International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

A Novel Hybrid Security Framework (HSF) with Vshield Based Firewall to Secure Cloud Computing Environment

J. Jeya Praise[1], N. Muthukumaran[2], R. Joshua Samuel Raj[3]
[1]Research Scholar: Department of Electronics and CommunicationEngineering,
Francis Xavier Engineering College,
Tirunelveli, India.
e-mail: jeyapraise14@gmail.com
[2]Professor: Centre for Computational Imaging and Machine Vision,
Department of Electronics and CommunicationEngineering,
Sri Eshwar College of Engineering,
Coimbatore, India.
e-mail: kumaranece@gmail.com
[3]Associate Professor: Department of Engineering, Design, Information and Communications Technology,
Bahrain Polytechnic,
Isa Town, Kingdom of Bahrain.
e-mail: joshuasamuelraj@gmail.com

Abstract—Cloud Computing is an emerging technology that provides an enormous amount of computing resources which includes networks, servers and storages which are accessed through the internet. In addition it allows useful provisioning of the resources based on the user's demands. A crucial aspect of cloud computing infrastructure is to provide secure and reliable services. The main challenge lies in the security issues is to reduce the impact of third party attacks in the cloud computing environment. Hence a novel Hybrid Security Framework(HSF) based on Reinforcement Learning (RL) Methodology with Vshield Firewall is proposed for securing the cloud environment. The RL method is used for deep packet inspection and VShiled based firewall is established to deny the attacks which are malicious when authenticating the signature of incoming packets. The bipartite pattern matching approach is integrated with the RL method to verify the signatures for obtaining the decisions quickly. The simulation results shows that the hybrid security framework is effective when compared with the existing methods by considering response time, resource utilization and denial of malicious attacks. This indicates that our proposed framework achieves not only better security but also attains better efficiency in cloud computing environment.

Keywords-Reinforcement Learning, Security Framework, VShield, Firewall, Bipartite Pattern Matching.

I. INTRODUCTION

Cloud computing is the recent innovative computing model which delivers the information technology as a services, where the resources can be retrieved from the cloud through internet. The cloud computing is a distrusted computing model because it allows the users to access resources and services provided by servers from various locations. Nowadays the cloud computing has been widely used in homes, companies, industries and businesses where the resources also contains sensitive information. Thus the risks for providing security and reducing malicious attacks have become an important aspect in cloud computing environment [1]. The firewall is one of the most popular security devices which have been widely used from early days of network security. However the cloud computing is totally virtualized when compared with the traditional technologies. Hence the traditional security mechanisms are not suitable for the cloud computing environment. Therefore, a novel Hybrid Security Framework (HSF) based on Reinforcement Learning (RL) Method along with the VShield Firewall is proposed for securing the cloud environment.

Firewalls are the essential security device in networks which protects public and private networks by blocking the traffic flow which is not necessary based on the filtering policy rules [2],[3]. Generally, a firewall policy contains a collection of rules which are regularly verified in a successive order. With the expansion of network complexities, it's quite common to find out the firewall policy with large number of rules. In order to overcome the above issue Vshield framework is presented for providing secure and efficient enforcement of firewall rules. The Vshield frameworks basic idea is to initially convert the firewall policies to non-overlapping numerical rules and then uses hashing technique for verifying if that particular request does match with the rule.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

Reinforcement Learning (RL) is a spontaneous decision making method that can be made use of in cloud computing environments to learn the environment and obtain the perfect results [4],[5]. Initially, Reinforcement Learning focused on learning by having the direct interaction between the slave agents and the environment which is shown in figure 1. The slave agent is called as the decision maker which will learn the entering payloads and headers in-order to attain its goal. The goal of slave agent is whether to accept the packet or to deny the packet by comparing with the database using the pattern matching algorithm and the results will be updated on Q-value table.

The pattern matching algorithm is performed by comparing the strings. The bipartite string matching algorithm works by comparing the pattern with the text files in databases in both of the directions. If the action matches with the database then the value 1 is updated in Q-value table and if no match is found then value 0 will get updated in the Q-value table. Let us assume a special scenario where in an industry makes its system migrate to the cloud. Additionally, the industry transfers its firewall to a different cloud for privacy and security issues. The firewall server for this industry is brought about by these two independent clouds as they work together for the service. So we proposed a Hybrid Security Framework (HSF) that works with the above scenario.

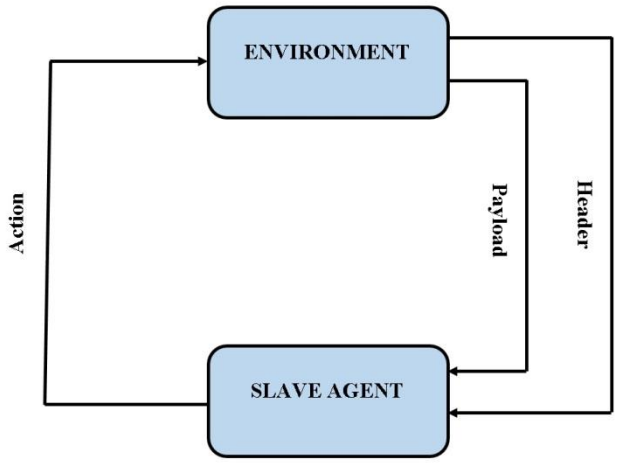

Figure 1. Direct Interaction in RL

A. Contributions

The main contributions for securing cloud computing are as follows:

- Proposed a Hybrid Security Framework (HSF) that prevents privacy of the firewall policy in cloud computing environment.
- An additional Vshield framework is presented to confidentially preserve the firewall policies which protects from malicious attackers and data loss or leakage during data transmission.
- The experimental results are indicative that the scheme proposed is secure and efficient in cloud computing environment.

B. Organization

The rest of this paper is organized as follows: An outline of related work is presented in Section 2. The system model is provided in Section 3. Section 4 presents proposed HSF methodology. Section 5 reveals the experimental results of the proposed HSF method. Finally, section 7 draws a conclusion.

II. RELATED WORKS

The related works reviews some of the work related to securing cloud computing environment. They are as follows:

With the help of firewalls and Virtual Private Networks (VPNs) most of the issues can be avoided in cloud computing infrastructure. An adequate secured solution can be provided at times by the firewalls which monitor the entering and existing traffic flow in the networks based on the security policy rules [6]. The security can be increased in VPN through an encrypted channel on the networks. In general, research on the same has been carried out to define and analyze the basic concepts in cloud. The results of firewalls and VPNs on cloud security have been evaluated.

The Bloom Filter Firewall Decision Diagram as a data structure was introduced by Gouda and Liu et. al [7] to anonymise firewall policies. But the Bloom filters were announcing false positives [8] which aren't secure at all [9], [10],[11].The impact of firewall in hybrid cloud environment was examined by Kurdi et. al. [12]. The performance of this model was evaluated with three different scenarios: firewall that blocks traffic, without firewall and with firewall. A security model was proposed by Ankush et. al. in [13]. The performance was evaluated with different scenarios in public clouds: firewall will blocking wed access, without firewall and using with firewall. The impact of firewalls and VPNs using some of the metrics of cloud performances was assessed in [14]. The analysis of security attacks and requirements in hybrid cloud was done by Na et. al. [15] and presented a secure and service model for cloud. But this limits to the lacks of scalability in cloud. Shi et. al. [11] provides privacy preserving network functionality outsourcing by constructing the conjunction obfuscator [16] in order to obfuscate the rules of firewall. The cryptographic multi-linear map exploits [11] which are created as Graded Encoding System [17]. But, the creation of multi-linear maps used in [11] resulted as insecure as proven due to the attack on Zero routine [18]. In [20], a framework had been designed depending on the Host Identity

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

Protocol and the firewall increases user security and enhances privacy in public and hybrid clouds. VGuard was proposed by Liu et. al. [21] which doesn't need any Third Party Auditor (TPA) which is constructed by X-hashfunction thus increasing the computational time to process every packet.

The pattern matching algorithm [19], [22] was introduced for parallelly matching the strings of the incoming packets. In [23], Delayed Signature Matching (DSM) technique was presented to reduce the signature matching effort when the firewall policy rules are created. COmpression INspection (COIN) framework was proposed in [24] which allows multiway pattern matching [25] over compressed traffic. This doesn't check the pattern again among the segments compressed that was matched previously.

For achieving the solution to the problems we proposed a novel Hybrid Security Framework (HSF) based on Reinforcement Learning (RL) Method along with the Vshield Firewall for securing the cloud environment. The RL method is used for deep packet inspection and VShiled based firewall is established to deny the attacks which are malicious when authenticating the signature of incoming packets. The bipartite pattern matching approach is integrated with the RL method to verify the signatures for obtaining the decisions quickly.

III. SYSTEM MODEL

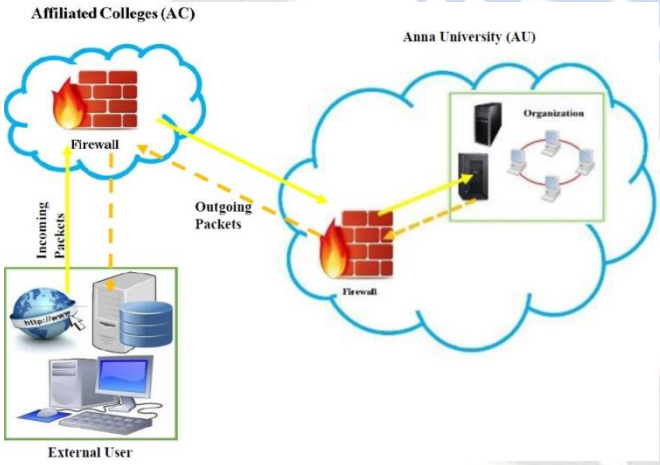

Figure 2. HSF System Architecture

A new scenario for Hybrid Security Framework (HSF) was described for an organization to outsource its firewall to a different cloud for concerns of security which is different from the scenarios used in [10], [11]. The figure 2 illustrates the framework of system architecture. Let us consider two organization clouds namely Affiliated Colleges (AC) and Anna University (AU). The infrastructure such as database server, application server etc., are located in the cloud AU and the AU cloud outsources the firewall to cloud AC. The clouds AU and AC have to cooperate with each other in-order to satisfy the Vshield firewall functions. An incoming packet from the outside network to the organization needs to be get accessed through cloud AC first and then cloud AU to reach the organization finally.

TABLE I. EXAMPLE OF FIREWALL RULE

Rule	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action
1	IP	192.168.37.*	6002	14.168.37.8	5001	Deny
2	TCP	192.168.45.*	7001	15.168.37.1	8179	Deny
3	UDP	192.145.32.*	8007	12.168.37.5	6003	Permit
4	TCP	192.*.*.*	8065	12.156.39.8	7005	Deny

An IP Firewall is a filtering method that filters packets by looking at network's ports, addresses and protocol of the packet. This will decide whether to accept the packet or to deny it. The firewall policy is created with 5-tuples such as Protocol, Source IP, Destination IP, Source Port, Destination Port and its resultant Action. The Table I shows an example of firewall rule.

In HSF architecture, the Vshield firewall functions are divided into two parts namely: 1) Bipartite Matching and 2) Decision Made (Action). Assume that the two clouds AC and AU are semitrusted. The two clouds will perform the protocol honestly. However, the clouds AC and AU are curious and try to understand the rules of Vshileld firewall. Moreover, the clouds AC and AU does not collude with each other. The Vshield framework will address cases where the AC's firewall executes deep packet inspection. The basic concept is that AC and AU applies the RL learning and Bipartite pattern matching methods to each and every character string in the database of signature, every character of incoming packet payload and finally verifies whether the result of packet payload contains the resulting string.

The cloud AC will know only the cipher-texts of the action and doesn't know about the decision made by the Vshield firewall rule. The cloud AC is also in-charge for performing matching operations. The matching operations are to discover which rule will get matched with the incoming packet. When the cloud AC found the matching among an incoming packet and Vshield firewall rules then it will transfer the packet along with the decision's cipher-texts to the cloud AU. The cloud AU is responsible for the decision making operation. When the cloud AU receives the packet and its cipher-texts, it performs the decryption for the cipher-texts and made the decision to accept or deny the packet by agreeing to the result of decryption.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

IV. PROPOSED HYBRID SECURTIY FRAMEWORK (HSF)

The cloud AC will automatically learns which rule gets matched up with the packet and also knows what rules and its corresponding decisions are. The cloud AU will process only the packets according to decryption and will not verify the header of packets. Hence, the cloud AU will know nothing about the rules of Vshield firewall except the decision made. Thus the proposed Hybrid Security Framework (HSF) method achieves security and also privacy in cloud computing environment.The Hybrid Security Framework (HSF) consists of the following three phases:

- Learning Phase
- Bipartite Pattern Matching Phase
- Decision Making Phase

A. Learning Phase

The initial phase is the Learning Phase. The work in this phase is performed by the administrator of the organization. The administrator will learn about the environment in order to set up the firewall rules. The cloud AU will set up the basic firewall rule as a parameter and the cloud AC will set up the Vshield based firewall rules. Then for each tuple the rule and its corresponding decision in firewall is generated by the administrator. The administrator of AU will generate its corresponding rule and decision's cipher-texts using AU's rule which then aggregates to Vshield firewall. The algorithm for generating the decision's cipher-texts is shown in algorithm 1. Now the administrator of AU will sends the Vshield firewall rule to cloud AC.

Algorithm 1: Generating Encryption Algorithm

*Input:*Assume plain-texts PT, String S, Block B, String Length SL, Text Left tl, Text Right tr and cipher-texts as CT.

*Output:*Encrypted Texts ET

```
*PT_S = "ABCD XYZA"
printf(" Encrypted Texts ET is");
begin
while(PT_SL)
{
   tl=tr=MSG;
   for(B=0;B<=3;B++)
   {
      tl=tl<<8;
      if(PT_SL)
      {
        tl+=*PT_S++;
        PT_SL--;
      }
      else
        tl+=0;
   }
   for(B=0;B<=3;B++)
   {
      tr=tr<<8;
      if(PT_SL)
      {
          tr=*PT_S++;
          PT_SL--;
      }
      else
      tr+=0;
   }
   encrypt(&CT,&tl,&tr);
   print("%x%x",tl,tr);
   *CT_S++=uint tl>>24;
   *CT_S++=uint tl>>16;
   *CT_S++=uint tl>>8;
   *CT_S++=uint tl;
   *CT_S++=uint tl>>24;
   *CT_S++=uint tl>>16;
   *CT_S++=uint tl>>8;
   *CT_S++=uint tr;
   CT_SL+=8;
}
end encryption algorithm
```

B. Bipartite Pattern Matching Phase

Next phase is the bipartite pattern matching phase. In this phase, the packet gets matched up with the firewall rules. The work is performed by the cloud AC in this phase. After receiving the Vshield firewall rules, the cloud AC will filter

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

the packets. For every incoming packet the cloud AC will verify the packet header using the Vshield firewall rules. If any one of the packet gets matched with the rule, then the cloud AC will transfers the packets and its corresponding decision's cipher-texts to the cloud AU. The matching operations will be performed in both the directions so that the filtering of packets time is reduced. The following algorithm reveals the training procedure of bipartite pattern matching algorithm.

Algorithm 2: Bipartite Pattern Matching Algorithm

Input:: Assume input string as *S="xyz"*, Time Taken for Matching as MT, Incoming Packet IP, Header Hr and Database db.

Output:: To find out when a key word matches occurred in S.

For all incoming packetsIP_i

Divide IP_i into set S_1 and set S_2

For each set S_1

Do

Assign every bit value to 1 in db and

Assume the length of strings as n

for(i=0;i<n;i++)

Begin

Initialize db

if db!=0 then

Read the input string

else

receive ()

do Update

db=1

if final==1

then

add to IP_i

end

For each set S2

Do

Receive ()

For string s_{i-1}

Do

Update database db

For every time Period T_i

Deny IP_i

End

end algorithm

C. Decision Making Phase

The final phase is the decision making phase. In this phase, the work is performed by the cloud AU. This phase performs the corresponding decision made with the Vshield firewall rule. When the cloud AU receives the packet and its corresponding decision's cipher-texts from the cloud AC, the AU will perform the decryption operation on cipher-texts to get the original text decision. The decryption algorithm for making the final decision is shown in algorithm 3. Now the cloud AU processes the packet according to the decision made in the original text.

Algorithm 2: Decryption Algorithm for Decision Making

Input: Assume plain-texts PT, String S, Block B, String Length SL, Text Left tl, Text Right tr and cipher-texts as CT.

*Output:*Decrypted Texts DT

```
print("Decrypted Original Texts DT is");
begin
while(CT_SL)
{
  tl=tr=MSG;
  for(B=0;B<=3;B++)
  {
    tl=tl<<8;
    tl+=*CT_SL++;
    if(CT_SL)
      CT_SL--;
  }
  for(B=0;B<=3;B++)
  {
      tr=tr<<8;
      tr+=*CT_SL++;
      if(CT_SL)
```

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

```
        CT_SL--;
    }
    decrypt(&CT,&tl,&tr);
    print("%x %x%x%x%x%x%x%x", int tl>>24, int tl>>16,
    int tl>>8, int tl, int tr>>24,int tr>>16, int tr>>8, int tr));
}
```

end decryption algorithm

V. EXERIMENTAL RESULTS

The evaluation of the proposed Hybrid Security Framework (HSF) scheme is done using the Riverbed Modeler comprises which evaluates the performance of the system by comparing with the existing frameworks. The cloud environment was developed without firewall and with firewall to study the effect of security and efficiency in cloud. Figure 3 shows the layout of public cloud infrastructure. The cloud is connected to the internet and subnets using DS links. The traffic flow, response time, throughput and delay have been examined with firewall and without firewall in cloud infrastructure. The figure 3 shows the layout of public cloud infrastructure.

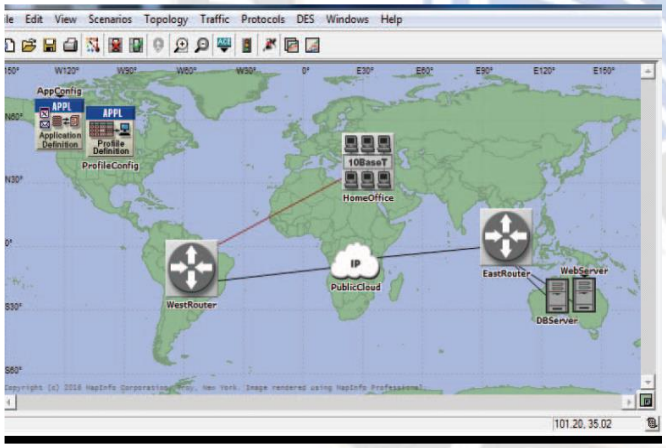

Figure 3. Layout of Public Cloud Infrastructure

A. *Performance in Learning Phase*

The figure 4 shows the performance in learning phase by comparing with and without firewall in terms of bit sizes of firewall rules and the time for processing the packets.

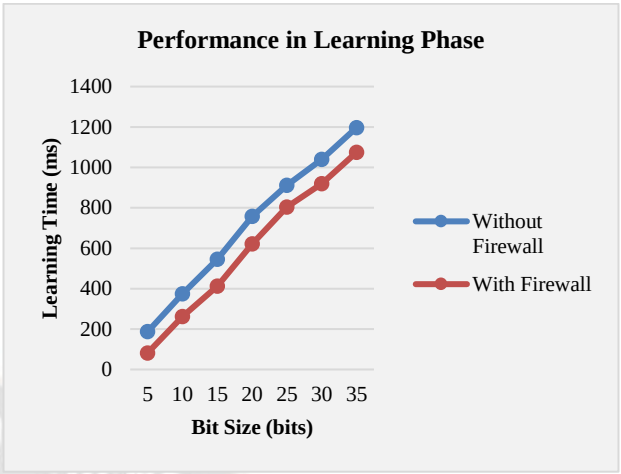

Figure 4. Performance in Learning Phase

B. *Performance in Bipartite Matching Phase*

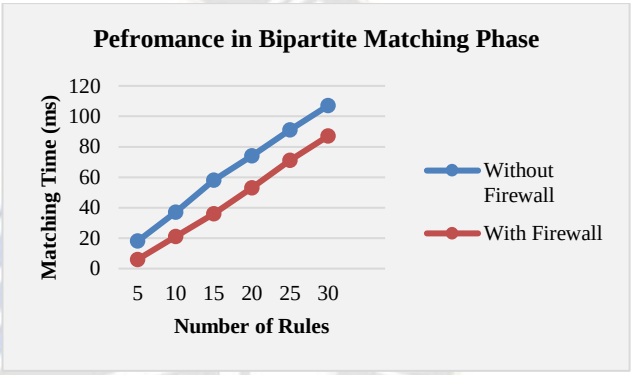

Figure 5. Performance in Bipartite Matching Phase

The figure 5 shows the performance in bipartite matching phase by comparing with and without firewall in terms of firewall rules while increasing in numbers and the time for processing the packets.

C. *Performance in Decision Making Phase*

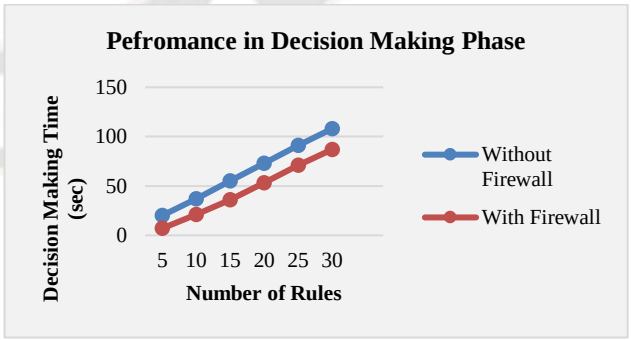

Figure 6. Performance in Decision Making Phase

The figure 6 shows the performance in Decision Making phase by comparing with and without firewall in terms of firewall rules while increasing and the time for processing the packets.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

VI. CONCLUSION

In this paper a novel Hybrid Security Framework (HSF) is proposed for providing more security and efficiency using firewall policies in Cloud Computing Environments. The proposed Vshield based firewall will also provide privacy among the networks in cloud environment. The bipartite pattern matching mechanism is used to reduce the time while matching within the databases. Thus the proposed framework achieves more security. Furthermore the simulation results reveal that the proposed HSF technique attains higher efficiency. Hence the proposed method is very useful when it is implemented with real-time cloud environment.

CONFLICTS OF INTERESTS

None to declare.

REFERENCES

[1] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012.

[2] Alhomdy, S., Thabit, F., Abdulrazzak, F.H., Haldorai, A., Jagtap, S. The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications (2021) International Journal of Intelligent Networks, 2, pp. 166-174.

[3] A. R. Khakpour and A. X. Liu, "First step toward cloud-based firewalling," Reliable Distributed Systems, 31st Symposium on. IEEE, 2012, pp. 41–50.

[4] Barret E, Howley E, Duggan J (2013) "Applying reinforcement learning toward automating resource allocation and application scalability in the cloud" Concurrency Computation and Pract Exp 25(12):1656–1674.

[5] J. Jeya Praise, R. Joshua Samuel Raj and J.V. Bibal Benifa, "Development of Reinforcement Learning and Pattern Matching (RLPM) Based Firewall for Secured Cloud Infrastructure", Wireless Personal Communcations 115, Pages: 993-1018, 2020. https://doi.org/10.1007/s11277-020-07608-4.

[6] G. Liyanage and S. Fernando, "Firewall model for cloud computing," IEEE 8th International Conference on Industrial and Information Systems, Peradeniya, 2013.

[7] M. G. Gouda and A. X. Liu, "Structured firewall design", ComputerNetworks, vol. 51, no. 4, pp. 1106–1120, 2007.

[8] B. H. Bloom, "Space/time trade-offs in hash coding with allowableerrors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.

[9] Balakrishnan, M., Nalina, M., Ramya, K., Senthilsriram, K. Cloud Computing based Data Validation and Migration in ETL using Talend (2022) 6th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2022 - Proceedings, pp. 1349-1355.

[10] L. Melis, H. J. Asghar, E. De Cristofano, and M. A. Kaafar, "Privateprocessing of outsourced network functions: Feasibility and constructions."

[11] J. Shi, Y. Zhang, and S. Zhong, "Privacy-preserving network functionalityoutsourcing," arXiv preprint arXiv:1502.00389, 2015

[12] H. Kurdi, M. Enazi and A. Al Faries, "Evaluating Firewall Models forHybrid Clouds," in Modelling Symposium (EMS), 2013 European,Manchester, 2013.

[13] Ankush Veer Reddy Vee,"Usage of OPNET IT tool to Simulate andTest the Security of Cloud under varying Firewall conditions,"Faculty of The School of Engineering & ComputingSciences, Texas A&M University-Corpus Christi, Corpus Christi, TX, 2012.

[14] S. Y. Ameen and S. W. Nourildean, "Firewall and VPN Investigationon Cloud Computing Performance," International Journal of ComputerScience & Engineering Survey, vol. 5, no. 2, pp. 15-25, 2014.

[15] Sukhmeet Singh, Nitin Sharma. (2023). Image Based Analysis for Bone Marrow Cancer Detection using Soft Computing Techniques: A Review. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 602–610. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2737

[16] S. Na, J. Park, E. Huh, "Personal Cloud Computing SecurityFramework," 2010 IEEE Asia-Pacific Services ComputingConference.

[17] Z. Brakerski and G. N. Rothblum, "Obfuscating conjunctions," inAdvances in Cryptology–CRYPTO 2013. Springer, 2013, pp. 416–434.

[18] J.-S. Coron, T. Lepoint, and M. Tibouchi, "Practical multilinear mapsover the integers," in Advances in Cryptology–CRYPTO 2013. Springer,2013, pp. 476–493.

[19] J. H. Cheon, K. Han, C. Lee, H. Ryu, and D. Stehl´e, "Cryptanalysisof the multilinear map over the integers," in Advances in Cryptology–EUROCRYPT 2015. Springer, 2015, pp. 3–12.

[20] Matti Virtanen, Jan de Vries, Thomas Müller, Daniel Müller, Giovanni Rossi. Machine Learning for Intelligent Feedback Generation in Online Courses . Kuwait Journal of Machine Learning, 2(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/188

[21] Karthika. A, Muthukumaran. N, Joshua Samuel Raj. R, 'An Ads-Csab Approach for Economic Denial of Sustainability Attacks in Cloud Storage', International Journal of Scientific & Technology Research, Vol. 9, Issue. 04, pp. 2575-2578, April 2020.

[22] M. Komu, M. Sethi, R. Mallavarapu, H. Oirola and R. Khan, " SecureNetworking for Virtual Machines in the Cloud," 2012 IEEEInternational Conference on Cluster Computing Workshops.

[23] Alex X. Liu, and Fei Chen, EEEPrivacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Network, IEEE Transactions on Parallel And Distributed Systems, VOL. 22, NO. 5, (2011)

[24] Maleeha Najam, Usman Younis, Raihan ur Rasool, "Speculative parallel pattern matching using stride-k DFA for deep packet inspection", Journal of Network and Computer Applications, Volume 54, Pages 78-87.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7650
***Article Received:** 05 June 2023 **Revised:** 30 July 2023 **Accepted:** 14 August 2023*

[25] Yingpei Zeng, and Shanqing Guo, "Deep Packet Inspection with Delayed Signature Matching in Network Auditing", https://doi.org/10.1007/978-3-030-01950-15.

[26] Andrew Hernandez, Stephen Wright, Yosef Ben-David, Rodrigo Costa, David Botha. Risk Assessment and Management with Machine Learning in Decision Science. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/196

[27] Xiuwen Sun, Hao Li, Dan Zhao, Xingxing Lu, Kaiyu Hou, Chengchen Hu, "COIN: A fast packet inspection method over compressed traffic", Journal of Network and Computer Applications, https://doi.org/10.1016/j.jnca.2018.12.008.

[28] Alexey Lukashin, Leonid Laboshin, Vladimir Zaborovsky, and Vladimir Mulukha, Distributed Packet Trace Processing Method for Information Security Analysis, LNCS 8638, pp. 535–543, 2014.