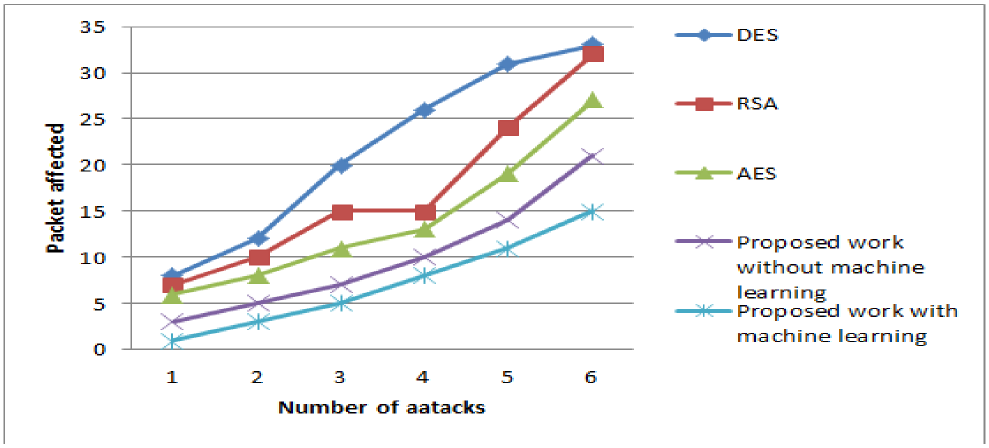


Fig 6: Comparative analysis in case of Brute force attack

5.3.3 DENIAL-OF-SERVICE

Cyberattacks known as (DoS) attacks aim to prohibit users from accessing a computer or a network resource. Having a smaller packet size and a shorter transmission time reduces the risk of a denial of service. As a result, the potential effect of a denial of service on planned machine learning activity is lower. A comparison of Denial-of-Service attacks is shown in the following graph.

Table 10: Comparative analysis of Denial of Service

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	9	8	7	4	2
20	13	11	9	6	3
30	21	16	12	8	4
40	27	16	14	11	6
50	32	25	20	15	9
60	34	33	28	22	12

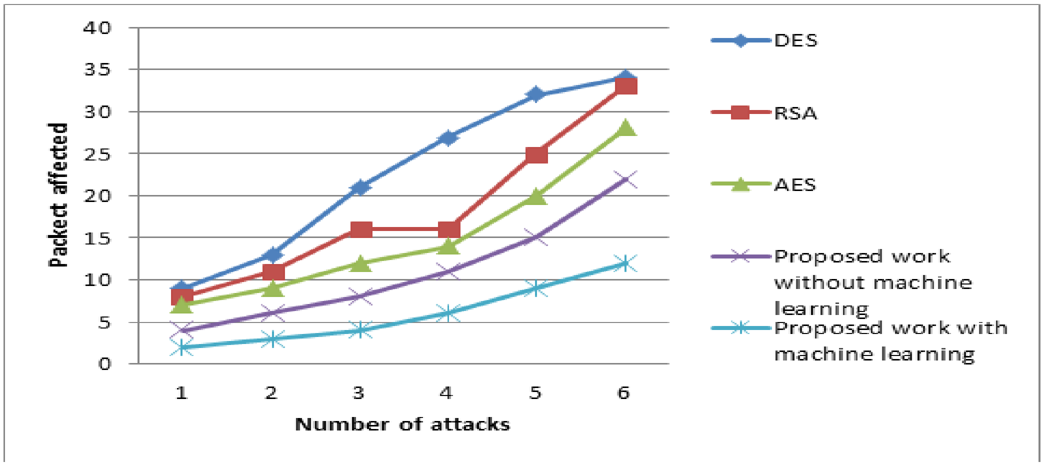


Fig 7: Comparative analysis in case of Denial-of-Service

5.3.5 ACCESS VIOLATION

As part of the proposed work, a user-defined port and security key will be used for each session. As a result, the proposed project has no access violation problems. It is shown in Figure 8 the comparison between RSA, DES and AES encryption, and the suggested research.

Table 11: Comparative analysis of Access violation

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	8	7	6	4	2
20	13	11	9	7	5
30	20	15	12	9	7
40	26	18	16	13	9
50	29	24	21	15	11
60	33	32	28	16	12

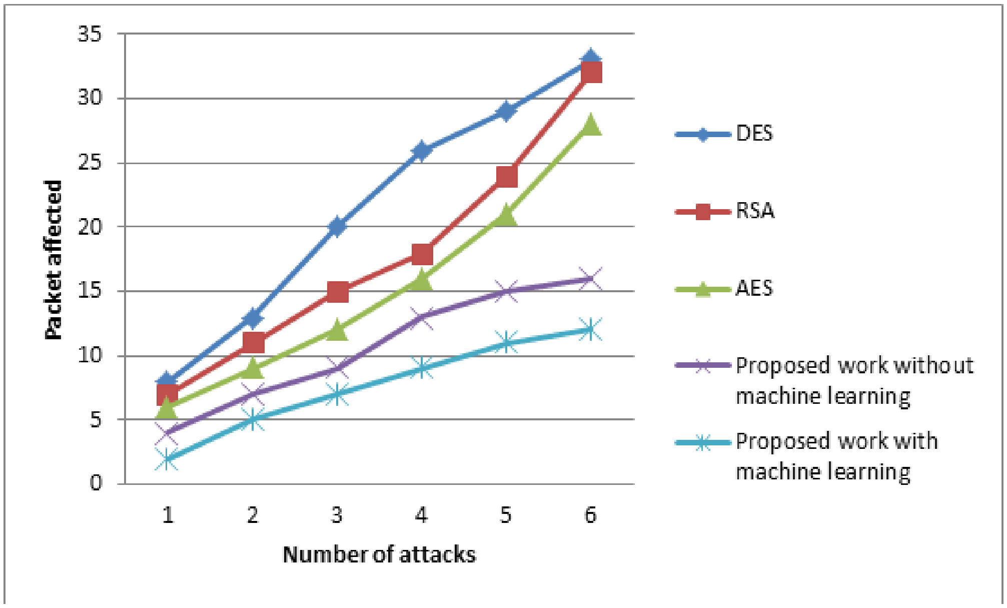


Fig 8: Comparative analysis in case of access violation

5.3.8 ATTACK ON CLOUD SERVICES

Use of exclusive or after compression of data and user defined port number has reduced the chances of different attacks on cloud services. Figure 9 presents the comparative analysis of the attack on cloud service in the case of RSA, DES and AES cryptography, and proposed work.

Table 12: Comparative analysis of Attack on cloud services

Number of attack	DES	RSA	AES	Proposed work without machine learning	Proposed work with machine learning
10	14	10	9	7	5

20	19	13	11	9	7
30	27	22	19	15	9
40	29	25	23	16	11
50	32	28	26	19	15
60	35	30	27	21	17

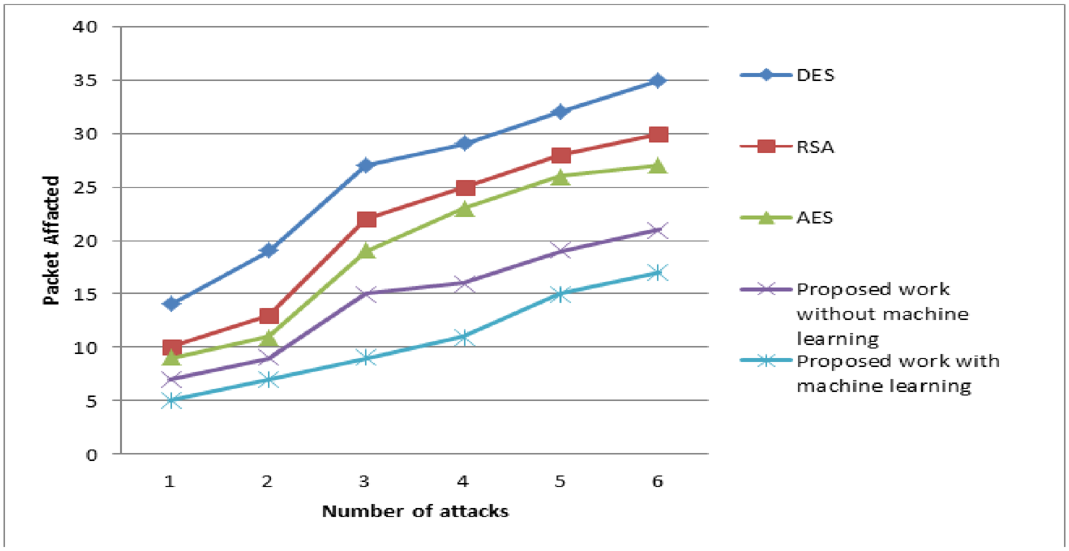


Fig 9 Attack on cloud services

[7] CONCLUSION

People may now try out new ideas thanks to cloud computing. The creation of a favourable environment for the administration of digital resources and content is essential. Existing research has shown a few potential security models. Other technologies, such as RSA, AES, DES, and DNA protection have made it possible to safeguard data stored on the cloud. There have been a number of studies looking at cloud-based teaching materials. Research on how clouds operate has been limited. Cloud security and performance were examined in depth by researchers. In order to enhance security without compromising performance, the suggested approach is designed to When implementing previously analysed operations, cloud security and performance must be taken into account.

[8] FUTURE SCOPE

In the actual world, a cloud solution like this may be quite useful. Data compression and machine learning based encryption system is most prevalent requirements in cloud computing. This hybrid technique of transmission is faster, more reliable, and less prone to mistakes than other methods. They all stand to profit from this kind of effort.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. atterson, A. Rabkin, I.Stoica, M.Zaharia (2009), Above Clouds: A Berkeley View of Cloud Computing, Electrical Engineering and Computer Sciences University of California at Berkeley, pp1-24, February 2009.
2. Kumar, G., & Chelikani, A. (2011). Analysis of security issues in cloud-based e-learning. University of Borås/School of Business and IT.
3. S.Malkowski, Y.Kanemasa, H.Chen, M.Yamamoto, Q.Wang, D.Jayasinghe, C.Pu, and M.Kawaba (2012), Challenges and opportunities in consolidation at high resource utilization: Non-monotonic response time variations in n-tier applications, in Fifth IEEE International Conference on Cloud Computing, Honolulu, HI, USA, 2012, pp. 162--169.

4. M.Georgescu and M.Matei (2013), The value of cloud computing in business environment, The USV Annals of Economics and Public Administration, vol.13, no.1, pp. 222--228, 2013.
5. E.Gorelik(January, 2013), "Cloud Computing Models", Massachusetts Institute of Technology.
6. 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.
7. B.H. Bhavani and H.S. Guruprasad (2014), Resource provisioning techniques in cloud computing environment: A survey, International Journal of Research in Computer and Communication Technology, vol.3, no.3, pp. 395--401, 2014.
8. Bandara, I., Ioras, F., & Maher, K. (2014). Cybersecurity concerns in e-learning education.
9. K. A. Parane, N. C. Patil, S. R. Poojara and T. S. Kamble (2014), "Cloud based Intelligent Healthcare Monitoring System," 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, pp. 697-701, doi: 10.1109/ICICICT.2014.6781365.
10. Asgarali Bouyer, Bahman Arasteh (2014) "The Necessity Of Using Cloud Computing In Educational System" CY-ICER 2014, 1877-0428 © Elsevier.
11. YinghuiShi , Harrison Hao Yang , Zongkai Yang and Di Wu (2014) " 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
12. Sudhir Kumar Sharma, Nidhi Goyal, Monisha Singh (2014) " Distance Education Technologies: Using E-learning System and Cloud Computing" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 1451-1454
13. Sanjay Karak, BasudebAdhikary (2015) "CLOUD COMPUTING AS A MODEL FOR DISTANCE LEARNING" International Journal of Information Sources and Services, Vol.2: july-aug 2015,issue 4
14. Arshad Ali , Amit Bajpeye , Amit Kumar Srivastava (2015) " E-learning in Distance Education using Cloud Computing" International Journal of Computer Techniques -– Volume 2 Issue 3.
15. J. Skrinarova, M. Povinsky (2015), Comparative Study of Simulators for Cloud Computing, IEEE, PP.1-8, 2015.
16. K.Shenoy, P.Bhokare, U.Pai (2015),Fog Computing Future of Cloud Computing, International Journal of Science and Research (IJSR) Volume 4 Issue 6, pp.55-56, June 2015.
17. K.P. Saharan, A. Kumar (2015), Fog in Comparison to Cloud: A Survey, International Journal of Computer Applications, Volume 122 – No.3, pp.10-12, July 2015.
18. K. Jakimoski (2016), Security Techniques for Data Protection in Cloud Computing, International Journal of Grid and Distributed Computing, ISSN: 2005-4262, Vol. 9, No. 1, pp.49-56, 2016.
19. N.M. murthy , Kavitha P B, P. Kasana , Vishnu S N (2016), RESEARCH STUDY ON FOG COMPUTING FOR SECURE DATA SECURITY, ISSN 2394-1537 Vol. No.5,Specail Issue No.01,PP.221-227,Feb 2016.
20. X .Ouyang (2016), Spotlight: An Information Service for Cloud, IEEE, pp.1-51, MAY 2016.
21. AgahTugrulKorucu, handanAtun (2016) "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.
22. Dr. Pranav Patil (2015), "A Study of E-Learning in Distance Education using Cloud Computing"

International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 5, Issue. 8, pg.110 – 113.

23. S.Khan, S.Parkinson, Y.Qin (2017), Fog computing security: are view of current applications and security solutions, Journal of Cloud Computing: Advances, Systems and Applications, Springer open, pp.2-22, 2017, DOI:10.1186/s13677-017-0090-3.
24. P.Dhiman (2017), Fog Computing Shifting from Cloud to Fog, International Journal of Engineering Science and Computing Volume 7 Issue No.3, pp.4993-4995, March 2017.
25. Esposito, C., Castiglione, A., Pop, F., Choo, K.K.R (2017), Challenges of connecting edge and cloud computing: A security and forensic perspective, IEEE Cloud Computing 4(2), pp.13-17, 2017.
26. Bushra Zaheer Abbasi, Munam Ali Shah (2017), Fog Computing: Security Issues, Solutions and Robust Practices, Proceedings of 23rd International Conference on Automation and Computing, University of Huddersfield, Hudders field, UK, 7-8September 2017
27. Vinay kumar Pant, Ashutosh Kumar (2016) "DNA Cryptography An New Approach to Secure Cloud Data".International Journal of Scientific & Engineering Research, Volume7, Issue 6, 890 ISSN 2229-5518.
28. 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.
29. P.suresh(2016) SECURE CLOUD ENVIRONMENT USING RSA ALGORITHM. 2016, IRJET
30. 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. 3.
31. Agah Tugrul Korucu, Handan Atun (2016) "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.
32. 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.
33. 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.
34. 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.
35. 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.
36. Akhtar, N., and Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: a survey. *IEEE Access* 6, 14410–14430. doi:10.1109/access.2018.2807385
37. Brendel, W., Rauber, J., and Bethge, M. (2017). “Decision-based adversarial attacks: reliable attacks against black-box machine learning models,” in International Conference on Learning Representations (ICLR)
38. Apruzzese, G., Colajanni, M., Ferretti, L., and Marchetti, M. (2019). “Addressing adversarial attacks against security systems based on

machine learning," in 2019 11th International conference on cyber conflict (CyCon), Tallinn, Estonia, May 28–31, 2019 (IEEE), 900, 1–18

39. Chen, Y., Gong, X., Wang, Q., Di, X., and Huang, H. (2020). Backdoor attacks and defenses for deep neural networks in outsourced cloud environments. *IEEE Network* 34 (5), 141–147. doi:10.1109/MNET.011.1900577
40. Demetrio, L., Valenza, A., Costa, G., and Lagorio, G. (2020). "Waf-a-mole: evading web application firewalls through adversarial machine learning," in Proceedings of the 35th annual ACM symposium on applied computing, Brno, Czech Republic, March 2020, 1745–1752