International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1126-1128 www.ijaem.net ISSN: 2395-5252

Privacy Leakage by Cyberspace Cookies Log for Web Application Using DOD Algorithm in Cyber Security

A.Ishwarya,K.Santhiya,M.Veeralakshmi,Professor.D.Pavun Raj,M.E(Asp/CSE)

Department of Computer Sceince Engineering For women, Sivakasi, Tamil Nadu

Submitted: 10-03-2021 Revised: 30-03-2021 Accepted: 01-04-2021

ABSTRACT: This project proposes the model for detecting and preventing the attack through cookies log file . This is made by analyzing the dataset of certain vital parameter such as identifying ,preventing the attack by using different techniques they are Greedy algorithm , Denial of Defense (DOD) algorithm ,PYQT5 algorithm. The dataset containing the history of attack files, type of protocols, cookies logs, types of attack, location classification for privacy leakage via tracking user cyberspace privacy leakage real potent threat to user privacy . where the cookie can contain a “secure” flag ,implying that it can only be transmitted over an HTTPS link. There is no corresponding flag to show how a cookies has been set: attackers who operate as a man in the middle attack this session will insert cookies to subsequent of HTTPS connection. This propose model is to improve the throughput and accuracy even if the number of malicious nodes is very small.

Keyword: Privacy, cookies, location classification, protocols

I. INTRODUCTION:

Nowdays man can able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but transmitted or sent to the other person safely without any leakage of information. The answer lies in cyber security. we utilize the network traffic data collected via a DPI system at the routers within one of the largest internet operators. only cookies in the HTTP header traffic which contain users’ online service IDs during the online login process are collected and used or other personally identifiable information is collected. Truth is that majority of computer systems including business ones have not any threat about the data DDOS attack in opposition to the other networks.

II. LITERATURE SURVEY:

In this research area the increasing popularity and diversity of social media sites . This problem faces tremendous challenges.1) extracting features and 2) constructing predictive models from a variety of perspectives. Propose work they used key achievements of user identity linkage across online social networks including state of the art algorithm.

These shows user in the protection of her privacy by allowing her to define her privacy requirements, which user been hidden from the advertising platforms an be revealed. our proposal allows fine grained and user tailored privacy protection.

In this scheme based on the trust or threat model and processing/ storage capacity at the server and the client. These results are compared with the traditional security hash function such as SHA-1 and MD5. To overcome this bottleneck.

III. EXISTING SYSTEM

The existing scheme has very low throughput even if the number of malicious node is very small. In this scheme severely affected by malicious nodes that drop or modifiy packets.OLSRv2 is susceptible to various attack such as worm hole attack, black hole attack, spoofing , jamming, and so on which is a type of denial of service attack

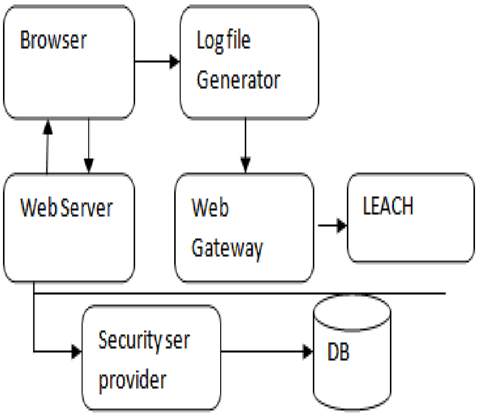
IV. PROPOSED SYSTEM

The proposed system focus on the dissertation to come up with better understanding of network security application and standards. The main aim to avoid performing membership test by the attacker, the ids of all storage cell are encrypted using cell keys, and the hashed and inserted into BF. Scheme which can achieves much faster response time and provide of parallelization on execution time.

V. MODULES

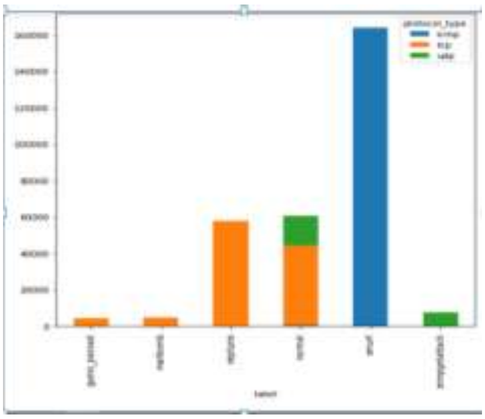
1.Admin Node Assembler
2.Cyberspace Cookie Log
3.Web Security Provider
4.Protocol Secure Device

VI. SYSTEM ARCHITECTURE:

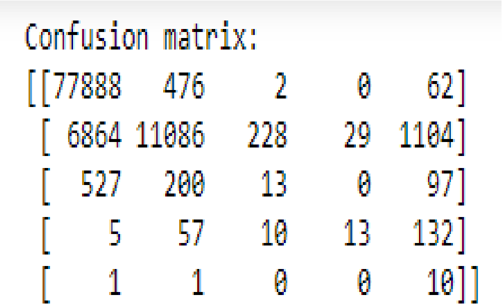


VII. METHODOLOGY

- Networking and Protocols
- Security threats and vulnerabilities
- Security attacks
- Security techniques and tools
- Extracting results on the basic of simulation results

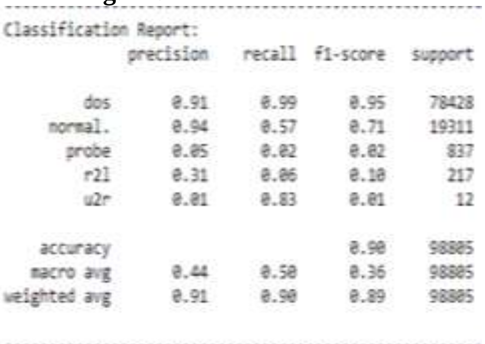


.Fig,No:1 Prototype used to prevent attack



```
Confusion matrix:
[[77888   476     2     0    62]
 [ 6864 11086   228    29  1104]
 [  527   200    13     0    97]
 [    5    57    10    13   132]
 [    1     1     0     0    10]]
```

Fig.No: 2 Confusion matrix

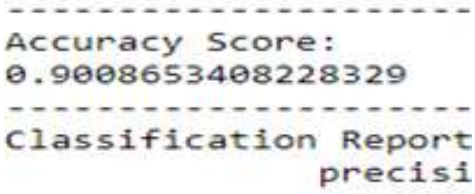


```
Classification Report:
              precision    recall  f1-score   support

         dos       0.91      0.99      0.95     78428
     normal.       0.94      0.57      0.71     19311
       probe       0.05      0.02      0.02       837
         r2l       0.31      0.06      0.10       217
         u2r       0.01      0.83      0.01        12

    accuracy                           0.90     98805
   macro avg       0.44      0.50      0.36     98805
weighted avg       0.91      0.90      0.89     98805
```

Fig.No: 3 Classification Report



```
---------------------
Accuracy Score:
0.9008653408228329
---------------------
Classification Report
              precisi
```

VIII. CONCLUSION

The aim of this thesis was to explore the network vulnerabilities and in-depth analysis of different security attack and security solutions. To identify the scope of latest technology and its application on the area of web cookies and it is time sensitive function.

IX. FUTURE WORK

Expert agree that today's major challenges is not the security technology itself but how to make appropriate procedures and controls for achieving IT security. Hackers will still remain in the market and even their number seem to be growing .Attacking tools will continue to advance , as will security solution. It is better to look for the major vulnerabilities and try to eliminate them using with existing resource.

REFERENCE:

[1]. K. Shu, S. Wang, J. Tang, R. Zafarani, and H. Liu, "User identity linkageacross online social networks: A review,"ACM SIGKDD ExplorationsNewsletter, vol. 18, no. 2, pp. 5–

17, 2017

[2]. X. Zhou, X. Liang, X. Du, and J. Zhao, “Structure based user identi-fication across social networks,”IEEE Transactions on Knowledge andData Engineering, vol. 30, no. 6, pp. 1178–1191, 2018.

[3]. D. Sanchez and A. Viejo, “Privacy-preserving and advertising-friendlyweb surfing,” Computer Communications, vol. 130, pp. 113–123, 2018.

[4]. H. Choi, J. Park, and Y. Jung, “The role of privacy fatigue in onlineprivacy behavior,”Computers in Human Behavior, vol. 81, pp. 42–51,2018.

[5]. X. Zhou, X. Liang, X. Du, and J. Zhao, “Structure based user identi-fication across social networks,”IEEE Transactions on Knowledge andEngineering ,vol. 30, no. 6, pp. 1178–1191, 2018

[6]. H. Wang, Y. Li, Y. Chen, and D. Jin, “Co-location social networks:Linking the physical world and cyberspace,”IEEE Transactions on Mobile Computing, vol. 18, no. 5, pp. 1028–1041, 2018.

[7]. H. Wang, Y. Li, G. Wang, and D. Jin, “You are how you move: Linking multiple user identities from massive mobility traces,” in. SDM,2018, pp. 189–197.

[8]. J. Feng, M. Zhang, H. Wang, Z. Yang, C. Zhang, Y. Li, and D. Jin,“Dplink: User identity linkage via deep neural network from heteroge-neous mobility data,”