Efficient Enumeration of URLs of Active Hidden Servers over Anonymous Channel

S.Cherishma sree[1], B.Chandu Ajay [2], P.Ram Vishal[3], Ch.Vasavi[4]

[1,2,3] UG Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.
[4]Associate Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.

Abstract. This project presents an innovative approach to the efficient enumeration of hidden service URLs (.onion) on the TOR network using a custom-built graphical user interface (GUI) application. The tool leverages web scraping techniques, targeting the Ahmia search engine, to retrieve and analyze active hidden server URLs. Through the integration of Python's Tkinter library for GUI development and the use of requests and regular expressions for content mining, the application simplifies the process of discovering and visualizing .onion URLs. The tool allows users to input search queries, clean them for web compatibility, and display the results in real time. Additionally, the application provides graphical insights into the search results by generating visual data representations using matplotlib. This paper discusses the architecture, development process, and functionality of the tool, providing a new method for researchers to explore the TOR network.

Keywords: TOR network, onion URLs, hidden services, web scraping, Ahmia search engine, Tkinter, data visualization, network security, anonymous browsing

INTRODUCTION

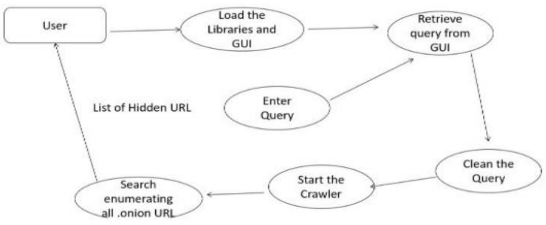
The TOR (The Onion Router) network is known for allowing anonymous communication and hosting hidden services, which can only be accessed through Onion URLs. These hidden services play an important role in protecting privacy, but they also present unique challenges for researchers, especially in the field of cybersecurity. Finding and listing these hidden services is crucial for understanding how the TOR network operates, but traditional search engines can't index .onion sites, making this process more difficult.

Ahmia is a search engine that focuses on indexing .onion websites, but manually searching through it can be time-consuming. This project aims to make that process easier by creating a simple graphical user interface (GUI) application that automatically searches for hidden service URLs. Using Python and web scraping techniques, the application interacts with Ahmia's search engine to retrieve results based on user input. The tool also includes data visualization features that allow users to see the results of their searches in a graph.

This project provides a straightforward way for researchers and cybersecurity professionals to explore the TOR network more efficiently, helping them discover active hidden services without the hassle of manual searching.

RESEARCH METHODOLOGY

The main focus of this project was to create a simple GUI-based application that can automatically find .onion URLs (hidden services) on the TOR network. The process involved several key steps: understanding the requirements, building the application, scraping the web for data, and visualizing the results.



1. **Understanding Requirements:** The first step was to identify the need for this project. Researchers and cybersecurity professionals often need a more efficient way to find .onion URLs, which led to the idea of developing a tool that could automate this process. The Ahmia search engine, which is specifically designed for searching .onion sites, was chosen as the best platform to scrape data from.
2. **Building the Application:** The application was built using Python's Tkinter library to create a simple and easy-to-use graphical interface. The interface includes:
    - An input field for users to type their search queries.
    - Buttons for cleaning the query, starting the search, generating graphs, and closing the app.
    - A text area that displays the results (the .onion URLs) after a search is completed.

    The idea was to keep the design straightforward so that anyone, regardless of technical background, could use it without difficulty.
3. **Scraping the Web:** The core of the project involved web scraping, where I used the requests library to send search queries to the Ahmia search engine. I added a User-Agent header to make the request look like it was coming from a web browser, which helped prevent the search engine from blocking the request. After getting the search results, I used regular expressions to extract the .onion URLs from the webpage. These URLs were then displayed in the text area of the app, and any duplicate URLs were removed.
4. **Visualizing the Results:** To make the results more meaningful, I added a feature that shows the number of .onion URLs found for each query in a bar graph. This was done using the matplotlib library. The graph helps users see how effective their search queries were at finding hidden TOR services, making it easier to compare results from different searches.
5. **Testing the Tool:** Once the application was built, I tested it with a variety of search queries to ensure it worked as expected. This included checking if the tool could properly find and display .onion URLs, handle any errors when a request failed, and create accurate graphs from the data.

Results and Discussion

After developing the application, I ran several tests to check how well it could find .onion URLs on the TOR network. I tried different search queries to see how effective the tool was, and the results gave some useful insights.

Search Results: The application worked as expected, successfully retrieving .onion URLs for every query I entered. In most cases, it was able to find multiple hidden service URLs from the Ahmia search engine and display them in the app. For example, when I used a query like "cybersecurity," the tool returned several active .onion sites related to that topic. Each search produced a unique list of URLs, which was also stored for later use in generating graphs.

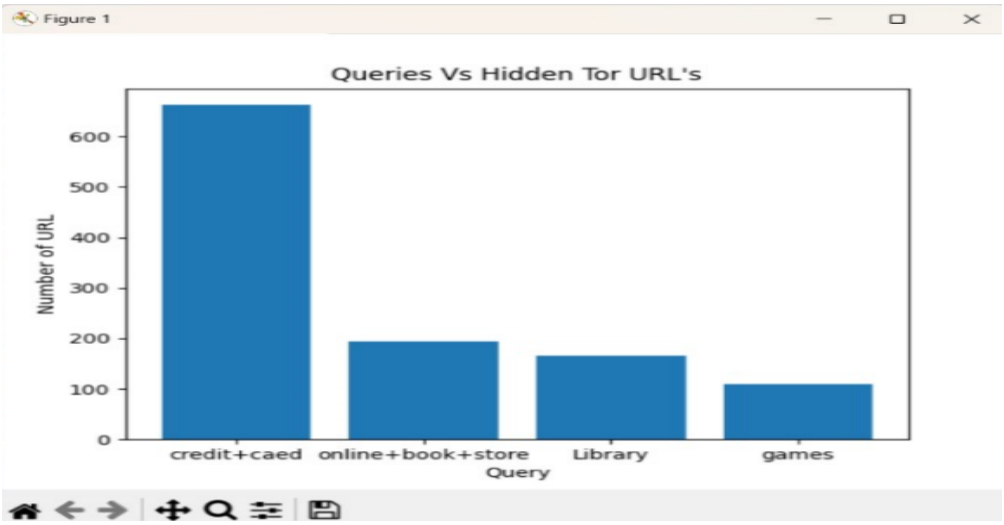
Graph Results: The graph feature turned out to be quite helpful in visualizing the search results. For every query, the tool created a bar graph that showed the number of .onion URLs found. This made it easy to compare how different search queries performed. For instance, more general queries like "marketplace" or "forum" brought back a larger number of URLs, while more specific queries such as "privacy tools" resulted in fewer. The graph provided a quick way to see which search terms were more effective at discovering hidden services.

Ease of Use: One of the goals of this project was to make the tool easy to use, and the tests confirmed that it achieved this. The simple design of the interface, combined with automatic search and graph creation, made it user-friendly even for people without a technical background. Users didn't need to manually visit websites or look through raw HTML, which saved a lot of time and effort when searching for hidden services on the TOR network.

Challenges and Limitations: While the tool worked well, there were a few challenges. The main issue is that the success of web scraping depends on the structure of the Ahmia website. If Ahmia changes how it displays search results, the tool may not be able to extract URLs properly. Some queries also returned fewer results because of the limited number of hidden services in certain categories. Additionally, since the tool relies on internet requests, occasional network issues or request failures could happen.

Future Improvements: There are a few ways the tool could be improved. One idea is to expand the search capability to include other TOR search engines beyond Ahmia, which could help find even more .onion

URLs. Another improvement would be to make the tool more robust against errors, so it can handle failed requests or changes in the website's structure better.



CONCLUSIONS

This project successfully created a simple and efficient tool for finding hidden service URLs on the TOR network. By using web scraping and a user-friendly interface, the tool allows users to easily search for .onion URLs through the Ahmia search engine. The ability to generate graphs also makes it easier to compare the effectiveness of different search queries.

Though the tool performs well, there are still some challenges, like its dependence on the structure of the Ahmia website and potential network issues. However, these can be addressed in future versions by adding support for more TOR search engines and improving how the tool handles errors.

In summary, this tool provides a practical solution for anyone looking to explore the TOR network, especially researchers and cybersecurity professionals. It cuts down on the time and effort needed for manual searches and makes the process of discovering hidden services more straightforward.

DECLARATIONS

Study Limitations

This tool has a few limitations that affect its performance. It relies entirely on the Ahmia search engine, so any changes to Ahmia's structure or availability could disrupt the tool's functionality. Additionally, the tool's search results are limited to what Ahmia indexes, meaning it might miss other active .onion sites. It also depends on a stable internet connection and successful web requests, which can be unreliable. The effectiveness of the tool is also influenced by the specificity of the search queries, with more specific queries returning fewer results. Finally, users must consider the legal and ethical aspects of web scraping and working with anonymous networks like TOR.

ACKNOWLEDGEMENTS

We would like to extend our heartfelt thanks to everyone who supported us throughout the development of this project. Our sincere gratitude goes to our mentors and advisors, whose valuable guidance and constructive feedback were crucial in helping us overcome challenges and refine our approach. We are also grateful to the open-source communities, particularly Ahmia, for providing the resources that made this project possible. Their contributions to web security and the TOR network were integral to the success of our work. Lastly, we would like to thank our friends, families, and teammates for their constant encouragement, collaboration, and support during this journey.

Funding Source

This project was developed independently and did not receive any external funding.

Competing Interests

We confirm that there are no competing interests involved in this project. The work was done purely for academic and research purposes, and there were no financial, personal, or professional factors that influenced the results or conclusions.

HUMAN AND ANIMAL RELATED STUDY

Ethical Approval

This project did not require formal ethical approval since it does not involve human or animal subjects. However, we acknowledge the importance of ethical considerations, especially regarding privacy and anonymity on the TOR network. The tool is intended for educational and research purposes, aimed at assisting cybersecurity professionals. We are committed to ensuring responsible use of the tool, emphasizing the need to respect the rights and anonymity of individuals using the TOR network for legitimate reasons.

Informed Consent

This project did not require formal ethical approval since it does not involve human or animal subjects. However, we acknowledge the importance of ethical considerations, especially regarding privacy and anonymity on the TOR network. The tool is intended for educational and research purposes, aimed at assisting cybersecurity professionals. We are committed to ensuring responsible use of the tool, emphasizing the need to respect the rights and anonymity of individuals using the TOR network for legitimate reasons.

REFERENCES

1. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
2. Ramakrishna, C., Kumar, G. S., & Reddy, P. C. S. (2021). Quadruple band-notched compact monopole UWB antenna for wireless applications. *Journal of Electromagnetic Engineering and Science*, *21*(5), 406-416.
3. Rasineni, G. K., Guha, A., & Reddy, A. R. (2013). Elevated CO2 atmosphere significantly increased photosynthesis and productivity in a fast growing tree species, Gmelina arborea Roxb. *Climate Change and Environmental Sustainability*, *1*(1), 81-94.
4. Ramaiah, M., Chithanuru, V., Padma, A., & Ravi, V. (2022). A review of security vulnerabilities in industry 4.0 application and the possible solutions using blockchain. *Cyber Security Applications for Industry 4.0*, 63-95.
5. Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. *Concurrency and Computation: Practice and Experience*, *35*(22), e7724.

6. Padma, A., Chithanuru, V., Uppamma, P., & VishnuKumar, R. (2024). Exploring Explainable AI in Healthcare: Challenges and Future Directions. In *Analyzing Explainable AI in Healthcare and the Pharmaceutical Industry* (pp. 199-233). IGI Global.
7. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
8. Tahseen, A., Shailaja, S. R., & Ashwini, Y. (2023, December). Security-Aware Information Classification Using Attributes Extraction for Big Data Cyber Security Analytics. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 365-373). Singapore: Springer Nature Singapore.
9. Tahseen, A., Shailaja, S. R., & Ashwini, Y. Extraction for Big Data Cyber Security Analytics. *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2023*, *993*, 365.
10. Murthy, G. V. L. N., Kavya, K. S., Krishna, A. V., & Ganesh, B. (2016). Chemical stabilization of sub-grade soil with gypsum and NaCl. *International Journal of Advances in Engineering & Technology*, *9*(5), 569.
11. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2014). Voltage stability analysis of radial distribution networks with distributed generation. *International Journal on Electrical Engineering and Informatics*, *6*(1), 195.
12. Murthy, G. V. K., Sivanagaraju, S. S., & Rao, B. H. (2012). Artificial bee colony algorithm for distribution feeder reconfiguration with distributed generation. *International Journal of Engineering Sciences & Emerging Technologies*, *3*(2), 50-59.
13. Mallikarjunaswamy, M. C., & Murthy, G. V. K. (1997). Antibiogram of bacterial pathogens isolated from bovine subclinical mastitis cases.
14. Banerjee, D. C., Krishna, K. V. G., Murthy, G. V. G. K., Srivastava, S. K., & Sinha, R. P. (1994). Occurrence of Spodumene in the Rare Metal-Bearing Pegmatites of Mariagalla-Allapatna Area, Mandya Dist., Karnataka. *Journal Geological Society of India*, *44*(2), 127-139.
15. Murthy, G., and R. Shankar. "Composite Fermions." (1998): 254-306.
16. Mahalakshmi, A., Goud, N. S., & Murthy, G. V. (2018). A survey on phishing and it's detection techniques based on support vector method (Svm) and software defined networking (sdn). *International Journal of Engineering and Advanced Technology*, *8*(2), 498-503.
17. Murthy, G., & Shankar, R. (2002). Semiconductors II-Surfaces, interfaces, microstructures, and related topics-Hamiltonian theory of the fractional quantum Hall effect: Effect of Landau level mixing. *Physical Review-Section B-Condensed Matter*, *65*(24), 245309-245309.
18. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2014). Optimal placement of DG in distribution system to mitigate power quality disturbances. *International Journal of Electrical and Computer Engineering*, *7*(2), 266-271.
19. Muraleedharan, K., Raghavan, R., Murthy, G. V. K., Murthy, V. S. S., Swamy, K. G., & Prasanna, T. (1989). An investigation on the outbreaks of pox in buffaloes in Karnataka.
20. Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., & Biamba, C. (2022). Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring. *Sensors*, *22*(3), 1076.
21. Edeh, M. O., Dalal, S., Obagbuwa, I. C., Prasad, B. S., Ninoria, S. Z., Wajid, M. A., & Adesina, A. O. (2022). Bootstrapping random forest and CHAID for prediction of white spot disease among shrimp farmers. *Scientific Reports*, *12*(1), 20876.
22. Onyema, E. M., Balasubaramanian, S., Iwendi, C., Prasad, B. S., & Edeh, C. D. (2023). Remote monitoring system using slow-fast deep convolution neural network model for identifying anti-social activities in surveillance applications. *Measurement: Sensors*, *27*, 100718.
23. Imoize, A. L., Islam, S. M., Poongodi, T., Kumar, R. L., & Prasad, B. S. (Eds.). (2023). *Unmanned Aerial Vehicle Cellular Communications*. Springer International Publishing.
24. Syed, S. A., & Prasad, B. V. V. S. (2019, April). Merged technique to prevent SYBIL Attacks in VANETs. In *2019 International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). IEEE.
25. Prasad, B. V. V. S., & Angel, S. (2014). Predicting future resource requirement for efficient resource management in cloud. *International Journal of Computer Applications*, *101*(15), 19-23.
26. Prasad, B. S., Gupta, S., Borah, N., Dineshkumar, R., Lautre, H. K., & Mouleswararao, B. (2023). Predicting diabetes with multivariate analysis an innovative KNN-based classifier approach. *Preventive Medicine*, *174*, 107619.
27. Khan, F., Siva Prasad, B. V. V., Syed, S. A., Ashraf, I., & Ramasamy, L. K. (2022). An efficient, ensemble-based classification framework for big medical data. *Big Data*, *10*(2), 151-160.

28. Ali, S. S., & Prasad, B. V. V. S. (2017). Secure and energy aware routing protocol (SEARP) based on trust-factor in Mobile Ad-Hoc networks. *Journal of Statistics and Management Systems*, *20*(4), 543-551.
29. Narayana, M. S., Prasad, B. V. V. S., Srividhya, A., & Reddy, K. P. R. (2011). Data mining machine learning techniques–A study on abnormal anomaly detection system. *International Journal of Computer Science and Telecommunications*, *2*(6).
30. Balram, G., & Kumar, K. K. (2022). Crop field monitoring and disease detection of plants in smart agriculture using internet of things. *International Journal of Advanced Computer Science and Applications*, *13*(7).
31. Balram, G., & Kumar, K. K. (2018). Smart farming: Disease detection in crops. *Int. J. Eng. Technol*, *7*(2.7), 33-36.
32. Balram, G., Rani, G. R., Mansour, S. Y., & Jafar, A. M. (2001). Medical management of otitis media with effusion. *Kuwait Medical Journal*, *33*(4), 317-319.
33. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
34. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
35. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
36. Prasad, P. S., & Rao, S. K. M. (2017). A Survey on Performance Analysis of ManetsUnder Security Attacks. *network*, *6*(7).
37. Keshamma, E., Rohini, S., Sankara Rao, K., Madhusudhan, B., & Udaya Kumar, M. (2008). Tissue culture-independent in planta transformation strategy: an Agrobacterium tumefaciens-mediated gene transfer method to overcome recalcitrance in cotton (Gossypium hirsutum L.). *Journal of cotton science*, *12*(3), 264-272.
38. Sundaresha, S., Manoj Kumar, A., Rohini, S., Math, S. A., Keshamma, E., Chandrashekar, S. C., & Udayakumar, M. (2010). Enhanced protection against two major fungal pathogens of groundnut, Cercospora arachidicola and Aspergillus flavus in transgenic groundnut over-expressing a tobacco β 1–3 glucanase. *European journal of plant pathology*, *126*, 497-508.
39. Keshamma, E., Sreevathsa, R., Manoj Kumar, A., Kumar, A., Kumar, A. R. V., Madhusudhan, B., & Udaya Kumar, M. (2008). A chimeric cry1X gene imparts resistance to Spodoptera litura (Fabricus) and Helicoverpa armigera (Hubner) in transgenic groundnut. *Eur J Biosci*, *2*, 53-65.
40. Keshamma, E., Rohini, S., Rao, K. S., Madhusudhan, B., & Kumar, M. U. (2008). Molecular biology and physiology tissue culture-independent In Planta transformation strategy: an Agrobacterium tumefaciens-mediated gene transfer method to overcome recalcitrance in cotton (Gossypium hirsutum L.). *J Cotton Sci*, *12*, 264-272.
41. Nelson, V. K., Nuli, M. V., Ausali, S., Gupta, S., Sanga, V., Mishra, R., ... & Jha, N. K. (2024). Dietary Anti-inflammatory and Anti-bacterial medicinal Plants and its compounds in Bovine mastitis associated impact on human life: A Comprehensive Review. *Microbial Pathogenesis*, 106687.
42. Chary, S. S., Bhikshapathi, D. V. R. N., Vamsi, N. M., & Kumar, J. P. (2024). Optimizing Entrectinib Nanosuspension: Quality by Design for Enhanced Oral Bioavailability and Minimized Fast-Fed Variability. *BioNanoScience*, 1-19.
43. Kumar, J. P., Ismail, Y., Reddy, K. T. K., Panigrahy, U. P., Shanmugasundaram, P., & Babu, M. K. (2022). PACLITAXEL NANOSPONGES'FORMULA AND IN VITRO EVALUATION. *Journal of Pharmaceutical Negative Results*, 2733-2740.
44. NULI, M., KUMAR, J. P., KORNI, R., & PUTTA, S. (2024). Cadmium Toxicity: Unveiling the Threat to Human Health. *Indian Journal of Pharmaceutical Sciences*, *86*(5).
45. Mohammed, M. A., Fatma, G., Akhila, K. P., & Sarwar, S. DISCUSSION ON THE ROLE OF VIDEO GAMES IN CHILDHOOD STUDYING.
46. Labhane, S., Akhila, K. P., Rane, A. M., Siddiqui, S., Mirshad Rahman, T. M., & Srinivasan, K. (2023). Online Teaching at Its Best: Merging Instructions Design with Teaching and Learning Research; An Overview. *Journal of Informatics Education and Research*, *3*(2).
47. KP, A., & John, J. (2021). The Impact Of COVID-19 On Children And Adolescents: An Indianperspectives And Reminiscent Model. *Int. J. of Aquatic Science*, *12*(2), 472-482.
48. John, J., & Akhila, K. P. (2019). Deprivation of Social Justice among Sexually Abused Girls: A Background Study.

49. Sheta, S. V. (2022). A Comprehensive Analysis of Real-Time Data Processing Architectures for High-Throughput Applications. *International Journal of Computer Engineering and Technology*, *13*(2), 175-184.
50. Sheta, S. V. (2022). A study on blockchain interoperability protocols for multi-cloud ecosystems. *International Journal of Information Technology and Electrical Engineering (IJITEE)-UGC Care List Group-I*, *11*(1), 1-11.
51. Khadse, S. P., & Ingle, S. D. (2011, February). Hydrogeological framework and estimation of aquifer hydraulic parameters using geoelectrical data in the Bhuleshwari river basin, Amravati District, Maharashtra. In *National Conference on Geology and Mineral Resources of India, Aurangabad* (pp. 11-12).
52. Ingle, S. D. Monitoring and Modeling Approaches for Evaluating Managed Aquifer Recharge (MAR) Performance.
53. Ingle, S. D., & Tohare, S. P. (2022). Geological investigation in the Bhuleshwari River Basin, Amravati District, Maharashtra. *World Journal of Advanced Research and Reviews*, *16*(3), 757-766.
54. Ingle, S. D. Hydrogeological Investingations in the Bhuleshwari River Basin with Emphasis on Groundwater Management Amravati District Maharashtra.
55. Thatikonda, R., Vaddadi, S. A., Arnepalli, P. R. R., & Padthe, A. (2023). Securing biomedical databases based on fuzzy method through blockchain technology. *Soft Computing*, 1-9.
56. Yendluri, D. K., Ponnala, J., Tatikonda, R., Kempanna, M., Thatikonda, R., & Bhuvanesh, A. (2023, November). Role of RPA & AI in Optimizing Network Field Services. In *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.
57. Vishwakarma, S., Goswami, R. S., Nayudu, P. P., Sekhar, K. R., Arnepalli, P. R. R., Thatikonda, R., & Abdel-Rehim, W. M. (2023). Secure federated learning architecture for fuzzy classifier in healthcare environment. *Soft Computing*, 1-12.
58. Thatikonda, R., Padthe, A., Vaddadi, S. A., & Arnepalli, P. R. R. (2023). Effective Secure Data Agreement Approach-based cloud storage for a healthcare organization. *International Journal of Smart Sensor and Adhoc Network*, *3*(4).
59. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
60. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*(Special Issue).
61. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1190-1198.
62. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3).
63. Rao, P. R., Kumar, K. H., & Reddy, P. R. S. (2012). Query decomposition and data localization issues in cloud computing. *International Journal*, *2*(9).
64. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
65. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
66. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7 S).
67. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, 255.
68. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, *13*(1), 159-168.
69. Latha, S. B., Dastagiraiah, C., Kiran, A., Asif, S., Elangovan, D., & Reddy, P. C. S. (2023, August). An Adaptive Machine Learning model for Walmart sales prediction. In *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)* (pp. 988-992). IEEE.
70. Dastagiraiah, C., Krishna Reddy, V., & Pandurangarao, K. V. (2018). Dynamic load balancing environment in cloud computing based on VM ware off-loading. In *Data Engineering and Intelligent Computing: Proceedings of IC3T 2016* (pp. 483-492). Springer Singapore.

71. Dastagiraiah, C., Reddy, V. K., & Pandurangarao, K. V. (2016). Evaluation of various VM based load balancing procedures in cloud environment. *International Journal of Engineering and Technology*, *8*(2), 845-851.
72. Rao, K. R., Kumari, M. S., Eklarker, R., Reddy, P. C. S., Muley, K., & Burugari, V. K. (2024, February). An Adaptive Deep Learning Framework for Prediction of Agricultural Yield. In *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.
73. Dastagiraiah, C., & Reddy, V. K. (2022). Novel Machine Learning Methodology In Resource Provisioning For Forecasting Of Workload In Distributed Cloud Environment. *Journal Of Theoretical and Applied Information Technology*, *100*(10).
74. Acharjee, P. B., Kumar, M., Krishna, G., Raminenei, K., Ibrahim, R. K., & Alazzam, M. B. (2023, May). Securing International Law Against Cyber Attacks through Blockchain Integration. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2676-2681). IEEE.
75. Ramineni, K., Reddy, L. K. K., Ramana, T. V., & Rajesh, V. (2023, July). Classification of Skin Cancer Using Integrated Methodology. In *International Conference on Data Science and Applications* (pp. 105-118). Singapore: Springer Nature Singapore.
76. Sravan, K., Gunakar Rao, L., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2023, July). Analyze the Quality of Wine Based on Machine Learning Approach. In *International Conference on Data Science and Applications* (pp. 351-360). Singapore: Springer Nature Singapore.
77. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).
78. Ramineni, K., Harshith Reddy, K., Sai Thrikoteshwara Chary, L., Nikhil, L., & Akanksha, P. (2024, February). Designing an Intelligent Chatbot with Deep Learning: Leveraging FNN Algorithm for Conversational Agents to Improve the Chatbot Performance. In *World Conference on Artificial Intelligence: Advances and Applications* (pp. 143-151). Singapore: Springer Nature Singapore.
79. Selvan, M. Arul, and S. Miruna Joe Amali. "RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE." (2024).
80. Selvan, M. Arul. "Fire Management System For Indutrial Safety Applications." (2023).
81. Selvan, M. A. (2023). A PBL REPORT FOR CONTAINMENT ZONE ALERTING APPLICATION.
82. Selvan, M. A. (2023). CONTAINMENT ZONE ALERTING APPLICATION A PROJECT BASED LEARNING REPORT.
83. Selvan, M. A. (2021). Robust Cyber Attack Detection with Support Vector Machines: Tackling Both Established and Novel Threats.
84. Tambi, Varun Kumar, and Nishan Singh. "A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data."
85. Tambi, V. K., & Singh, N. A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
86. Tambi, V. K., & Singh, N. Evaluation of Web Services using Various Metrics for Mobile Environments and Multimedia Conferences based on SOAP and REST Principles.
87. Tambi, V. K., & Singh, N. Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
88. Tambi, V. K., & Singh, N. A New Framework and Performance Assessment Method for Distributed Deep Neural Network-Based Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
89. Tambi, Varun Kumar, and Nishan Singh. "Creating J2EE Application Development Using a Pattern-based Environment."
90. Tambi, Varun Kumar, and Nishan Singh. "New Applications of Machine Learning and Artificial Intelligence in Cybersecurity Vulnerability Management."
91. Tambi, V. K., & Singh, N. Assessment of Possible REST Web Service Description for Hypermedia-Focused Graph-Based Service Discovery.
92. Tambi, V. K., & Singh, N. Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
93. Tambi, V. K., & Singh, N. Analysing Methods for Classification and Feature Extraction in AI-based Threat Detection.
94. Arora, P., & Bhardwaj, S. Mitigating the Security Issues and Challenges in the Internet of Things (IOT) Framework for Enhanced Security.
95. Arora, P., & Bhardwaj, S. Research on Various Security Techniques for Data Protection in Cloud Computing with Cryptography Structures.

96. Arora, P., & Bhardwaj, S. Examining Cloud Computing Data Confidentiality Techniques to Achieve Higher Security in Cloud Storage.
97. Arora, P., & Bhardwaj, S. Techniques to Implement Security Solutions and Improve Data Integrity and Security in Distributed Cloud Computing.
98. Arora, P., & Bhardwaj, S. Integrating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-based Analysis.
99. Arora, P., & Bhardwaj, S. Using Knowledge Discovery and Data Mining Techniques in Cloud Computing to Advance Security.
100. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. *Methods*, *8*(2).
101. Arora, P., & Bhardwaj, S. A Thorough Examination of Privacy Issues using Self-Service Paradigms in the Cloud Computing Context.
102. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
103. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
104. Khan, A. (2020). Formulation and Evaluation of Flurbiprofen Solid Dispersions using Novel Carriers for Enhancement of Solubility. *Asian Journal of Pharmaceutics (AJP)*, *14*(03).
105. Shaik, R. (2023). Anti-Parkinsonian Effect Of Momordica Dioica On Haloperidol Induced Parkinsonism In Wistar Rats. *Journal of Pharmaceutical Negative Results*, 69-81.
106. Selvan, M. A. (2023). INDUSTRY-SPECIFIC INTELLIGENT FIRE MANAGEMENT SYSTEM.
107. Selvan, M. Arul. "PHISHING CONTENT CLASSIFICATION USING DYNAMIC WEIGHTING AND GENETIC RANKING OPTIMIZATION ALGORITHM." (2024).
108. Selvan, M. Arul. "Innovative Approaches in Cardiovascular Disease Prediction Through Machine Learning Optimization." (2024).
109. FELIX, ARUL SELVAN M. Mr D., and XAVIER DHAS Mr S. KALAIVANAN. "Averting Eavesdrop Intrusion in Industrial Wireless Sensor Networks."
110. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
111. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
112. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*(Special Issue 1).
113. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
114. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
115. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.
116. Amarnadh, V., & Moparthi, N. R. (2024). Range control-based class imbalance and optimized granular elastic net regression feature selection for credit risk assessment. *Knowledge and Information Systems*, 1-30.
117. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
118. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.