International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

PHISHING WEBSITE DETECTION USING MACHINE LEARNING

N.Ramadevi[1], M.Sharmila Devi[2], V.Hemanth[3], A. Jithender Reddy [4], N.Manoj[5], G. Praveen[6], P.Ajay Kumar[7]

[1]Associate Professor, Department of Computer Science and Engineering(Data Science), anthiram Engineering College, Nandyal
[2]Assistant Professor, Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal
3, 4,5,6,7 Department of Computer Science and Engineering,Santhiram Engineering College, Nandyal
E-mail:**ramadevi.cse@srecnandyal.edu.in**

Abstract: Phishing sites represent a serious gamble to web security since they attempt to get private data from naïve guests. Specialists have fostered various strategies to recognize phishing sites in light of this danger. The ongoing framework utilizes AI calculations like Decision Tree, SVM, and Slope Lift, however these techniques produce low exactness. To address this, we have presented a proposed framework that utilizes Irregular Woodland and Outrageous Inclination Lift, which produce higher precision. Enormous datasets of trustworthy and phishing sites might be utilized to prepare AI calculations to find examples and characteristics that separate the two. Hence, these calculations might be utilized to recognize and forestall phishing sites from taking advantage of clients. to perceive sites that are phishing.

1. INTRODUCTION

Distinguishing phishing locales is vital for shielding private information from online assaults. Phishing attacks have formed into complex plots over the long run, utilizing different stratagems to fool clients into unveiling individual data, for example, social designing and fake login screens. These assaults for the most part involve the creation of fake messages, messages, or sites that look real trying to trick individuals into uncovering private data like login passwords or financial balance information.

Phishing sites should be recognized and forestalled to effectively battle phishing attacks. Utilizing AI calculations to examine metadata, content, and different parts of sites to recognize conceivable phishing destinations is one strategy. These calculations can distinguish normal examples and attributes related with such phony stages since they have been prepared on huge datasets containing known phishing sites. Besides, a few AI models utilize continuous information inputs to distinguish and check newly made phishing sites rapidly.

Utilizing notoriety based frameworks, which monitor sites that are known to be risky, is an extra technique for distinguishing phishing destinations. These frameworks utilize various information sources, for example, danger insight takes care of, client reports, and boycotts, to recognize and boycott phishing locales. These standing based calculations are utilized by a great deal of online programs to caution clients when they attempt to visit a known phishing site, lessening the probability that they would succumb to these cheats.

Moreover, by spotting strange or problematic web-based action, social examination strategies are fundamental in the recognizable proof of phishing tricks. These procedures help stop cyberattacks before they compromise touchy information by watching out for client collaborations and site action. Thusly, they can distinguish early admonition marks of conceivable phishing endeavors.

To summarize, one of the main parts of successful network protection measures is the ID and obstructing of phishing sites. By utilizing a mix of notoriety based frameworks, AI calculations, and conduct scientific strategies, individuals and associations might go to proactive lengths to shield themselves from the continually changing risk climate that is introduced by phishing endeavors. Through diligent observing and creative location procedures, the classification of private information might be saved, subsequently lessening the dangers connected to cybercrime.

2. LITERATURE SURVEY

The spread of phishing attacks lately has introduced serious hardships for network safety specialists and analysts all through the globe. Phishing sites are made to seem like real stages fully intent on fooling guests into uncovering private data like ledger data and login passwords. Scientists have taken a gander at various techniques, for example, AI, natural language processing (NLP), and URL investigation, to counter this peril effectively. In this audit of the writing, we look at significant examinations that arrangement with phishing site discovery, underlining the methodologies, systems, and ends that have been accounted for in the exploration writing.

To distinguish phishing sites, Shad and Sharma [1] proposed a progressive AI method. Their exploration focused on utilizing AI calculations to look at site qualities and spot phishing endeavors. Powerful separation among hurtful and certified sites was the objective of the analysts' preparation classifiers and component extraction processes.

To perceive the attributes of phishing sites, Sonmez et al. [2] introduced a characterization framework in view of outrageous learning machines (ELM). They utilized a procedure that involved removing components from phishing sites and ordering them utilizing ELM. To achieve exact and successful phishing recognition, the specialists utilized ELM, which is eminent for its computational productivity.

The utilization of AI and natural language processing (NLP) in phishing assault location was explored by Peng et al. [3]. Their exploration focused on utilizing normal language handling (NLP) to examine text based content — like messages or page message — to detect semantic examples reminiscent of phishing endeavors. The objective of the analysts' blend of NLP and AI was to work on the accuracy of phishing discovery methods.

Karabatak and Mustafa [4] utilized a dense dataset of phishing sites to look at the exhibition of classifiers. Their examination evaluated how well unique AI calculations ordered phishing sites utilizing a determination of qualities. The scientists looked to figure out which classifier performed best to decide the best technique for phishing discovery.

A clever procedure for distinguishing phishing sites utilizing URL investigation was put out by Parekh et al. [5]. Their examination focused on looking at URL examples and design to recognize fake sites from bona fide ones. The specialists needed to make a phishing recognition framework that worked by removing qualities from URLs and utilizing grouping calculations.

Utilizing the sack of bytes strategy, Shima et al. [6] took a gander at the order of URL bitstreams. To distinguish phishing endeavors, their examination focused on looking at URLs' byte-level portrayals. To work on the exactness of phishing recognition frameworks, the scientists utilized the sack of bytes approach, which catches the successive idea of URL information.

A correlation exploration of shallow and profound organizations for malevolent URL location was done by Vazhayil et al. [7]. To recognize phishing sites in view of URL qualities, their exploration differentiated the adequacy of profound learning models with shallow brain organizations. The analysts tried to figure out which network engineering would turn out best for URL-based phishing identification by contrasting the viability of a few plans.

To anticipate phishing sites, highlight choice procedures were concentrated by Fadheel et al. [8]. Their exploration fixated on figuring out which characteristics give the most valuable data to phishing recognition and evaluating how well they work with regards to arrangement. To expand the exactness of phishing discovery frameworks, the scientists prepared classifiers and picked appropriate attributes.

Zhang et al's. [9] idea was to utilize semantic investigation to work on the exhibition of phishing discovery. Their exploration focused on recognizing phishing endeavors by inspecting the semantic substance of online pages. The scientists needed to work on the recognizable proof of complex phishing attacks, thusly they incorporated semantic examination approaches into phishing identification calculations.

A phishing identification strategy in view of the C4.5 choice tree calculation was made by Machado and Gadge [10]. To really sort phishing sites, their review focused on building choice trees using highlights taken from such sites. To make a noticeable and productive phishing identification framework, the specialists utilized choice tree calculations, which offer intelligible classification rules.

All in all, many methodologies, for example, AI, regular language handling, URL examination, and semantic investigation, are concentrated on in the field of phishing site identification study. By using these techniques, analysts desire to make exact and compelling phishing recognition frameworks that can effectively balance evolving cyberthreats. In an undeniably connected advanced world, concentrate on in this field is significant to forestalling complex phishing endeavors and safeguarding clients' delicate information.

3. METHODOLOGY

i) Proposed Work:

The proposed directed AI calculation based phishing site discovery framework tries to address the inadequacies of the ongoing strategies. We utilize directed learning techniques, which don't require named preparing information. This can expand adaptability and cut down on the time and cost of information labeling. since we utilize dynamic URLs from the web. The latest data is provided to the framework through this continuous information. The recommended strategy utilizes calculations like Irregular Woods and Outrageous Angle Supporting, which produce precision that is higher than that of existing methods.

ii) System Architecture:

The dataset, which comprises of a bunch of marked examples with credits taken from both legitimate and phishing sites, is the foundation of the framework engineering for phishing site expectation. The preparation period of AI calculations utilizes this dataset to recognize patterns that highlight phishing action. In view of the elements provided, the calculations are prepared to separate among true and fake sites. The prepared model is then put through testing to survey how well it functions and ensure it can perceive phishing sites with precision. After approval, the model is utilized for continuous expectation, where it predicts the likelihood of phishing movement in light of info information reflecting site ascribes. This engineering assists people and organizations with lessening the dangers related with online extortion and information breaks by empowering the programmed distinguishing proof of phishing sites.

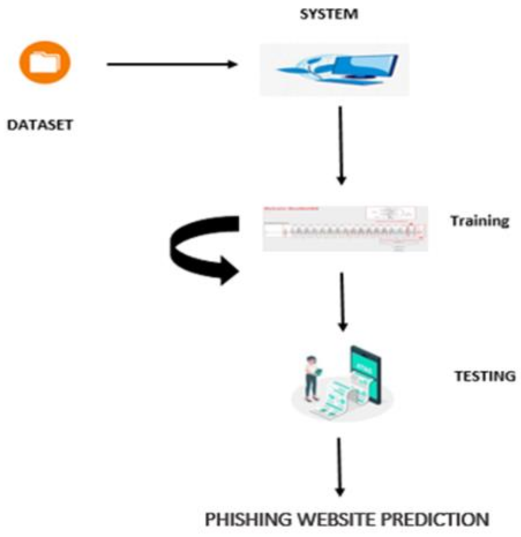


Fig 1 Proposed Architecture

iii) Dataset:

The dataset the executives framework stacks the information into CSV records subsequent to performing tests to guarantee that the information is accessible. This system ensures the dataset's openness and respectability for additional review. The innovation makes information dealing with tasks more straightforward by deliberately checking the presence of information and organizing it into CSV records for successful recovery and alteration. This strategy additionally further develops information consistency and steadfastness, which makes it workable for experts and scientists to go through the dataset top to bottom and concentrate important bits of knowledge. In light of everything, the dataset the executives framework is fundamental for supporting information driven navigation and growing exploration drives across a scope of fields.

iv) Pre-processing:

Pre-handling information is important to increment model exactness and get familiar with the dataset. Cleaning, changing over, and coordinating crude information to set it up for AI model examination is a basic stage simultaneously. The information should be standardized, reliable, and absent any and all irregularities or irregularities. Strategies like component scaling, information normalization, and overseeing missing qualities help in this cycle. Include designing is one more part of pre-handling that might be utilized to further develop the expectation force of the model by choosing or inferring new highlights. Pre-handling upgrades the model's ability to sum up to new information by limiting commotion, diminishing the impact of exceptions, and further developing information planning. Furthermore, it provides scientists with a superior information on the properties, dissemination, and linkages of the information, engaging them to make more taught decisions all through the development and evaluation of models. Taking everything into account, information pre-handling lays out the basis for creating solid and exact AI models that productively use the accessible information to deliver sagacious examinations and estimates.

v) Training & Testing:

A basic move toward pre-handling the dataset is separating it into two subsets: the preparation information and the testing information. This part empowers the model's exhibition on speculative information to be evaluated. The preparation set, which is utilized to prepare the AI calculations, normally contains the main part of the dataset. By gaining examples and relationships from the information, the model turns out to be more prescient thanks to the preparation set of information. Then again, the testing information — which makes up a more modest level of the dataset — is used to assess the model's ability for speculation during the preparation stage. Through the evaluation of the model's presentation on autonomous test information, researchers can decide the model's adequacy and spot any issues like under-or overfitting. The train-test split ensures the legitimacy of the model's exhibition assessments and their appropriateness to new, untested information.

vi) Algorithms:

AdaBoost:

Versatile Helping, or AdaBoost, is a strong gathering learning technique in AI that is generally applied as a characterization approach. By progressively making various powerless students and pooling their forecasts, it looks to bring down predisposition and variety. AdaBoost gives misclassified models from prior students a higher need than ordinary helping draws near, which construct each progressive student independently. Up until a foreordained number of essential students are created, this iterative methodology is proceeded. Curiously, AdaBoost utilizes choice stumps — single hubs with two branches — as frail students. The arrangement of the stumps is significant in light of the fact that the missteps made in the underlying stump influence the creation of the stumps that follow. AdaBoost means to improve the model's presentation by more than once changing the loads of inaccurately distinguished cases; this makes the model particularly fitting for twofold arrangement issues. It is notable for further developing choice trees' precision, especially in circumstances when discrete arrangement errands are involved.

XGBoost:

Outrageous Inclination Supporting, or XGBoost for short, is a disseminated slope helping tool compartment for AI applications that is exceptionally compelling and versatile. It effectively deals with the inclination fluctuation compromise by successively assembling solid classifiers from powerless ones utilizing the helping group learning approach. Helping calculations, like XGBoost, are more effective since they control both predisposition and change, as opposed to packing calculations, which exclusively handle unreasonable difference. As a result of its extraordinary exhibition and versatility, especially while handling organized information, XGBoost has become notable in the AI people group and Kaggle challenges. It settles on slope supported choice trees quicker and more compelling, which makes it a well known choice for different information science applications.

Random Forest:

Utilizing gathering figuring out how to coordinate a few classifiers to tackle troublesome issues, Irregular Backwoods is an AI approach utilized for relapse and grouping applications. It comprises of numerous choice trees that have been prepared by bootstrap total or packing. In light of the joined result of these trees, expectations are framed, much of the time by casting a ballot or averaging. Arbitrary Random Forest decreases overfitting and further develops exactness by consolidating various decision trees, which gets around the downsides of individual trees. Its better precision over choice trees and its capacity to deal with missing information actually are two of its key assets. Appreciating thoughts, for example, entropy and data gain from choice tree hypothesis explains Irregular Woodland's working. As opposed to decision trees, Random Forest utilizes the sacking way to deal with create various subsets of preparing information for each tree, building root and decision trees at arbitrary. Strength and unwavering quality are guaranteed in grouping or relapse errands by utilizing the typical result of all trees or the larger part vote to make the last expectation.

Gradient Boosting:

One famous AI strategy is the angle helping calculation, which is exceptionally valuable for decreasing predisposition botches in models. Slope Helping utilizes a predefined base assessor, typically a Choice Stump, as opposed to AdaBoost, where the base assessor might be tweaked. Despite the fact that it is feasible to change the quantity of assessors, 100 is every now and again utilized as the default setting. Utilizing Mean Squared Error (MSE) for relapse and Log Misfortune for grouping, this method can deal with occupations including both relapse and order. Inclination Supporting is a strategy that further develops precision and diminishes botches by building succeeding assessors on top of the residuals of the earlier ones. The GradientBoostingRegressor would be utilized, for example, in a circumstance where Age is the objective variable and LikesExercising, GotoGym, and DrivesCar are free traits. Each every assessor enhances the residuals of the ones that preceded it, step by step further developing conjectures.

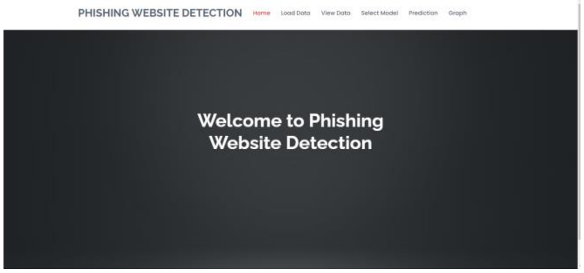
SVM:

To productively separate the data of interest into particular gatherings, the Support Vector Machine

(SVM) technique looks to find a hyperplane in a N-layered space. Hyperplanes are choice limits that assistance with information point arrangement; powerful grouping is guaranteed by boosting the edge. The information focuses closest to the hyperplane, or support vectors, influence the bearing and area of the hyperplane. SVM makes a proficient classifier by utilizing the help vectors to expand the edge. Enormous room for error instinct is utilized in SVM, where expectations are predicated on whether the direct capability's result outperforms explicit limits (like 1 or - 1). Pivot misfortune, an expense capability, punishes misclassifications while aiding edge expansion. Inclination refreshes consider weight adjustments in view of exact or off base expectations by performing fractional subordinates of the misfortune capability concerning the loads. Just the regularization boundary influences slope refreshes without misclassification, while misclassifications bring about refreshes that incorporate both misfortune and regularization terms.

4. EXPERIMENTAL RESULTS

Here user view the home page of phishing website prediction web application.

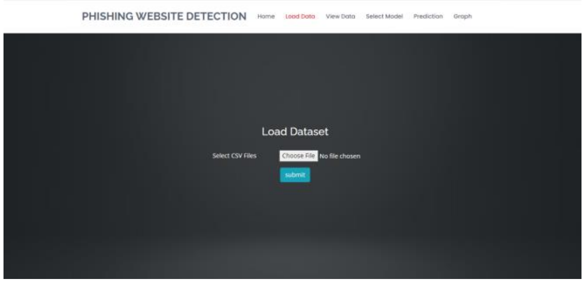


Welcome to Phishing Website Detection

Fig 2 Home Page

Load:

In the load page, users can load the website dataset.



Load Dataset

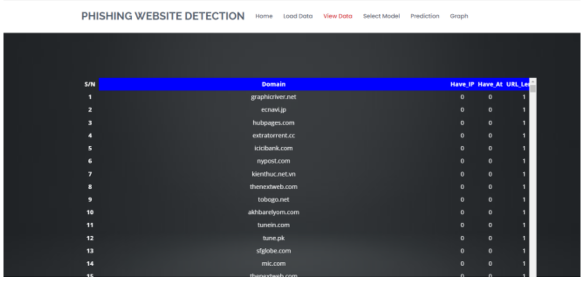
Select CSV Files: Choose File No file chosen

submit

Fig 3 Load Dataset

View:

Here we can see the uploaded data set.

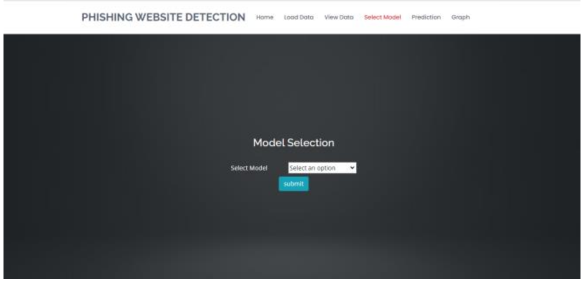


S/N	Domain	Have_IP	Have_At	URL_Le
1	graphicriver.net	0	0	1
2	ecnavi.jp	0	0	1
3	hubpages.com	0	0	1
4	extratorrent.cc	0	0	1
5	icicibank.com	0	0	1
6	nypost.com	0	0	1
7	kienthuc.net.vn	0	0	1
8	thenextweb.com	0	0	1
9	tobogo.net	0	0	1
10	akhbarelyom.com	0	0	1
11	tunein.com	0	0	1
12	tune.pk	0	0	1
13	sfglobe.com	0	0	1
14	mic.com	0	0	1
15	thenextweb.com	0	0	1

Fig 4 View Data

Model:

Here we can train our data using different algorithm.



Model Selection

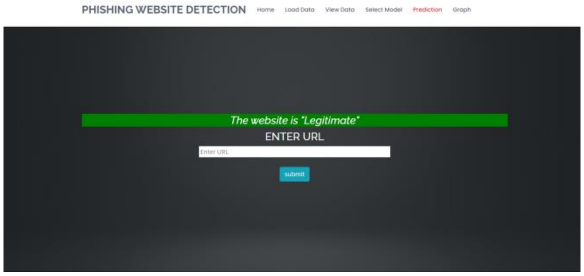
Select Model: Select an option

submit

Fig 5 Model Selection for train our data

Prediction:

This page show the detection result that whether the website is a phishing website or legitimate.



The website is "Legitimate"

Fig 6 Prediction result

5. CONCLUSION

AI based phishing site distinguishing proof is a likely method for countering the rising issue of online misrepresentation. Via preparing calculations to perceive patterns in the way of behaving and highlights of phishing sites, AI can identify and forestall risky sites before they cause damage. As per ongoing exploration, AI calculations are profoundly precise in distinguishing phishing sites. These calculations might evaluate a site's probability of being a phishing site by taking a gander at various qualities, including the substance, UI, and URL structure. It's memorable's significant that AI calculations are not faultless and can sometimes bring about bogus up-sides or misleading negatives. Moreover, as phishing aggressors continually adjust their procedures, AI models additionally should be refreshed and enhanced to stay fruitful. In light of everything, AI based phishing site recognizable proof is a valuable device in the fight against online extortion, however for the best client wellbeing, it ought to be utilized couple with other safety efforts.

6. FUTURE SCOPE

Future advancements in AI based phishing site recognition could consolidate more mind boggling calculations, including profound learning models, to further develop flexibility and exactness. Moreover, adding social scientific techniques and constant information streams could upgrade identification abilities significantly further. Joint efforts between AI specialists and network protection experts could likewise bring about effective fixes for phishing assault risks that are continuously developing. Supporting a lead over creating cyberthreats and ensuring proficient client security later on will require continuous innovative work.

REFERENCES

[1] Mahammad, F. S., &Viswanatham, V. M. (2020). Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach. The Journal of Supercomputing, 76(4), 2275-2288.

[2] Karukula, N. R., & Farooq, S. M. (2013). A route map for detecting Sybil attacks in urban vehicular networks. Journal of Information, Knowledge, and Research in Computer Engineering, 2(2), 540-544.

[3] Farook, S. M., &NageswaraReddy, K. (2015). Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications. Inter national journal of Scientific Engineering and Technology Research, 4(0), 41.

[4] Sunar, M. F., &Viswanatham, V. M. (2018). A fast approach to encrypt and decrypt of video streams for secure channel transmission. *World Review of Science, Technology and Sustainable Development*, *14*(1), 11-28.

[5] Mahammad, F. S., &Viswanatham, V. M. (2017). A study on h. 26x family of video streaming compression techniques. *International Journal of Pure and Applied Mathematics*, *117*(10), 63-66.

[6] Devi,S M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M.,& Swathi, P. V. (2022).”Machine Learning Based Classification and Clustering Analysis ofEfficiency of Exercise Against Covid-19 Infection.” Journal of Algebraic Statistics, 13(3),112-117.

[7] Devi, M. M. S., & Gangadhar, M. Y. (2012).”A comparative Study of Classification Algorithm forPrinted Telugu Character Recognition.” *International Journal of Electronics Communication andComputerEngineering*,*3*(3), 633-641.

[8] Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G., Vineela, G., & Padmavathi, M.MISSINGCHILDIDENTIFICATIONSYSTEMUSINGDEEPLEARNING.

[9] V. Lakshmi chaitanya. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13, no. 2 (2022): 2477-2483.

[10] Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori vs Genetic algorithms for Identifying Frequent Item Sets. International journal of Innovative Research &Development, 3(6), 249-254.

[11] Chaitanya, V. L., Sutraye, N., Praveeena, A. S., Niharika, U. N., Ulfath, P., & Rani, D. P. (2023). Experimental Investigation of Machine Learning Techniques for Predicting Software Quality.

[12] Lakshmi, B. S., Pranavi, S., Jayalakshmi, C., Gayatri, K., Sireesha, M., & Akhila, A. Detecting Android Malware with an Enhanced Genetic Algorithm for Feature Selection and Machine Learning.

[13] Lakshmi, B. S., & Kumar, A. S. (2018). Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity checking in Public Cloud. International Journal of Research, 5(22), 744-757.

[14] Lakshmi, B. S. (2021). Fire detection using Image processing. Asian Journal of Computer Science and Technology, 10(2), 14-19.

[15] Devi, M. S., Poojitha, M., Sucharitha, R., Keerthi, K., Manideepika, P., & Vasudha, C.Extracting and Analyzing Features in Natural Language Processing for Deep Learning withEnglishLanguage.

[16] Kumar JDS, Subramanyam MV, K umar APS. Hybrid Chameleon Search and Remora Optimization Algorithm-based Dynamic Heterogeneous load balancing

clustering protocol for extending the lifetime of wireless sensor networks. Int J Commun Syst. 2023; 36(17):e5609. doi:10.1002/dac.5609

[17] David Sukeerthi Kumar, J., Subramanyam, M.V., Siva Kumar, A.P. (2023). A Hybrid Spotted Hyena and Whale Optimization Algorithm-Based Load-Balanced Clustering Technique in WSNs. In: Mahapatra, R.P., Peddoju, S.K., Roy, S., Parwekar, P. (eds) Proceedings of International Conference on Recent Trends in Computing. Lecture Notes in Networks and Systems, vol 600. Springer, Singapore. https://doi.org/10.1007/978-981-19-8825-7_68

[18] Murali Kanthi, J. David Sukeerthi Kumar, K. Venkateshwara Rao, Mohmad Ahmed Ali, Sudha Pavani K, Nuthanakanti Bhaskar, T. Hitendra Sarma, "A FUSED 3D-2D CONVOLUTION NEURAL NETWORK FOR SPATIAL-SPECTRAL FEATURE LEARNING AND HYPERSPECTRAL IMAGE CLASSIFICATION," J Theor Appl Inf Technol, vol. 15, no. 5, 2024, Accessed: Apr. 03, 2024. [Online]. Available: www.jatit.org

[19] Prediction Of Covid-19 Infection Based on Lifestyle Habits Employing Random Forest Algorithm FS Mahammad, P Bhaskar, A Prudvi, NY Reddy, PJ Reddyjournal of algebraic statistics 13 (3), 40-45

[20] Machine Learning Based Predictive Model for Closed Loop Air Filtering System P Bhaskar, FS Mahammad, AH Kumar, DR Kumar, SMA Khadar, ...Journal of Algebraic Statistics 13 (3), 609-616

[21] Kumar, M. A., Mahammad, F. S., Dhanush, M. N., Rahul, D. P., Sreedhara, K. L., Rabi, B. A., & Reddy, A. K. (2022). Traffic Length Data Based Signal Timing Calculation for Road Traffic Signals Employing Proportionality Machine Learning. Journal of Algebraic Statistics, 13(3), 25-32.

[22] Kumar, M. A., Pullama, K. B., & Reddy, B. S. V. M. (2013). Energy Efficient Routing In Wireless Sensor Networks. International Journal of Emerging Technology and Advanced Engineering, 9(9), 172-176.

[23] Kumar, M. M. A., Sivaraman, G., Charan Sai, P., Dinesh, T., Vivekananda, S. S., Rakesh, G., & Peer, S. D. BUILDING SEARCH ENGINE USING MACHINE LEARNING TECHNIQUES.

[24] " Providing Security in IOT using Watermarking and Partial Encryption. ISSN No:

2250-1797 Issue 1, Volume 2 (December 2011)

[25] The Dissemination Architecture of Streaming Media Information on Integrated CDN andP2P, ISSN 2249-6149 Issue 2, Vol.2 (March-2012)

[26] Provably Secure and Blind sort of Biometric Authentication Protocol using Kerberos,ISSN: 2249-9954, Issue 2, Vol 2 (APRIL 2012)

[27] D.LAKSHMAIAH, DR.M.SUBRAMANYAM, DR.K.SATYA PRASAD," DESIGN OF LOW POWER 4- BIT CMOS BRAUN MULTIPLIER BASED ON THRESHOLD VOLTAGE TECHNIQUES", GLOBAL JOURNAL OF RESEARCH IN ENGINEERING, VOL.14(9),PP.1125-1131,2014.

[28] R SUMALATHA, DR.M.SUBRAMANYAM, "IMAGE DENOISING USING SPATIAL ADAPTIVE MASK FILTER", IEEE INTERNATIONAL CONFERENCE ON ELECTRICAL, ELECTRONICS, SIGNALS, COMMUNICATION &AMP; OPTIMIZATION (EESCO-2015), ORGANIZED BYVIGNANS INSTITUTE OF INFORMATION TECHNOLOGY, VISHAKAPATNAM, 24 TH TO 26TH JANUARY 2015. (SCOPUS INDEXED)

[29] P.BALAMURALI KRISHNA, DR.M.V.SUBRAMANYAM, DR.K.SATYA PRASAD, "HYBRID GENETIC OPTIMIZATION TO MITIGATE STARVATION IN WIRELESS MESH NETWORKS", INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY,VOL.8,NO.23,2015. (SCOPUS INDEXED)

[30] Y.MURALI MOHAN BABU, DR.M.V.SUBRAMANYAM,M.N. GIRI PRASAD," FUSION AND TEXURE BASED CLASSIFICATION OF INDIAN MICROWAVE DATA – A COMPARATIVE STUDY", INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, VOL.10 NO.1, PP. 1003-1009, 2015. (SCOPUS INDEXED)