International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 1341-1346

Detecting Malware In The Iot Usingmixtureofexpertsneuralnetwork.

[1]Krishna Bhargava Anantha ramaiah,[2]DeepaTP

[1]*PG Student, Department Of CSE,MTECH, Jain Deemed To Be University Bengaluru*
[2]*assistantprofessor,Department Of CSE,MTECH, Jaindeemedtobeuniversity*

Abstract

Today's neural networks are capable of detectingmalwares found in the internet of things platform. In this paper,discussion is about usingthemixture ofexpertsneural Networktodetecteverydayemergingmalwaresandbenignwares.Themixture of experts uses the evolutionary computation principles, toevolvenewstrategieseachtimetodetectnewtypesofmalwaresfound.

Keywords—Malware,Benignware,Evolutionary Computation,MixtureofExperts,Neuralnetwork,Cybersecurity,InternetofThings.

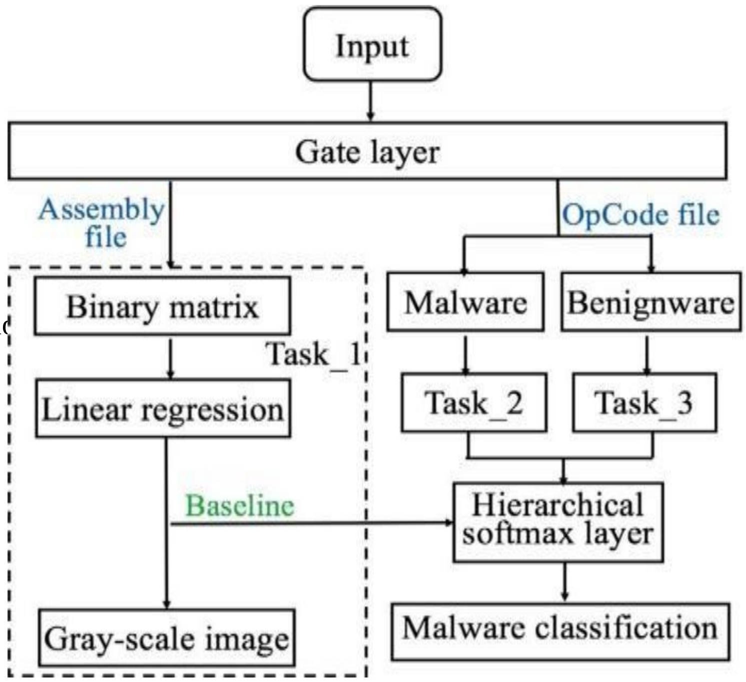
INTRODUCTION

In the present day computer science, we come across all kindsof algorithms for solving problems of society. A specific set ofalgorithmsforglobal optimizationusingbiologicalevolutionis known as evolutionary computation. It is a sub-field ofartificial intelligence and soft-computing. Here we use theevolutionary algorithm known as the Mixture of Experts,which is a neural network that is evolutionary in behaviour. Intoday's world, IOT is gaining as a major player in the world'sbusinesses. Therefore Cybersecurity is gaining momentumeveryday. The rise of artificial intelligence technologiesincluding deep learning and machine learning have madecybersecurity easier to deploy. As the threats of malware andbenignwares increases everyday and new threats emerge daily,the mixture of experts neural network intelligently evolves todetect new malware signatures that arise in the internet ofthingsplatform.

DESIGN

The figure 2.1, is the system block diagram. The gate layer,receives the input from the malware data. The assembly fileconverts the malware data into a binary matrix. Then usinglinearregressionmachinelearningtechnique,thedataisconverted into a grey scale image, to feed to the mixture ofexperts neural network. Then the hierarchical soft-max layerdetectsthemalwareandreportsittothesystem.

Figure2.1:Systembl



ISSN: 2233-7857IJFGCN

B.**MixtureofExperts**.

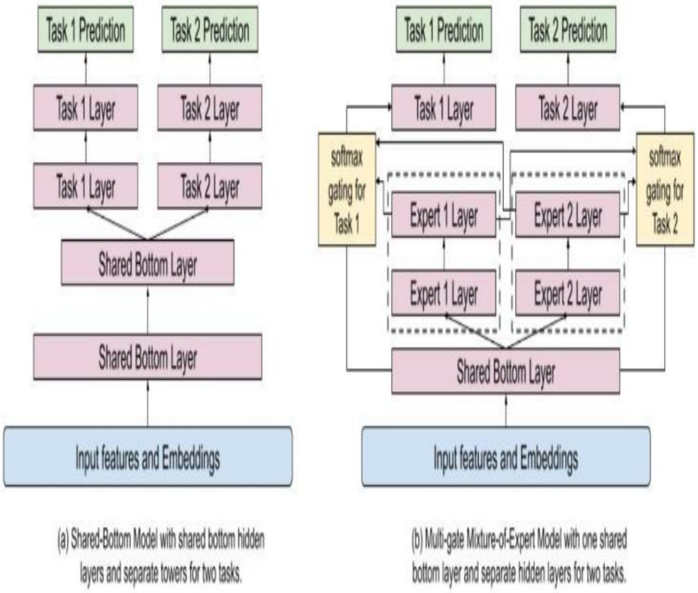


Figure2.2:Mixture ofExperts.

The mixture of experts contain two parts, first is the gatingfunction and the second is the expert system. The expertsystems are hidden layers in the neural network that classifyspecific intellectual parts of malware and benignwaresignatures.Thesoft-maxhierarchicalgatingfunctionsfeedtherequired gated signals to the experts layers to successfullydetect and verify known malware and benignware signaturesasthe output.

C. **Trainingdatacomparisons**.

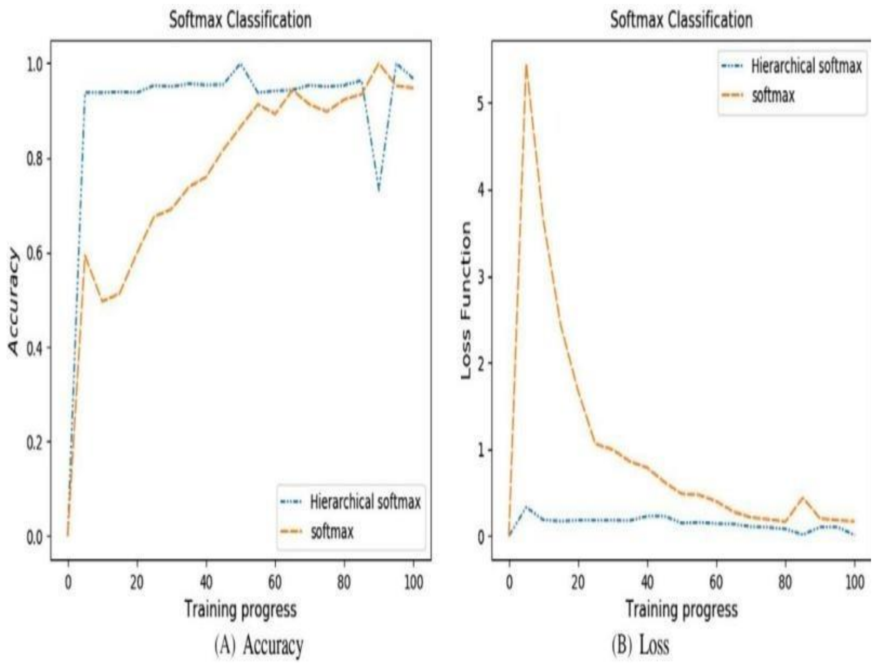


Figure2.3:Trainingusingsoft-maxclassification.

ISSN: 2233-7857IJFGCN

Theaccuracytrainingofthehierarchicalsoft-maxfunctionissaturation in time, but at the end, it delivers more accuracy.Alsothe lossfunctionislow, whichisverymuchdesirable.

***C.* Clusteringanalysisofmalware.**

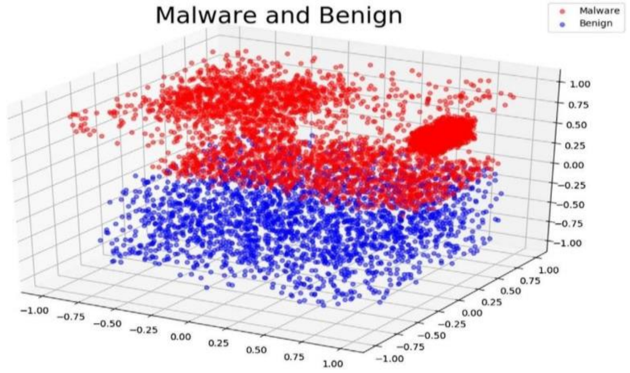


Figure2.4: Typesofmalware.

The clustering analysis shows the merging behaviour ofdifferentclusterswhichcanbeeasilyclassifiedanddetectedusing themixtureofexpertsneuralnetwork.

*C.*Psuedocode.

1:

Loop start for binary matrix and operational codes.2:

Ifassemblyfilefoundthen.3:

Encode the input data from the gating network into a binarymatrix(task 1).

4:

Starttheloopforlinearregression.5:

Input a random value.6:

Addthe biasvalue.7:

Compute value to be feed into task 2 and task 3.8:

Calculatethegradientdescent.9:

Calculatethelossfunction.10:

end for11:

end if12:

Ifoperationalcodesfoundandprocessed,continue.13:

Gettheencodedbinarymatrix.14:

Start loop for task 2 and 3.15:

Computetherandomvaluematrix.16:

Compute the bias value.17:

Outputtheresult.18:

Lettask2declarethe result,ifmalwarefound.Lettask3declaretheresultif benignware found.

19:

ISSN: 2233-7857IJFGCN

Calculategradientdescent.20:

Calculatelossfunction.21:

end for22 :end if

LITERATURESURVEY.

A. An internet of things malware classification method basedonmixture of expertsneural network.

Thispaperdiscussesusingthemixtureofexpertstoclassifymalware.

A. Machine Learning with Big Data: Challenges andApproaches.

This paper discusses the binary matrix and linear regressiontechniquesneeded for malwaredetection.

B. AnalyzingDisinformationandCrowdManipulationTacticsonYouTube.

Thispaperdiscussesthecybersecurityissuesencounteredin YouTube.

C. Videomakesthecodingstar?

Thispaperdiscussesthemachinelearningcapabilitiesinimageclassificationof malwaresignatures.

D. YouTube Data Analysis using MapReduce on Hadoop.This paper discusses how this method of malwareclassification can be extended to Big Data applicationsthrough YouTubedataanalysis.

E. RecommendingWhatVideotoWatchnext:AMultitaskRankingSystem.

Thispaperdiscussesbriefrankingsystemsofpopularvideostreamingplatforms, usedintheneuralnetwork.

F. Ahybridrecommendationsystemwithmany-objectiveevolutionaryalgorithm.

Thispapergivesintroductiontoevolutionarycomputation.

G. AMusicRecommendationSystembasedonMelodyCreation byInteractive GA.

This paper discusses signal processing in data and musicanalysis.Usedforsignalprocessingapplicationsinthegatingfunction.

REFERENCES

1. GubbiJ,BuyyaR,MarusicS,PalaniswamiM.InternetofThings (IoT): a vision, architectural elements, and futuredirections. Future
2. GeneratComputSyst.2013;29(7):1645-1660.
3. Chen X, Li A, Guo W, Huang G. Runtime model basedapproachtoIoTapplicationdevelopment.FrontiersComputSci. 2015;9(4):540-553.
4. Huh S, Cho S, Kim S. Managing IoT devices usingblockchainplatform.Paperpresentedat:Proceedingsofthe201719thInternational
5. ConferenceonAdvancedCommunicationTechnology(ICACT);2017:464-467; IEEE.
6. Hamdan O, Shanableh H, Zaki I, Al-Ali AR, Shanableh T.IoT-basedinteractive dualmodesmarthomeautomation.
7. Paperpresentedat:
8. Proceedings of the 2019 IEEE International Conference onConsumerElectronics(ICCE);2019:1-2;IEEE.
9. Yang Y, Zheng X, Tang C. Lightweight distributed securedatamanagementsystemforhealthinternetofthings.JNetwComputAppl.
10. 2017;89(7):26-37.
11. Khan MA, Salah K. IoT security: review, blockchainsolutions,andopenchallenges.FutureGeneratComputSyst.2018;82:395-411.
12. SicatoS, CostaJ,Sharma PK,LoiaV,ParkJH.VPNFiltermalwareanalysis oncyberthreatinsmarthomenetwork.
13. ApplSci.2019;9(13):2763.
14. SharmaP,ZawarS,PatilSB.Ransomwareanalysis:Internetof Things (Iot) security issues challenges and open problemsinthecontext

ISSN: 2233-7857IJFGCN

15. of worldwide scenario of security of systems and malwareattacks.Paperpresentedat:ProceedingsoftheInternationalConferenceon
16. RecentInnovationsEngineeringandManagement;2016.
17. WangA,LiangR,LiuX,ZhangY,ChenK,Li J.Aninsidelook at IoT malware. Paper presented at: Proceedings of theInternational
18. ConferenceonIndustrialIoTTechnologiesandApplications;2017:176-186;Springer.
19. Zhiwu XU, Ren K, Song F. Android malware familyclassificationandcharacterizationusingCFGandDFG.Paperpresented at:
20. Proceedings of the 2019 International Symposium onTheoreticalAspectsofSoftwareEngineering(TASE);2019:49-56;IEEE.
21. Alasmary H, Khormali A, Anwar A, et al. Analyzing,comparing,anddetectingemergingmalware:agraph-basedapproach;2019.arXiv
22. preprintarXiv:1902.03955.
23. AlhanahnahM,LinQ,YanQ,ZhangN,ChenZ. Efficientsignature generation for classifying cross-architecture iotmalware.Paper
24. presented at: Proceedings of the 2018 IEEE Conference onCommunications and Network Security (CNS); 2018:1-9;IEEE.
25. Su J, Vasconcellos VD, Prasad S, Daniele S, Feng
26. Y,SakuraiK.LightweightclassificationofIoTmalwarebasedonimage recognition.
27. Paper presented at: Proceedings of the 2018 IEEE 42ndAnnualComputerSoftwareandApplicationsConference(COMPSAC);vol.2,
28. 2018:664-669;IEEE.
29. HaddadPajouhH,DehghantanhaA,KhayamiR,ChooK-KR. A deep recurrent neural network based approach forInternetofthingsmalwarethreathunting.FutureGeneratComputSyst.2018;85:88-96
30. AzmoodehA,DehghantanhaA,ContiM,ChooK-KR.Detecting crypto-ransomware in IoT networks based onenergy consumption
31. footprint. J Ambient Intell Humaniz Comput. 2018;9(4):1141-1152.
32. BanT,Isawa R,HuangS-Y,YoshiokaK,Inoue D.Across-platform study on emerging malicious programstargeting IoTdevices. IEICE
33. TransactInfSyst.2019;102(9):1683-1685.
34. Meidan Y, Bohadana M, Mathov Y, et al. N-BaIoT:network-based detection of IoT botnet attacks using deepautoencoders.IEEEPervas
35. Comput.2018;17(3):12-22.
36. Azmoodeh A, Dehghantanha A, Choo K-KR. Robustmalwaredetectionforinternetof(battlefield)thingsdevicesusing deepeigenspace
37. learning.IEEETransactSustainComput.2018;4(1):88-95.
38. Shazeer N, Mirhoseini A, Maziarz K, et al. Outrageouslylargeneuralnetworks:thesparsely-gatedmixture-of-expertslayer;2017.arXiv
39. preprintarXiv:1701.06538.
40. MaJ,ZhaoZ,Yi X,ChenJ,HongL,ChiEH.Modelingtask relationships in multi-task learning with multi-gatemixture-of-experts. Paper
41. presented at: Proceedings of the 24th ACM SIGKDDInternationalConferenceonKnowledgeDiscovery&DataMining;2018:1930-1939;
42. ACM.
43. DarabianH,DehghantanhaA,HashemiS,HomayounS,Choo K-KR. An opcode-based technique for polymorphicInternetofthings
44. malwaredetection.ConcurrComputPractExp.2019;32(6):e5173.
45. Usha Kiruthika,Thamarai Selvi Somasundaram, S. Kanaga Suba Raja, (2020) 'Lifecycle Model of a Negotiation Agent: A Survey of Automated Negotiation Techniques', Group Decision and Negotiation, ISSN 0926-2644, Volume 29, Issue - 6, pp. 1239–1262. https://doi.org/10.1007/s10726-020-09704-z
46. EigenD,RanzatoMA,SutskeverI.Learningfactoredrepresentations in a deep mixture of experts; 2013. arXivpreprintarXiv:1312.4314.

ISSN: 2233-7857IJFGCN

47. Martinez MT. An Overview of Google's MachineIntelligenceSoftwareTensorFlow.Albuquerque,NM:SandiaNationalLab.(SNL-NM);2016.12of12
48. YANGetal.
49. Weisberg S. Applied Linear Regression. Hoboken, NJ:JohnWiley&Sons; 2005.
50. LiuP,QiuX,HuangX.Recurrentneuralnetworkfortextclassification with multi-task learning; 2016. arXiv preprintarXiv:1605.05101
51. ChenM,AnnadataAK,ChanL.Adaptivecommunicationapplication programming interface. Google Patents; U.S.PatentNo.7,581,230,
52. August25,2009.
53. Asadi K, Littman ML. An alternative softmax operator forreinforcementlearning.Paperpresentedat:Proceedingsofthe34thInternational
54. ConferenceonMachineLearning;2017:243-252.
55. Oh J, Yun K, Maoz U, Kim T-S, Chae J-H. Identifyingdepression in the national health and nutrition examinationsurvey datausinga
56. deep learning algorithm. J Affect Disorders.2019;257(10):623-631.
57. Morin F, Bengio Y. Hierarchical probabilistic neuralnetwork language model. Paper presented at: Proceedings ofthe10thInternational
58. WorkshoponArtificialIntelligenceandStatistics;2005:246-252;Citeseer.
59. Kasongo SM, Sun Y. A deep long short-term memorybasedclassifierforwirelessintrusiondetectionsystem.ICTExpress. 2019.https://
60. doi.org/10.1016/j.icte.2019.08.004.
61. Ficco M. Detecting IoT malware by Markov chainbehavioralmodels.Paperpresentedat:Proceedingsofthe2019IEEEInternational
62. Conference on Cloud Engineering (IC2E); 2019:229-234;IEEE.
63. Nataraj L, Karthikeyan S, Jacob G, Manjunath BS.Malwareimages:visualizationandautomaticclassification.Paperpresentedat: Proceedings of the 8th International Symposium onVisualizationforCyberSecurity;2011:118-125;ACM.
64. AhmadiM,UlyanovD,SemenovS,Trofimov M,Giacinto
65. G.Novelfeatureextraction,selectionandfusionforeffectivemalwarefamily
66. classification.Paperpresentedat:Proceedingsofthe6thACMConference on Data and Application Security and Privacy;2016:183-194;ACM.
67. Xia Y, Leung H, Kamel MS. A discrete-time learningalgorithmforimagerestorationusinganovel L2-normnoiseconstrained estimation.
68. Neurocomputing.2016;198(7):155-170.
69. SantosI,BrezoF,NievesJ,etal.Idea:opcode-sequence-based malware detection. International Symposium onEngineering Secure Software and Systems.NewYork,NY:Springer;2010:35-43.
70. Murugan, S., Jeyalaksshmi, S., Mahalakshmi, B., Suseendran, G., Jabeen, T. N., & Manikandan, R. (2020). Comparison of ACO and PSO algorithm using energy consumption and load balancing in emerging MANET and VANET infrastructure. Journal of Critical Reviews, 7(9), 2020.
71. Efficient Contourlet Transformation Technique for Despeckling of PolarimetricSyntheticApertureRadarImage Robbi Rahim, S. Murugan, R. Manikandan, and AmbeshwarKumarJ. Comput. Theor. Nanosci. 18, 1312–1320 (2021)

ISSN: 2233-7857IJFGCN