IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing

Syed Suleman [1], Khaja Mohammed Ali Khan [2], Mohammed Aftab Uddin [3], Mrs. Imreena Ali [4]

[1,2,3]B.E Student, Dept. of Computer Science Engineering, ISL Engineering College

[4]Assistant Professor (PhD), Dept. of Computer Science Engineering, ISL Engineering College

ABSTRACT

In recent years, there has been a noticeable decrease in the time it takes for hackers to exploit newly discovered vulnerabilities. This is well shown by recent incidents, such the Log4j vulnerability. Hackers began searching the web for sites that would be susceptible to the vulnerability in the hours after its publication, with the intention of deploying malware such as bitcoin miners and ransomware on such hosts. Therefore, in order to maximise the efficacy of preventative operations, it is crucial for the cybersecurity defence strategy to recognise threats and their capabilities as early as feasible. The enormous amount of data and information sources that need to be analysed for indications that a danger is growing makes finding new threats a tough undertaking for security analysts, despite how vital it is. To that end, we provide a system that can automatically detect and profile new threats based on their characteristics, with MITRE ATT&CK serving as a database of threat information and Twitter posts as an event source. The three primary components of the framework are as follows: first, the naming and classification of cyber threats; second, the use of two machine learning layers to filter and categorise tweets in order to profile the detected danger according to its aims or goals; and third, the creation of alarms depending on the risk posed by the threat. Our study primarily offers a method to categorise and profile the detected threats according to their objectives, which gives more background information about the danger and potential ways to lessen its impact. Our tests showed that the profiling stage was 77% accurate in its threat profiling.

INTRODUCTION

Because of the rise of hyper-connectivity and hyper-mobility, people are more and more dependent on the Internet for their personal, professional, and societal lives. The Internet has grown into an essential tool for governments, corporations, and society as a whole, but it has also raised concerns about the prevalence of cyber assaults driven by malicious actors. Intelligence on cyber vulnerabilities and assaults, often called threats, must be timely if organisations are to be protected against cyber exploits [1].

An example of threat intelligence would be "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." [2]. Cyber threat intelligence, also known as threat intelligence in the cyber security sphere, aids in the identification of possible security vulnerabilities and assaults by providing up-to-date and pertinent information, such as attack signatures.

Both official and informal sources formally disseminate threat information in structured data format, from which cyber threat intelligence may be typically retrieved. A similar format and structure are adhered to by structured threat intelligence, which follows a well-defined data model. Security technologies may quickly analyse and react to security risks based on structured cyber threat information. Two official databases that collect information on cyber threats are the National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE) database.Informal sources of cyber threat intelligence include public forums, social media, dark webs, blogs, and public blogs. Any Internet user or organisation may use informal sources to instantly disseminate danger intelligence in an unstructured data or natural language manner. One name for the freely accessible, unstructured threat information is

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

Open Source information (OSINT). Intelligence services pertaining to cyber defence serve as early warning systems for cyber security incidents including exploitation of security vulnerabilities. Cybercriminals usually need to do the following before launching an attack: 1) find security holes; 2) learn how to exploit such holes; 3) choose a target and enlist help; 4) build or buy the infrastructure required; and 5) plot and carry out the assault. It is possible for victims, security experts, and system administrators to coordinate a response to assaults or discuss potential vulnerabilities. The digital footprints left behind by these behaviours are commonly traced back to their occurrence on social media, (open and dark) web forums, and professional blogs. Taken as a whole, these digital footprints provide important information about the ever-changing nature of cyber threats and may alert users to an impending or ongoing assault before any harmful actions are detected on the targeted system. As an example, Twitter is a good place to talk about vulnerabilities before they're publicly announced, and dark web forums are even better.

LITERATURE SURVEY

Intelligence collected via publicly accessible sources, including as blogs, social media, wikis, and forums, is known as open source intelligence (OSINT). Platforms like this are often used by cybercriminals, system administrators, security experts, and victims of cyberattacks to discuss exploits and vulnerabilities and to coordinate responses to assaults. Data collected from open source intelligence (OSINT) sources can supplement intelligence gathered from structured intelligence sources, which typically provide indicators of compromise (IOCs) like malicious IP addresses and hashes, which security platforms must monitor or block, but its volume and unstructured format make it more difficult to consume. Given Twitter's big data features—a huge amount of data, a very broad pool of users, high accessibility, and, most importantly, the fast generation of new content—and its capacity to naturally aggregate numerous sources, we have decided to utilise it as an OSINT source. The cybersecurity industry loves this platform because it allows offensive and defensive practitioners to talk shop, report attacks, promote malware, and provide timely signs of vulnerabilities, assaults, and other cyber events that security researchers find interesting. Over the last decade, Twitter has grown into a significant intelligence resource. Researchers have been able to utilise Twitter to gather intelligence on a variety of topics, including terrorist acts, earthquakes, forest fires, and more, because to the real-time nature of the information posted there. various first reports of cyber incidents, such as the revelation of various 0-day vulnerabilities, user reports of distributed denial of service assaults, and the exposing of ransomware operations, highlight Twitter's usefulness in terms of security. As an example, the worldwide ransomware epidemic of "Petya/NotPetya" in June 2017 was covered by mainstream media after extensive discussion on Twitter. Log4Shell is another example of a more modern cyber threat that was first discussed on Twitter. An attack known as Log4Shell took use of a flaw in the widely used Java logging library Log4j2 (CVE 2021-44228). On December 9, 2021, the Twitter account @P0rZ9 revealed the Log4j2 vulnerability and provided a link to the attack code, which allows a simple approach to exploit a vulnerability. In the hours after this tweet went live, hundreds of Twitter accounts, including those of cyber security experts and independent researchers, began discussing the flaw. Several frameworks for detecting and analysing threat indicators in the TwitteR have been proposed in recent years as a result of research on Twitter-based OSINT collection, which is expected given the significant and persistent presence of the cyber security community on Twitter. Based on real-world observations, Mitre ATT&CK is a knowledge library on adversary tactics and procedures that is available worldwide. Cybersecurity product and service providers, government agencies, and commercial companies all utilise the ATT&CK knowledge source as a springboard for creating their own unique threat models and approaches.4 When first developed in September 2013, the ATT&CK paradigm mainly targeted the Windows business environment, as stated in MITRE ATT&CK Design and Philosophy. Just so we're clear, let's say an enemy is planning to hack into a company's systems in order to steal sensitive information. If the attacker wants to steal data from a company's systems, they'll need to get into those systems, hop from host to host until they reach the server. The MITRE ATT&CK database may be used to trace every step an attacker has taken since breaking into the company's systems in order to steal the data. For instance, the 'Valid Credentials' method may be used to access the company's system, which is connected to the 'Initial Access' approach. Maintaining this example, MITRE ATT&CK not only maps strategies and methods but also gives a list of procedures on how adversaries proceed to implement each approach. Every approach has its own set of mitigation and detection processes, which are both provided by MITRE ATT&CK.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

While detection refers to techniques to identify an intrusion using the approach, mitigations are suggestions for how defenders might use the technique to lessen the likelihood of being effectively targeted by it. By now it should be clear that MITRE ATT&CK is a gold mine of information for cyber security experts everywhere, but notably for defenders, who can utilise it to research and prepare for a wide variety of assault methods. However, our goal in this study is to find more ways to use MITRE ATT&CK as a resource for both people and robots. Our goal is to use this collaborative and ever-changing knowledge base to build machine learning algorithms that can automatically profile cyber threats based on their intentions and block out tweets about harmful conduct.

SYSTEM ANALYSIS

There has been a lot of progress in cybersecurity research in recent years, and it is a growing issue for most organisations. The Security Operations Centre (SOC) serves as the nerve centre of these organisations, protecting them from cyber attacks. In order to keep an IT infrastructure safe and up-to-date, the SOC needs reliable threat information that is both timely and relevant. As a result, security analysts aim for danger awareness via the consumption of several information sources. Doing it manually, however, is a time-consuming and laborious process that, due to the abundance of irrelevant data, may provide little useful information. Open Source Intelligence (OSINT) is a valuable tool for spotting new cyber dangers, according to studies.

Gathering, analysing, and using information derived from publicly accessible sources is known as open source intelligence (OSINT) [21]. Blogs, forums, social media, black web, and deep web are some examples of open source intelligence (OSINT) sources. Cybersecurity events, new threats, and vulnerabilities, as well as any other relevant information, may be published in real-time using natural language on such platforms. Among open source intelligence (OSINT) sources for cyber threat information, Twitter stands out as a prominent example [22]. Hackers, system administrators, and cyber security specialists are always sharing their experiences and discussing the technical aspects of cyber assaults on Twitter [4].

SYSTEM DESIGN

The system requirements, operating environment, architecture of the system and subsystems, design of files and databases, input formats, layouts of output, processing logic, external interfaces, and detailed design are all documented in the system design document.

MODULES

Service Provider:

The Service Provider must provide their username and password in order to access this module. After he successfully logs in, he will be able to perform things like browse datasets and run tests and training on them. View the results of the trained and tested accuracy in a bar chart, see the predicted data sets, see the ratio of cyber threat identification types, see all remote users, and view the cyber threat identification types.

View and Authorize Users

The admin can get a complete rundown of all registered users in this section. Admins may see user information including name, email, and address, and they can also authorise people here.

METHODOLOGY:

The data is partitioned into sets and then trained for distinct models, as seen in the picture above. A training set (consisting of 80% of the dataset) and a pre-training set (20%) were first created. Both the pre-train and pre-test subsets made up 80% of the pre-training set. • The next step is to split the training set in half, with 80% going into the train set and 20% into the validation set. A similar split exists here, with 80% going to the train set and 20% to the test set. I now have two non-overlapping sets: one for train validation and one for test. • To determine which models performed best on the provided dataset, the pretrain set was used. I selected the top four models from the pretest batch. The mean absolute errors were used to compare their performance. After identifying the top four models, we fine-tuned their hyperparameters and picked the most effective one.

SYSTEM ARCHITECTURE

The conceptual model that describes the structure, behaviour, and additional perspectives of a system is called a system architecture. A system may be formally described and represented in an architectural description. Structured to facilitate

https://doi.org/10.5281/zenodo.11517825

reasoning about the system's architecture and behaviours.

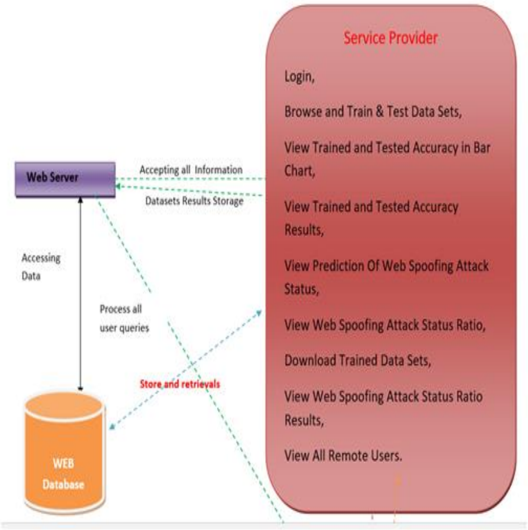

Service Provider
Login,
Browse and Train & Test Data Sets,
View Trained and Tested Accuracy in Bar Chart,
View Trained and Tested Accuracy Results,
View Prediction Of Web Spoofing Attack Status,
View Web Spoofing Attack Status Ratio,
Download Trained Data Sets,
View Web Spoofing Attack Status Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database

Figure 1: System Architecture

Construction of Use case diagrams:

Using the results of a use-case study, UML developers may construct a specific kind of behavioural diagram known as a use case diagram. Its objective is to provide a visual summary of a system's functionality shown in terms of players, their objectives (use cases), and any interdependencies among those use cases. A use case diagram's primary goal is to reveal which actors are responsible for the execution of certain system operations. One may illustrate the functions of the system's participants.

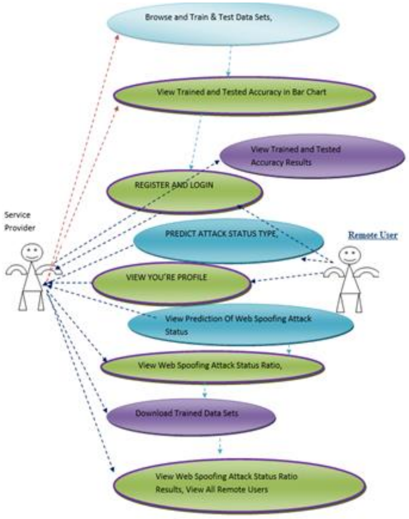
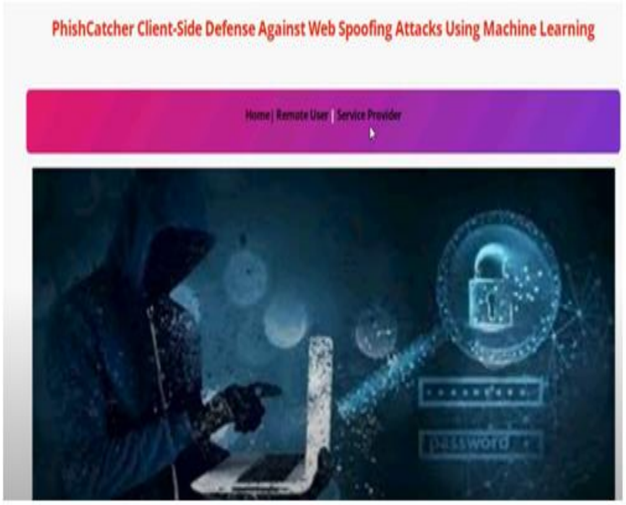

Browse and Train & Test Data Sets,
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
REGISTER AND LOGIN
Service Provider
PREDICT ATTACK STATUS TYPE,
Remote User
VIEW YOU'RE PROFILE
View Prediction Of Web Spoofing Attack Status
View Web Spoofing Attack Status Ratio,
Download Trained Data Sets
View Web Spoofing Attack Status Ratio Results, View All Remote Users

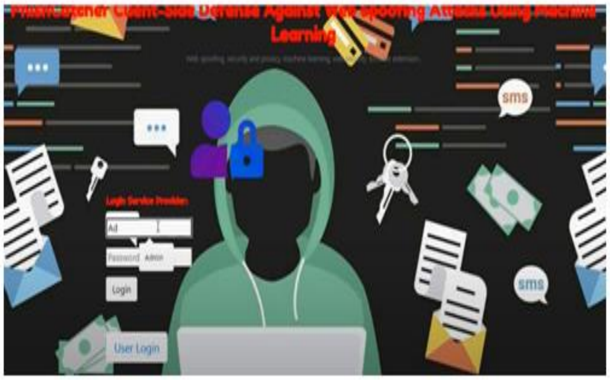
Figure 1 Use Case Diagram

OUTPUT SCREENS

MAIN PAGE


PhishCatcher Client-Side Defense Against Web Spoofing Attacks Using Machine Learning

Login page

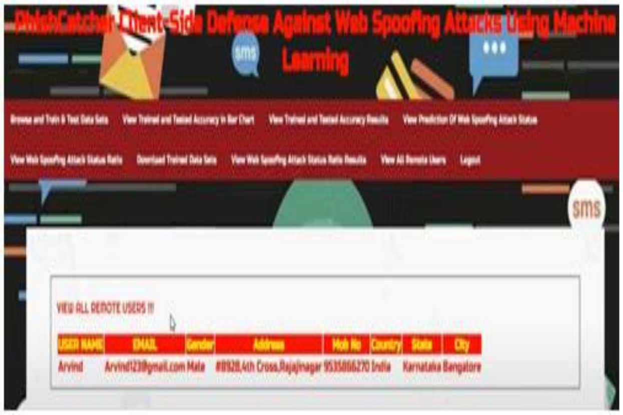


User page

ISSN 2319-5991 www.ijerst.com

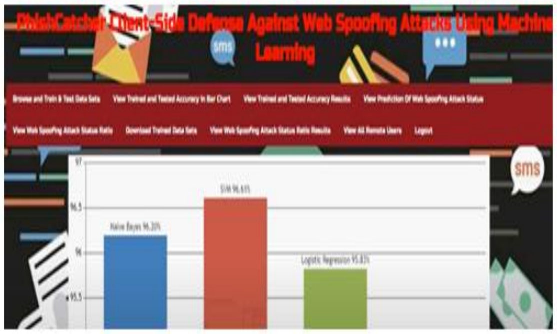
https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

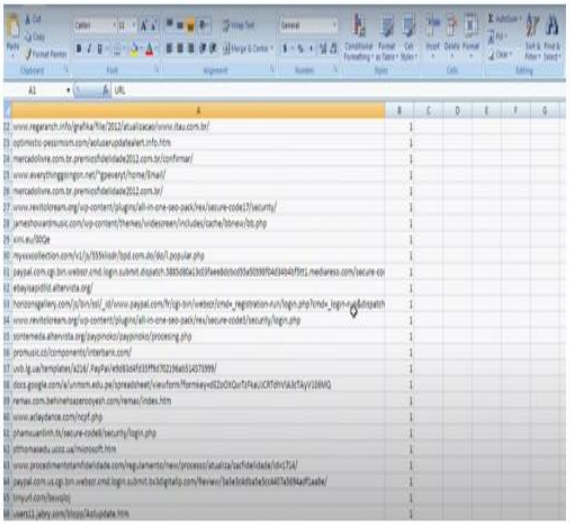

PhishCatcher Client-Side Defense Against Web Spoofing Attacks Using Machine Learning
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Web Spoofing Attack Status
View Web Spoofing Attack Status Ratio
Download Trained Data Sets
View Web Spoofing Attack Status Ratio Results
View All Remote Users
Logout
sms

VIEW ALL REMOTE USERS !!!

USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Arvind	Arvind123@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore

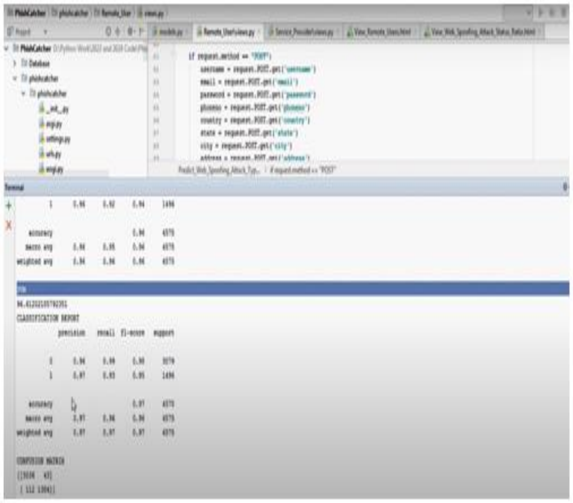


Dataset values



A1 URL

	A	B	C	D	E	F	G
22	www.regaranch.info/grafika/file/2012/atualizacao/www.itau.com.br/	1					
23	optimistic-pessimism.com/aoluserupdatealert.info.htm	1					
24	mercadolivre.com.br.premiosfidelidade2012.com.br/confirmar/	1					
25	www.everythinggoingon.net/~gpeveryt/home/Email/	1					
26	mercadolivre.com.br.premiosfidelidade2012.com.br/	1					
27	www.revitolcream.org/wp-content/plugins/all-in-one-seo-pack/rex/secure-code17/security/	1					
28	jameshowardmusic.com/wp-content/themes/widescreen/includes/cache/bbnew/bb.php	1					
29	xini.eu/00Qe	1					
30	myxxxcollection.com/v1/js/555klindr/bpd.com.do/do/l.popular.php	1					
31	paypal.com.cgi.bin.webscr.cmd.login.submit.dispatch.5885d80a13c03faee8dcbcd55a50598f04d34b4bf5tt1.mediareso.com/secure-co	1					
32	ebayisapidlld.altervista.org/	1					
33	horizonsgallery.com/js/bin/ssl/_id/www.paypal.com/fr/cgi-bin/webscr/cmd=_registration-run/login.php?cmd=_login-run&dispatch	1					
34	www.revitolcream.org/wp-content/plugins/all-in-one-seo-pack/rex/secure-code5/security/login.php	1					
35	sontemeda.altervista.org/paypinoko/paypinoko/procesing.php	1					
36	promusic.co/components/interbank.com/	1					
37	uvb.lg.ua/templates/a216/.PayPal/e9d93d4fd35ff9d702196a6514573999/	1					
38	docs.google.com/a/unmsm.edu.pe/spreadsheet/viewform?formkey=dEZoOXQxrTzFkaUJCRTdhVlA3cTAyV1E6MQ	1					
39	remax.com.behinehsazeroyesh.com/remax/index.htm	1					
40	www.aclaydance.com/ncpf.php	1					
41	phamsuanlinh.tk/secure-code6/security/login.php	1					
42	stthomasedu.ucoz.ua/microsoft.htm	1					
43	www.procedimentotamfidelidade.com/regulamento/new/processo/atualiza/sacfidelidade/id=1714/	1					
44	paypal.com.us.cgi.bin.webscr.cmd.login.submit.tx3digitallp.com/Review/3a5e3c4d0a5e5cc4407a5694adf1aabe/	1					
45	tinyurl.com/bwvqlxj	1					
46	users11.jabry.com/bloqss/Aolupdate.htm	1					



```
if request.method == "POST":
    username = request.POST.get('username')
    email = request.POST.get('email')
    password = request.POST.get('password')
    phoneno = request.POST.get('phoneno')
    country = request.POST.get('country')
    state = request.POST.get('state')
    city = request.POST.get('city')
    address = request.POST.get('address')
```

```
           1       0.96      0.92      0.94      1496

    accuracy                           0.96      4675
   macro avg       0.96      0.95      0.96      4675
weighted avg       0.96      0.96      0.96      4675

SVM
96.61231015792351
CLASSIFICATION REPORT
              precision    recall  f1-score   support

           0       0.96      0.99      0.98      3179
           1       0.97      0.93      0.95      1496

    accuracy                           0.97      4675
   macro avg       0.97      0.96      0.96      4675
weighted avg       0.97      0.97      0.97      4675

CONFUSION MATRIX
[[3136   43]
 [ 112 1384]]
```

CONCLUSION

Analysts have the difficult but critical responsibility of staying abreast of the ever-changing cyber security industry, where new vulnerabilities and threats emerge at any moment. A novel danger may provide an unconventional method to circumvent the defences, necessitating a prompt reaction, even after implementing the best controls and adopting the best practices. In this approach, a comprehensive cyber security system relies heavily on up-to-date information on new cyber risks.

Based on the natural language analysis of Twitter tweets, this study suggests an automated system for identifying and classifying cyber threats. Timely extraction of useful information about emerging dangers requires cooperation with the laborious process of monitoring Twitter, a rich source of information.

What sets this piece apart from others is that it does more than just identify the problem. By comparing the language used in tweets with the actions taken by actual threats documented in the MITRE ATT&CK database, it hopes to determine the threat's objectives. The cyber security community is working to automatically characterise cyber threats based on their intentions, and one method to make the most of this effort is to train machine learning algorithms using this developing and collaborative knowledge base.

We conducted a research experiment and then put our strategy to the test by running the suggested pipeline for 70 days to generate online warnings for the Threat Intelligence Team of a major Brazilian financial institution. During this time, the team took precautions in response to at least three dangers, including the Petit Potam instance (discussed in Section V). Our system notified the team about Petit-Potam seventeen days before to Microsoft's official patch release. During this time, the defence team put measures in place to prevent exploits and, by extension, mishaps.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

Based on our experimental results, the profiling stage achieved an F1 score of 77% when it came to accurately identifying threats from 14 distinct strategies, with a false alarm ratio of 15%. We believe it is critical to make progress in the profiles stage to achieve greater accuracy in identifying the method linked with the detected threat, as well as in the tweets selection phases (Unknown Words and One-class) to improve the false positive rate. Here, we're trying out a new natural language processing strategy by modifying the Spacy29 Python library's part-of-speech (POS) algorithm implementation. The goal is to find tweets where the activity described (the root verb) is referring to the unknown term (the subject), and then figure out which sentences include that word (the object).

REFERENCES

1. W. Khan, A. Ahmad, A. Qamar, M. Kamran, and M. Altaf, ‘‘SpoofCatch: A client-side protection tool against phishing attacks,’’ IT Prof., vol. 23, no. 2, pp. 65–74, Mar. 2021.
2. B. Schneier, ‘‘Two-factor authentication: Too little, too late,’’ Commun. ACM, vol. 48, no. 4, p. 136, Apr. 2005.
3. S. Garera, N. Provos, M. Chew, and A. D. Rubin, ‘‘A framework for detection and measurement of phishing attacks,’’ in Proc. ACM Workshop Recurring malcode, Nov. 2007, pp. 1–8.
4. R. Oppliger and S. Gajek, ‘‘Effective protection against phishing and web spoofing,’’ in Proc. IFIP Int. Conf. Commun.Multimedia Secur. Cham, Switzerland: Springer, 2005, pp. 32–41.
5. T. Pietraszek and C. V. Berghe, ‘‘Defending against injection attacks through context-sensitive string evaluation,’’ in Proc. Int. Workshop Recent Adv. Intrusion Detection. Cham, Switzerland: Springer, 2005, pp. 124–145.
6. M. Johns, B. Braun, M. Schrank, and J. Posegga, ‘‘Reliable protection against session fixation attacks,’’ in Proc. ACM Symp. Appl. Comput., 2011, pp. 1531–1537.
7. M. Bugliesi, S. Calzavara, R. Focardi, andW. Khan, ‘‘Automatic and robust client-side protection for cookie-based sessions,’’ in Proc. Int. Symp.Eng. Secure Softw. Syst. Cham, Switzerland: Springer, 2014, pp. 161–178.
8. A. Herzberg and A. Gbara, ‘‘Protecting (even naıve) web users from spoofing and phishing attacks,’’ Cryptol.ePrint Arch., Dept. Comput. Sci. Eng., Univ. Connecticut, Storrs, CT, USA, Tech. Rep. 2004/155, 2004.
9. N. Chou, R. Ledesma, Y. Teraguchi, and J. Mitchell, ‘‘Client-side defense against web-based identity theft,’’ in Proc. NDSS, 2004, 1–16.
10. B. Hämmerli and R. Sommer, Detection of Intrusions and Malware, and Vulnerability Assessment: 4th International Conference, DIMVA 2007 Lucerne, Switzerland, July 12-13, 2007 Proceedings, vol. 4579. Cham, Switzerland: Springer, 2007.
11. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay,” Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes”, International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023
12. Md. Zainlabuddin, "Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction”, Journal of Sensor, Volume2023.
13. Md. Zainlabuddin, "Security Enhancement in Data Propagation for Wireless Network”, Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).
14. Dr MD Zainlabuddin, "CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS”, Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)
15. Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies”, Industrial Engineering

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022

16. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
17. Ijteba Sultana, Mohd Abdul Bari and Sanjay," Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021
18. M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," A Comparative Study and Performance Analysis of Routing Algorithms", in 3rd International Conference ICCIDM, Springer - 978- 981-10-3874-7_3 Dec (2016)
19. Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017
20. Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022
21. Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7
22. Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
23. Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
24. Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
25. Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.
26. Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.
27. Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017
28. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering", JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;
29. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
30. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.5281/zenodo.11517825

Vol. 17, Issue 2, 2024

Engineering (Toronto) Elsevier SCI Oct : 021

31. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
32. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
33. .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011
34. Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253
35. Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)

36. Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)
37. Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486
38. Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016

39. Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)
40. Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)