A Hybrid approach using digital forensics for attack detection in a cloud network environment

Shaweta Sachdeva [1], Aleem Ali [2]
Research Scholar Department of CSE, Glocal University Saharanpur, U.P., India [1]
Associate Professor, Department of CSE, Glocal University Saharanpur, U.P., India [2]

Abstract

In the recent era, the web is the major means used by cyber-criminals to carry out attacks alongside people and groups. Due to the continually increasing number of Internet users these attacks might influence from an enormous goal surface. Characteristic attacks commit during the ICMP Attack, TCP Sync Attack, UDP ATTACK, log analysis scamming, and so on. In the few last years, we have seen the growth of a threat through data sending or receiving via the internet. In demanding they use various web technologies for arranging the victim's machine and to build, at runtime, the appropriate response to being sent to the client. Provide a deep insight into this problem and proposes narrative solutions for the analysis of existing ICMP Attack, TCP Sync Attack, UDP Attack, log analysis. With the Hybrid approach using digital forensics for attack detection in a cloud network environment make a less complex system for improving the current issues of the computational complexity and applying cyber Forensic investigation (KNN, MLP). Our proposed approach is very effective for classification the attack dataset.

Keywords: Digital forensics, Attack detection, Cloud Computing, TCP,ICMP, UDP.

1. INTRODUCTION

Establish a network of multi-hop cloud we are mainly at the network's fingertips. An authenticating user consents to the use of a cloud space for the storage or retrieval of the file or several data, so each nod is associated with the neighboring node and is deployed to compete in the network neighborhood when a packet is generated by a sender. Cloud networks [1] that build and manage cloud networks and security events. Before that, browse and pick the source files and the selected data is rehabilitated to a set packet size and sent to a destination from the source. Track and analyze the events in the network using the genetic algorithm [2] to identify irregular behaviors. The intruding identification is different for the identification of improper, wrong, or anomalous moving attackers as a mechanism for a network packet. The packet is blocked when the genetic algorithm stipulates an abnormal behavior. After the invalid packets are screened, they are blocked and any correct packet arrives at the destination. Depending on cloud networks for location and technique employed by the engine to generate warnings, there are many ways to identify IDs. All three elements are merged into a single system or computer in several simple implementations. After the invalid packets are screened, they are blocked and any correct packet arrives at the destination.Depending on cloud networks form and location and technique employed by the engine to generate warnings, there are many ways to identify IDs. All three elements are merged into a single system or computer in several simple implementations.The proposed method for selecting the wrapper feature can optimize feature subsets and kernel parameters at the same time, which allows the functionality of the Cloud environment data feature selection process.

1.1 SECURED PROTOCOL

The convention includes in the cloud environment ought to be made more secure and propel, which can guarantee more security to client's information. UDP [3] is an untrustworthy convention that ought to be stayed away from in the information bundle exchange, while then again HTTP is a secured convention that ought to be taken in thought by cloud administration. Such conventions give security to the client information at the season of information exchange from one client record to the next.

1.2 SESSION SECURITY

To confer a more secure cloud environment to the client the session made ought to be of lesser timeframe which implies sessions ought to be made secured by diminishing the time interim of session expiry. With this procedure it would be troublesome for a programmer to peep into the session of some client.

1.3 DIGITAL EVIDENCE

Advanced proof can be characterized, data or information of essential utilize that has created through some computerized medium. The advanced proof may include documents store, memory information, and virtual memory information in structure recordings or depictions and so on exchanged over some system [2].

1.4 ATTACKS CLOUD NETWORK

The term security includes insurance against anything else, such as hazards or attacks that may hurt the system. Danger is an item, a single person or a separate material that is a persistent threat to a benefit. This danger involves acts carried out without any intention or sinister intent causing more misconceptions through freshness and dishonor. Human disappointment can bring about an issue with the general system. Planned demonstrations of trespass happen when unapproved singular access the system that has been ensured by the proprietor. It implies that the system is currently not secret for the proprietor Intentional demonstrations of treachery. This class of danger includes a demonstration of treachery or vandalism to either annihilate the system's advantages or harm the association. Case of this danger are an extremist or digital lobbyist operations furthermore digital fear based oppression. The hazard of theft implies that the illicit taking of another's property.This is a perilous risk where at some point the proprietor's system may not know until the wrongdoing is unreasonably late.

2. RELATED WORK

A literature review found few journals, newspaper articles or lectures based on cloud forensics analysis;
We identify two attack modes to detect DDoS attacks: Fixed IP Attacks (FSIA) and RSIA
JiaO, J. et al[1], proposed the idea to detect attack, we identify two attack modes: Based on the attacker's source IP address. We also propose an in-house DDoS detection method based on TCP in real time to extract successful features of TCP traffic and distinguish between malicious and natural traffic across two decision tree classifications.
Saini, P. S., et al. [2], proposed machine learning based approach to detect and classify different types of network traffic flows. The proposed approach is validated using a new dataset which is having mixture of various modern types of attacks such as HTTP flood, SID DoS and normal traffic. A machine learning tool called WEKA is used to classify various types of attacks. It has been observed that J48 algorithm produced best results as compared to Random Forest and Naïve Bayes algorithms.
Dominik Birk in et al[3] ,this proposed the idea that it used addressing part for the technological issues of forensics in all three main models of the cloud infrastructure, they center the notion of cloud forensics and take interdisciplinary aspects into account. Also it discusses the usefulness of different evidence sources for research purposes and provides possible approaches from a realistic perspective to the issues. This article should be viewed as an exploration of a virtually unexplored area of study.
Grispos in et al [4] , In this paper firstly they show that the end devices can be used in a cloud forensic study to provide a partial view of the evidence. In this contribution, practitioners are centered on methods that offer a fresh approach to realistic approaches to emerging cloud issues. Second, it helps record and provide proof to evaluate the artifacts generated on iOS and Android smartphone for different Cloud storage applications.

Georgios Pierris in et al [5] ,This paper proposed the automated forensic examiner has another more practical problem to address files which are not in the file-system and more precisely missing files, or broken files, and how to transform the proof after an automated process that is very computer-intensive. It addresses explicitly the issue of cloud data mining, where deleted data is almost instantly overwritten; thus, the majority of deleted files are removed.

Josiah Dykstra in et al[6], This research still continues to exist in the cloud as an objective system for the forensic investigation. The versatile nature of cloud computing enables a criminal to commit crimes and to destroy the evidence immediately, but this condition is not taken into consideration here. While some cases include the cloud as the weapon of crime, others are targeted by the cloud-hosted infrastructure.

Hong Guo, Bo Jin in et al[7],The rise of cloud computing pushes digital forensics into a different horizon..The acquisition and analysis of digital evidence is likely to be complicated by cloud computing. The number of computer forensic analysis devices inside the cloud that may need forensic examination in cloud environments will take longer and more effort.

Joshi R.C., et al.[8],Cloud forensics and analysis issues are addressed. A common cloud forensics method model and four steps are addressed, including discovery, compilation, acquisition and conservation.

Liu C., et al. [9], ATTACK is a worldwide information centre for adverse strategies and methods built by real-world assault observations.

Moustafa N., Slay J. [10], proposed a forensic network control and analysis system for threats dependent on the network. The scheme collects and saves network traffic data. Using the chi-square figures, it chooses main network traffic features and identifies anomalous incidents using a modern technology for correction.

Fernandes, D.A.B., et al. [11],In addition to problems arising from Internet and Network technology, clouds raise new problems which need to be deleted first ,to further expand the amount of cloud installations.

Hemdan E.ED., et al. [12] ,The model in this paper will improve the chance of tracking attackers, find vulnerabilities in potential usage of virtual machines and can even help digital evidence gathering and extraction.

Möller D.P.F., et al. [13], This paper Contains a broad variety of concerns on automotive data protection issues and sources and recommendations for further reading.

3. PROPOSED METHODOLOGY

In data management, ICMP Attack, TCP Sync Attack, UDP ATTACK[14] are all the businesses which need to log analysis based on the information or data which is a stored or transacted entity. Every effort [15] must be made to guard the effects and secure their information too securely. Throughout this phase, there are legal departments that partly seek to protect their records. The legal requirements are an essential component of the company’s contact. The trade has to ensure in some cases that the vendor meets the demands.

For a special purpose, a forensics server [16] in the company cloud can be hand-down.A dedicated forensic server is offline and can be accessed whenever appropriate. It is a strategic option as the client is not faced with the organizational problem involved. In a company, a copy of virtual machines will be assigned to different occurrence [17] respondents. This happens if new sources of substantiation emerge and a company-level analysis is needed. When it's found to be compromise on a demanding cloud, the cloning on that server is done to reduce the confirmation acquisition time. This cloned disk can be accessed for the discovery purpose from a forensic site [18]. When the equipment is unaware of the datacenter, the process of forensic screening development slows down. When the hunt for data goes on, the program has to be careful for a short time. The project was divided into two phases by the limitation of the position [19]. A prototype called trust surveillance system was used on the provisioned server [20] in the first step. During the second process, a range of freeware cloud tools were examined with a conservative forensic system on the client side for evidence.

To overcome the above listed issues in ICMP Attack, TCP Sync Attack, UDP ATTACK, log analysis [21]and pattern discovery[22] required to design a new data model by which the problem is satisfied. To evaluate the large scale [23] data a search algorithm is suitable. Therefore, genetic algorithm [24] is used for frequent pattern analysis. However, to handle this huge amount of log genetic algorithm is relatively slow process. On the other hand the available data includes the number of unique web pages and their access patterns thus, required to optimize the algorithm by pre-processing of the data. Therefore, k-nearest neighbour algorithm is applied to keep in track the selection process of KNN, MLP [25] .That algorithm helps to find the duplicate data patterns from the available set of data. For analysing the nearest data patterns over number of session algorithm uses the Euclidian distance and the similar data is eliminated from the data set. This process reduces the amount of data for evaluation. The combination of two different models is leads to design a hybrid approach for data analysis.

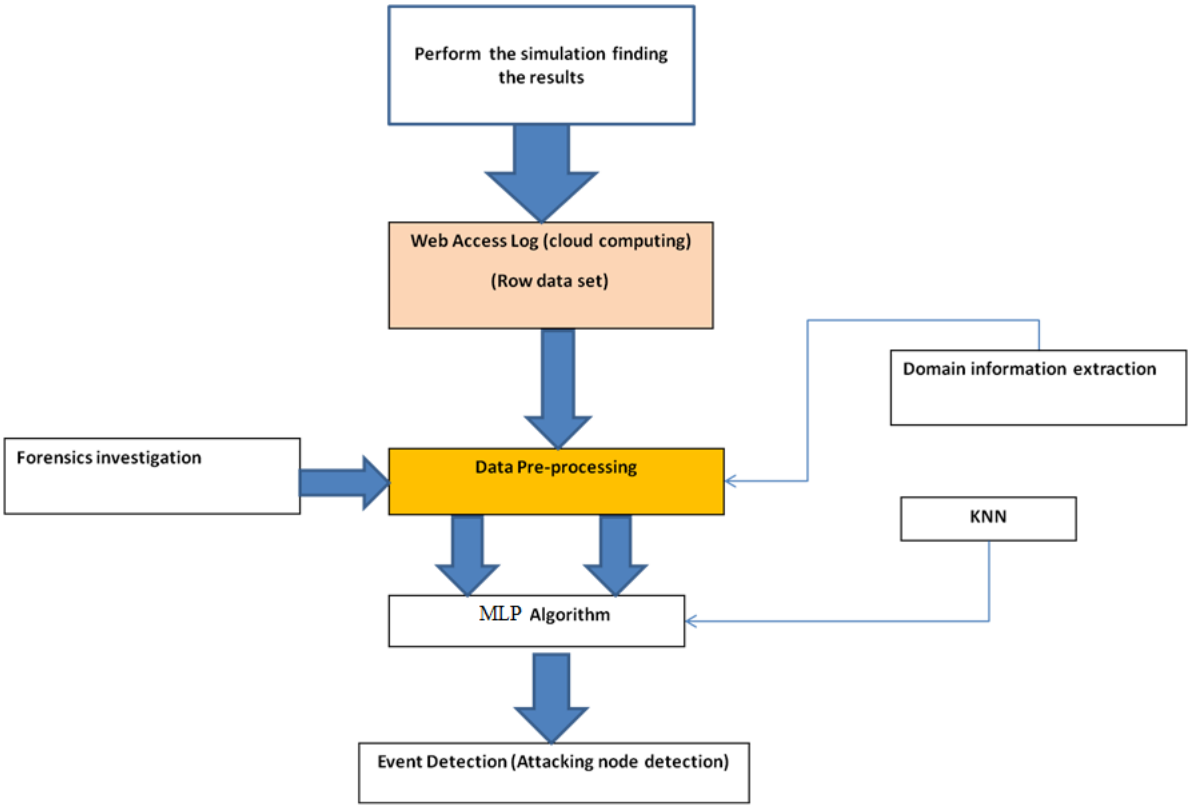

Perform the simulation finding the results
Web Access Log (cloud computing)
(Row data set)
Domain information extraction
Forensics investigation
Data Pre-processing
KNN
MLP Algorithm
Event Detection (Attacking node detection)

Figure 1: proposed model

Our plan incorporates KNN[26] and genetic algorithms to enhance the precision of the classification of attacks.We was using genetic search to prune the redundant, unimportant packet and to classify the packet[27] that more contributes to categorization[28]. The least classified packet is erased and the algorithm of classification is based on evaluated data. The classifier is trained as an attacker to classify data [29]. There are two parts to our proposed algorithm.

1) Primary part deals with evaluate attributes using genetic search

2) Part two deals with construction classifier and measure accuracy of the classifier

Proposed algorithm

Step 1) load the data set

Step 2) be appropriate genetic search on the data set

Step 3) Attributes are ranked based on their value

Step 4) Select the partition of higher ranked data set

Step 5) Apply (KNN+ MLP) on the subset of attribute that maximizes Classification accuracy

Step 6) compute correctness of the classifier, which procedures the ability of the

Classifier to suitably classify unidentified sample.

Step 1 to 4 comes below part 1 which deals with attributes and their position.

Step 5 is use to construct the classifier and step 6 proceedings the accuracy of the classifier.

Correctness of

The classifier is compute as Accuracy = no. of model appropriately classified in test data / Total no. of illustration in the test data

Moreover, many current cloud issues such as the question of authority and the lack of international cooperation are intensified. Software forensic analysis can be more complicated because data can be stored or processed on web-based cloud computing[28] platforms in various jurisdictions.The data model developed is evaluated[30]. The achieved results and the performance parameters assessed are discussed in this section during experiments. This section also reports comparative findings[31] with conventional genetic algorithms.

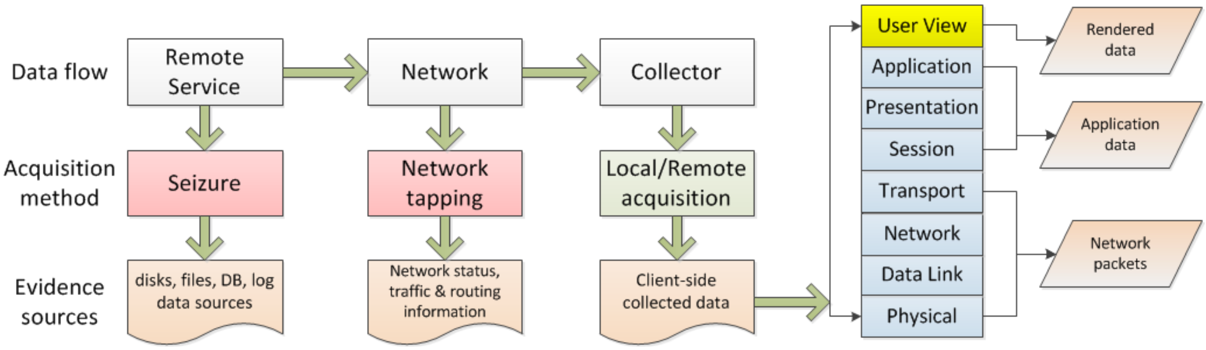
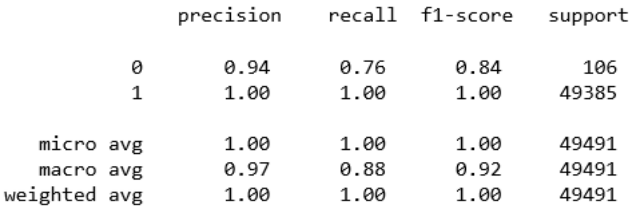


Figure 2: Simulation Architecture

Show in Figure2 function of the proposed data flow first technical, acquisition methods , data source such as ICMP attack, TCP Sync Attack, UDP ATTACK, network analysis access to data via network status, traffic, and routing information.The packet headers include the IP addresses of the source and destination that can be used to correctly classify the parties involved and the network of the examined server. The packet inspection can be used to detect potential communication errors which may have altered the target service details. In addition, each packet header contains correct low-level information with time stamps a packet stream is considered a reliable source of evidence. A packet analyzer can track the quality of the stream, and also provides a high-level view of traffic.As a result, numerous static and semi static detection systems are looking at programming patterns which, in conjunction met other clues, look like decoding or deobfuscation routines in all to determine whether they may or may not be malware.

Attacking log analysis Classification with proposed Hybrid approach using digital forensics for attack detection using machine learning results shown below:

ICMP attack



```
              precision    recall  f1-score   support

           0       0.94      0.76      0.84       106
           1       1.00      1.00      1.00     49385

   micro avg       1.00      1.00      1.00     49491
   macro avg       0.97      0.88      0.92     49491
weighted avg       1.00      1.00      1.00     49491
```

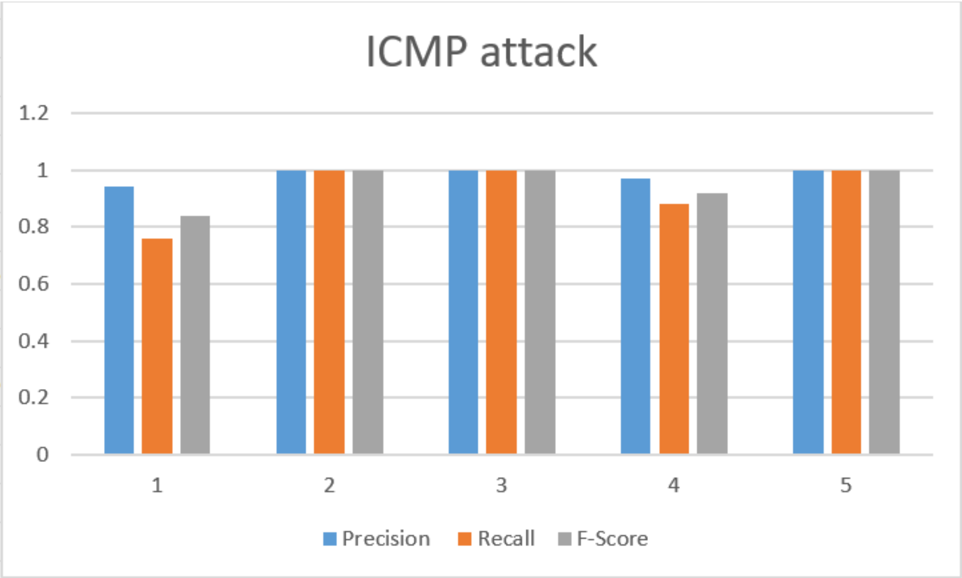
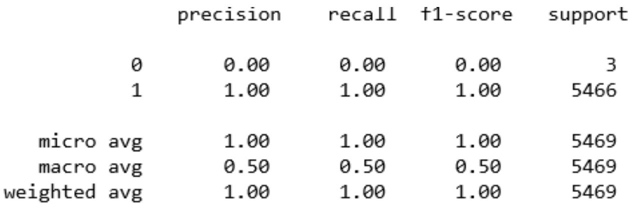


Figure 3: ICMP attack

Accuracy is

Accuracy of the model is: 99.93938291810632 Confusion Matrix: [[81 25] [5 49380]]

TCP attack



```
              precision    recall  f1-score   support

           0       0.00      0.00      0.00         3
           1       1.00      1.00      1.00      5466

   micro avg       1.00      1.00      1.00      5469
   macro avg       0.50      0.50      0.50      5469
weighted avg       1.00      1.00      1.00      5469
```

Accuracy is

Accuracy of the model is: 99.94514536478333 Confusion Matrix: [[0 3] [0 5466]]

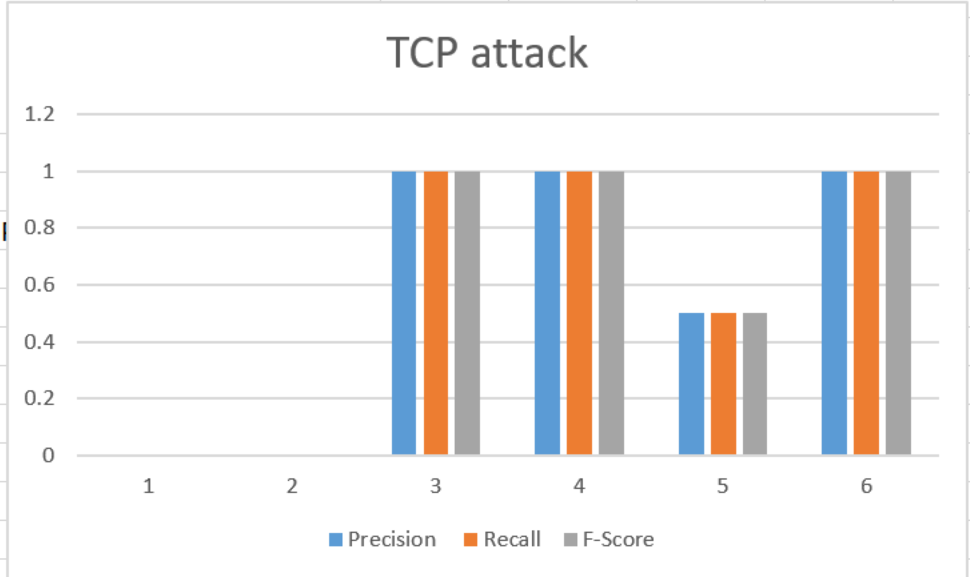
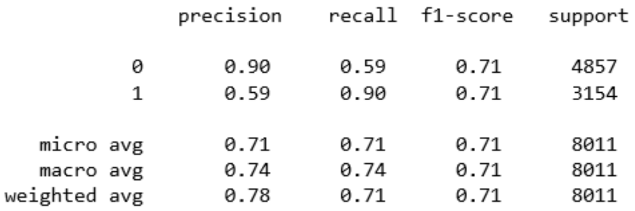


Figure 4: TCP attack



```
              precision    recall  f1-score   support

           0       0.90      0.59      0.71      4857
           1       0.59      0.90      0.71      3154

   micro avg       0.71      0.71      0.71      8011
   macro avg       0.74      0.74      0.71      8011
weighted avg       0.78      0.71      0.71      8011
```

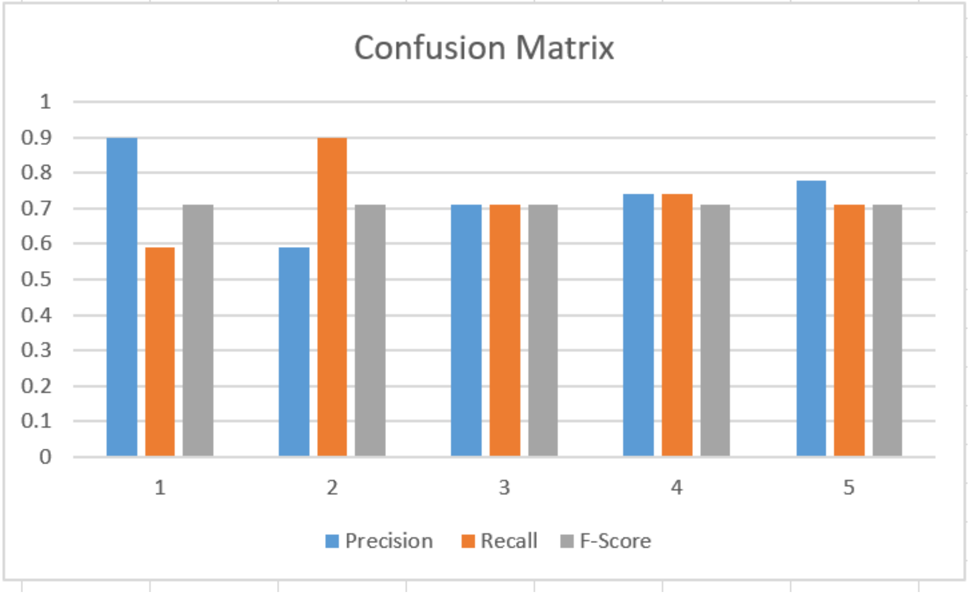
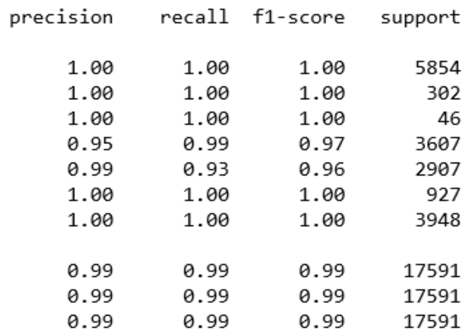


Figure 5:Confusion Matrix

Accuracy of the model is: 70.98988890275871 Confusion Matrix: [[2852 2005] [319 2835]]

Performance Report is



```
precision    recall  f1-score   support

     1.00      1.00      1.00      5854
     1.00      1.00      1.00       302
     1.00      1.00      1.00        46
     0.95      0.99      0.97      3607
     0.99      0.93      0.96      2907
     1.00      1.00      1.00       927
     1.00      1.00      1.00      3948

     0.99      0.99      0.99     17591
     0.99      0.99      0.99     17591
     0.99      0.99      0.99     17591
```

Accuracy: 0.99’

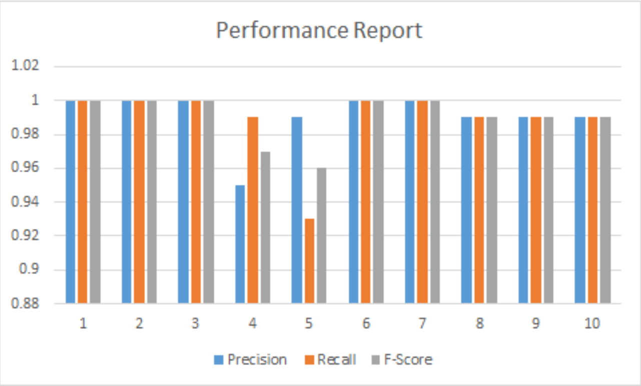


Figure 6: Performance Report is Accuracy: 0.99’

To perform the simulation using the python tools with anaconda platform with help of Jupiter notebook we write the code and using the different number of the attacking with log file data set then applying our proposed machine learning (KNN+ MLP) algorithm compute the accuracy level of this algorithm and compute the precision , recall , f1 score , support. Our proposed approach accuracy level is 99.93.

Conclusion

The main purpose of the combined technology is to identify and obtain digital forensic evidence from cloud-based environments. The composite methodology needs to consider the variety of cloud modelling among modern forensic practitioners.They may as well have tested a range of methods to collect data from a variety of Cloud based applications that subsist before the execution of a search warrant. The proposed selection technique for function (KNN+MLP) will at a similar time optimize the sub-sets and parameters of characteristics and thus function containers in hyper-spectral data collection. We represent through the experiment our proposed approach accuracy is 99% in compare to existing ones.

Reference

[1]. Jiao, J., Ye, B., Zhao, Y., Stones, R. J., Wang, G., Liu, X., Xie, G.”Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers”. IEEE 36th Symposium on Reliable Distributed Systems (SRDS). pp: 256-258, 2017 ,doi:10.1109/srds.2017.37.

[2]. Saini, P. S., Behal, S., & Bhatia, S. “Detection of DDoS Attacks using Machine Learning Algorithms”. 7th International Conference on Computing for Sustainable Global Development (INDIA.Com).pp;16-21,2020. Doi:10.23919/indiacom49435.2020.9083716.

[3]. Dominik Birk,ChristophWegener,"Technical Issues of Forensic Investigations in Cloud Computing Environments".Systematic Approaches to Digital Forensic Engineering (SADFE), IEEE Sixth International Workshop on Publication Year: 2011 , Pp: 1-10, 2011 .

[4]. George Grispos,William Bradley Glisson,TimStorer,"Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services".pp:4910-4919,2013 IEEE- DOI 10.1109/HICSS.2013.592.

[5]. Georgios Pierris, Stilianos Vidalis,"Forensically Classifying Files Using HSOM Algorithms",Third International Conference on Emerging Intelligent Data and Web Technologies.pp:225-230,2012, doi: 10.1109/EIDWT.2012.46.

[6]. Josiah Dykstra, Alan T. Sherman,"Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques" Digital Investigation .pp:590-598, 2012, https://doi.org/10.1016/j.diin.2012.05.001.

[7]. Hong Guo, Bo Jin,TingShang,"Forensic Investigations in Cloud Environments" International Conference on Computer Science and Information Processing (CSIP) pp:248-251 ,2012. **DOI:** 10.1109/CSIP.2012.6308841.

[8]. Joshi R.C., Pilli E.S. "Cloud Forensics. In: Fundamentals of Network Forensics" ,Computer Communications and Networks. Springer, London.pp:187-202,2016, https://doi.org/10.1007/978-1-4471-7299-4_10.

[9]. Liu C., Singhal A., Wijesekera D. "Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments".. IFIP Advances in Information and Communication Technology, vol 589. Springer,2020,pp:161-180,2020, https://doi.org/10.1007/978-3-030-56223-6_9.

[10]. Moustafa N., Slay J."A Network Forensic Scheme Using Correntropy-Variation for Attack Detection. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIV. DigitalForensics" IFIP Advances in Information and Communication Technology, vol 532. Springer, Cham. pp: 225-239, 2018, https://doi.org/10.1007/978-3-319-99277-8_13.

[11]. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V. et al. "Security issues in cloud environments: a survey". Int. J. Inf. Secur. 13, pp: 113–170, 2014. https://doi.org/10.1007/s10207-013-0208-7.

[12]. Hemdan, E.E.-D., Manjaiah D.H."CFIM: Toward Building New Cloud Forensics Investigation Model".Innovations in Electronics and Communication Engineering. Lecture Notes in Networks and Systems, vol 7. Springer, Singapore. pp: 545-554, 2018, https://doi.org/10.1007/978-981-10-3812-9_56.

[13]. Möller D.P.F., Haas R.E." Automotive Cybersecurity. In: Guide to Automotive Connectivity and Cybersecurity". Computer Communications and Networks. Springer, Cham.pp:265-377, 2019, https://doi.org/10.1007/978-3-319-73512-2_6.

[14]. AbhaBelorkar,G. Geethakumari,"Regeneration of events using system snapshots for cloud forensic analysis" Annual IEEE India Conference ,2011. Doi:10.1109/INDCON.2011.6139350

[15]. Rainer Poisely, Erich Malzer, and Simon Tjoa,"Evidence and Cloud Computing:The Virtual Machine Introspection Approach"Reliability and Security (ARES'12), Prague, Czech Republic, pp:135-152,August 2012.

[16]. Ahalawat, A., Dash, S. S., Panda, A., &Babu, K. S. (2019)." Entropy Based DDoS Detection and Mitigation in OpenFlow Enabled SDN". International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) ,2019,doi:10.1109/vitecon.2019.8899721.

[17]. Shams Zawoad, RagibHasan," I Have the Proof: Providing Proofs of Past Data Possession in Cloud Forensics" Xiv:1211.4328v1 [cs.CR] 19 Nov 2012.

[18]. Mark Taylor, John Haggerty, David Gresty, David Lamb,"Forensic investigation of cloud computing systems" Elsevier B.V. or its licensors or contributors .pp:907-917, 2016, https://doi.org/10.1016/j.procs.2020.03.390.

[19]. Denis Reilly, Chris Wren, Tom Berry,"Cloud Computing: Pros and Cons for Computer Forensic Investigations"International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, pp:26-34, March 2011, DOI:10.20533/ijmip.2042.4647.2011.0004.

[20]. Shams Zawoad, RagibHasan,"Digital Forensics in the Cloud", pp:16353-16359, 2013, DOI:10.15680/IJIRSET.2016.0509112.

[21]. Inikpi O. Ademu, Dr Chris O. Imafidon, Dr David S. Preston "A New Approach of Digital Forensic Model for Digital Forensic Investigation," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.12, pp:175-178 ,2011, DOI : 10.14569/IJACSA.2011.021226.

[22]. Duy, P. T., Hien, D. T. T., & Pham, V.-H. " A role-based statistical mechanism for DDoS attack detection in SDN" ,5th NAFOSTED Conference on Information and Computer Science (NICS),pp:177-182, 2018, doi:10.1109/nics.2018.8606851.

[23]. A. A. Shaikh, H. Qi, W. Jiang and M. Tahir, "A novel HIDS and log collection based system for digital forensics in cloud environment", 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, pp: 1434-1438, 2017,doi: 10.1109/CompComm.2017.8322779.

[24]. E. E. Hemdan and D. H. Manjaiah, "Spark-based log data analysis for reconstruction of cybercrime events in cloud environment," 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT), Kollam, pp: 1-8, 2017, doi: 10.1109/ICCPCT.2017.8074209.

[25]. A. K., S. Grzonkowski and N. A. Lekhac, "Enabling Trust in Deep Learning Models: A Digital Forensics Case Study," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, pp: 1250-1255, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00172.

[26]. Liu C., Singhal A., Wijesekera D."A Layered Graphical Model for Cloud Forensic Mission Attack Impact Analysis", In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIV. DigitalForensics IFIP Advances in Information and Communication Technology, vol 532. Springer, Cham.pp:263-289,2018, https://doi.org/10.1007/978-3-319-99277-8_15.

[27]. Karabiyik U., Akkaya K. "Digital Forensics for IoT and WSNs" Ammari H. (eds) Mission-Oriented Sensor Networks and Systems: Art and Science. Studies in Systems, Decision and Control, vol 164. Springer, Cham.pp:171-207,2019 https://doi.org/10.1007/978-3-319-92384-0_6.

[28]. Hemdan E.ED., Manjaiah D.H. " Cybercrimes Investigation and Intrusion Detection in Internet of Things Based on Data Science Methods",Sangaiah A., Thangavelu A., MeenakshiSundaram V. (eds) Cognitive Computing for Big Data Systems Over IoT. Lecture Notes on Data Engineering and Communications Technologies, vol 14. Springer, Cham.pp:39-62, 2018, https://doi.org/10.1007/978-3-319-70688-7_2.

[29]. Rajawat A.S., Upadhyay P., Upadhyay A. " Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing". Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham.pp:652-661, 2020, https://doi.org/10.1007/978-3-030-55180-3_49.

[30]. Liu C., Singhal A., Wijesekera D."Identifying Evidence for Cloud Forensic Analysis", Chaudhary S., Somani G., Buyya R. (eds) Research Advances in Cloud Computing. Springer, Singapore.pp:371-391,2017, https://doi.org/10.1007/978-981-10-5026-8_15.

[31]. Mohiddin S.K., Babu Y.S. " Role of Cloud Forensics in Cloud Computing",Das K., Bansal J., Deep K., Nagar A., Pathipooranam P., Naidu R. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol 1057. Springer, Singapore.pp:978-981,2020, https://doi.org/10.1007/978-981-15-0184-5_9.

[32]. Aleem Ali, Neeta Singh.“M/M/1/n+Flush/n model to enhance the QoS for Cluster Heads in MANETs” published in “International Journal of Advanced Computer Science and Applications (IJACSA)”, U.K. 2018. ESCI, Scopus.

[33]. Aleem Ali, Neeta Singh. “QoS Analysis in MANETs Using Queueing Theoretic Approaches A review”, International Journal of Latest Trend in Engineering and Technology (IJLTET), Vol. 7, Issue 1, pp. 120-124, May 2016. UGC listed.

[34]. Nazia Parveen, Ashif Ali, Aleem Ali.” IOT Based Automatic Vehicle Accident Alert System”, 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), pp. 330-333, 30-31 Oct. 2020, Greater Noida, DOI: 10.1109/ICCCA49541.2020.9250904. (Scopus Indexed) .