© MAY 2024 | IRE Journals | Volume 7 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I11-1712451

Logo Image Focused Method for Phishing Detection

K. MANI RAJU[1], GATTU RAMYA[2], NAGAVELLI YOGENDER NATH[3], R. PRASANTH REDDY[4]
[1]*Assistant Professor, Department of Computer Science & Engineering, Malla Reddy Engineering College, Hyderabad.*
[2]*Assistant Professor, Department of Computer Science & Engineering, Vignan Institute of Management and Technology for Women, Hyderabad.*
[3]*Assistant Professor, Department of Computer Science & Engineering (AI&ML), Sumathi Reddy Institute of Technology for Women, Hyderabad.*
[4]*Assistant Professor, Department of Computer Science & Engineering, RSR Engineering College*

Abstract- Phishing is a type of cyberattack in which a phoney website imitates a genuine, authentic website. Because the website gives the impression that it is legitimate, users divulge sensitive information online, including credit card numbers, passwords, PINs, and social security numbers. These websites pose a serious risk to internet users since they contain extremely sensitive information, making their detection and blocking essential. In order to shield internet users from these kinds of attacks, we present a novel phishing detection technique in this thesis. Specifically, our suggested approach may distinguish between a legal website and a phishing website based only on a screenshot of the website's logo. Any hidden logo won't be able to fool the algorithm into thinking the website is phishing, as was the case with previous solutions, because the screenshot is used to extract the logo. The first study concentrated on collecting datasets before extracting the logo image. The URLs linked to this image are returned by an automated script that uploads the logo image to the Google image search engine. It makes sense to treat the logo image as the original URL's identity because the logo and domain name have an exclusive link. As a result, when Google searches for the logo picture, the phishing website will not be retrieved as a URL and will not have the same relationship to the logo image as such. Additionally, the detection accuracy is strengthened by using Alexa page rank.

Index Terms—Anti-phishing; Website logo; Google image search, Image Processing, etc.

I. INTRODUCTION

Phishing is the practice of impersonating a reliable website in order to get private information from internet users, such as credit card details and PINs. We decided to investigate this as APWG data indicate that 40–50% of phishing attacks are based on legitimate websites. To that end, we created a list of target words that includes numerous well-known phishing targets, like PayPal and Ebay [1, 2]. The majority of the time, thieves create websites by either copying authentic content or slightly altering it in order to obtain sensitive user data. For instance, a system may be sufficiently secure in theory to prevent password theft, but if a user clicks on an HTTP link without knowing, their passwords could be compromised, endangering the system's overall security. There are numerous ways to identify phishing attacks, however there isn't yet a foolproof method that can identify every kind of phishing assault. The first thing to consider when determining whether a website is a phishing website is how to distinguish it from a legitimate website, as the two types of websites can have similar appearances. We can determine whether a website is authentic or a phishing site if we know the portrayed identity of the query website. The depicted identity will be the identity of the besieged legitimate website if the website in question is a phishing website [3], allowing us to distinguish between the two. It motivates the proposal of an anti-phishing technique based on the recognition of website identity through the logo because it is known that phishers will employ optical elements, particularly the logo, that are stolen from the legitimate website in their phishing websites. This makes sense because a genuine website's identity is typically represented by its logo.

© MAY 2024 | IRE Journals | Volume 7 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I11-1712451

The website being tested to determine if it is a legitimate website or a phishing website is known as the "query website. "The trademark or organisation that a genuine website highlights is known as the "portrayed identity. "For instance, the domain http://www.ebay.com, where eBay is depicted as the authentic website. The domain http://www.www1-ebaee.com, for instance, is a phishing website that imitates the eBay website, with eBay being the projected identity. Real identity: This is a query website's true identity [4]. As an illustration, consider the domain http://www.ebay.com, where ebay is the actual name of a trustworthy website. Its true identity is www1-ebaee, but the URL http://www.www1-ebaee.com is a phishing website that imitates the eBay website. Phishing can take many different forms, including man-in-the-middle phishing, email phishing, malware-based phishing, keylogger and screenloggers (certain types of malware that capture keyboard input and relay relevant information to hackers via the internet), etc. In recent years, a number of anti-phishing techniques have been created [5].

Phishing is the term used to describe an attempt to get private information, usually in the form of bank account information, credit card numbers, usernames, passwords, or other sensitive data, with the intention of using or selling the information. Similar to how a fisherman uses bait to catch a fish, an attacker deceives the victim by posing as a reliable source and making an alluring request.

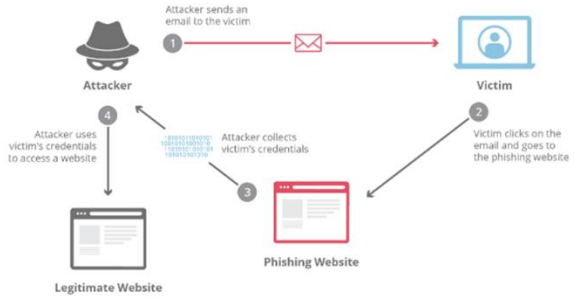

Figure 1: Concept of Phishing [6]

Phishing is most frequently used to facilitate other malevolent activities, like ransomware assaults, account takeovers, and business email compromises. Phishing attacks used to mostly happen through instant messaging or email. Phishing assaults now take place over a range of media, including social media posts, phone calls, and SMS texts.

Attackers might employ a number of strategies to increase the efficacy of their phishing attempts:

- Locating, acquiring, or scraping known contact details
- Establishing phoney apps and websites that mimic the authentic ones
- Disguising their hosting servers with methods like DNS fast fluxing
- Making messages look authentic by using email and domain spoofing
- Link manipulation to make phishing mails appear right
- Emails sent from reliable infrastructure that can evade detection and bypass spam filters
- Using generative AI to produce error-free, realistic-sounding messages fast
- The majority of phishing assaults fall into a few broad categories. Knowing a few of these various phishing attack vectors may help you recognise them when they occur.

II. RELATED WORK

However, there are several distinct methods for detecting phishing attempts. These are as follows:
To determine the identification trustworthiness between a website's genuine and projected identities, J. Hong et al. [7] used a logo image. Incompatible identities indicate a phishing website, while trustworthy identities indicate a genuine website. The two steps in the suggested technique are identity and logo extraction.

Varification: The first step will locate and extract the logo picture from each of a webpage's downloaded image resources. The approach uses a machine learning algorithm to determine the appropriate logo image. The second process will use a Google image search to find the depicted identity based on the removal of a logo image. Treating the domain name as the identity makes sense because of the unique relationship between the logo and domain name. Therefore, if the domain name from the query website differs from the one that Google returned, we can tell

the difference between a phishing and a genuine website. The outcomes of the conducted experiments are consistent and encouraging. This demonstrates the effectiveness and viability of identifying a phishing website using a graphical feature like a logo.

L. Cranor and J. Hong et al. [8] The unmediated heuristic method comprises the majority of the strategies that have been proposed in the literature. CANTINA is one of the widely used techniques. This technique will generate a lexical signature by calculating the TF-IDF from a webpage's content. The method will conduct a web search using the Google search engine using the generated lexical signature. The result that is produced will be utilised to determine a website's authority. Even so, this method can be used logically to detect phishing attempts. Umar, Syed, and associates [9] The primary goal of the technique is to identify the phishing target when a phishing webpage is detected, according to a more current research study on the characteristics-based heuristic approach. The method is based on the creation of a self-organised semantic data model known as the Semantic Link Network, which is commonly employed for web resource organisation. The foundation of this approach is the textual components (i.e., the removal of hyperlinks, keywords, and textual contents for the process of link relations, search relations, and text relations, respectively), even though it employs several detection algorithms.[10] Habeeb, M. S. et al. It is possible to compile a list of authentic URLs. This technique is known as whitelisting and is a form of list-based methodology. The research suggested by the authors created an automated method that keeps and stores a whitelist at the client side, which is an example of a whitelisting methodology. PhishNet is a more active and adaptable list-based method that was proposed by Dikshendra DS et al. [11]. This method processes the current blacklisted URLs and creates several variant URLs using a number of URL variant criteria. An analytical blacklist will be created from the supplied URLs. It can successfully identify both new and old phishing websites, according to the results. Although a list-based method is simple to create and use, maintaining a complete and current list requires a lot of work and constant attention to detail. Usman et al. [12] Blacklisting is suggested as one of the often used strategies. This method is used by several popular web browsers to identify phishing websites. This method involves comparing a query webpage to a list (i.e., a list that is identified as phishing URLs) that has been compiled and maintained by an association or organisation. The website will be classified as phishing if the verification yields a match. According to Naveen et al. [13], PhishZoo is one of the widely used strategies. This study suggests PhishZoo, a phishing detection method that uses the outer shell profiles of trustworthy websites to identify phishing. Its ability to classify zero-day phishing assaults and troubled hits against small websites (like corporate intranets) is a benefit. This research is important since it includes a presenting study and a framework for using computer vision techniques sensibly. In order to identify phishing websites, R. Gnanakumaran et al. [14] suggested a method that considers and uses an intelligent model. Ten distinct forms of information, including headings, keywords, and connecting text, are removed from this model to represent the webpage. These disparate features are then used to generate different classifiers. To combine the anticipated outcomes from various phishing detection classifiers, they suggested an ethical ensemble classification system. For mechanical phishing classification, the hierarchical clustering technique has proven effective. Their suggested methodology beats other widely used anti-phishing techniques and technologies in phishing website detection, as shown by case studies on excellent and real everyday phishing websites created by King Soft Internet Security Naveen et al. [15] suggested a way to evaluate how well three well-known internet resources—Yahoo! Inlink data, Yahoo! directory service, and Google PageRank system—identify phishing websites. Their findings suggest that, when combined with current phishing countermeasures, these internet resources can be leveraged to increase the detection accuracy of phishing sites. Three characteristics of a goal location (place under inspection) are investigated by the suggested loom: (1) The target site's dependabilitypsilas hosting domain, (2) the consistency of nearby websites that link to the hosting domain, and (3) the relationship between the hosting domain's psilas web type and its target site's psilas web category. The web resources listed above are insufficient on their own to focus on the issue of phishing attacks. This method offers guidelines on how to combine each of those resources with current

phishing detection methods to give a more effective solution.In [16], K. Kartheeban et al. suggested a solution for maintaining secrecy in instant messaging (IM) using the Association Rule Mining (ARM) technique, a data mining technique combined with a speech recognition system. FFT spectrum analysis and LPC coefficient techniques are used to identify verbal skills. These days, online criminals use voice chats and text messages in tandem, or both, in instant messaging apps, and stifle personal information, which leads to intimidation and privacy barriers. The Anti Phishing Detection System (APD) in instant messaging (IMs) can be used to help focus attention on privacy preservation in residential settings [17].

The untrustworthy phishing for both audio and text combined. In [18], D Veerendra et al. suggested an anti-phishing technique to shield users from online phishing scams. The identification of phishing websites with English content is the primary subject of this method study. Phishers typically insert brand names in various locations throughout the URL to entice users to visit the website that the website purports to be. By assigning weights to words extracted from the HTML text based on their co-appearance at path, hostname, and file names of URLs, they suppressed this phishing trend. The corresponding TF-IDF weights are then supplemented with these weights. The most probable terms are specific and are entered into Yahoo Search in order to retrieve the domain name with the highest frequency among the top 30 search results. To identify the vendor behind the chosen domain name, a WHOIS lookup is performed. If the owner of the domain name provided by the search engine differs from the vendor of the query domain name, a phishing website can be easily identified.

In [19], Naveen et al. suggested a method for phishing detection that uses an artificially secured system. The technology uses memory detectors and sophisticated detectors to identify phishing emails. The training data set, which successively includes the phishing emails the system has seen up to that point, is used to create the memory detectors. The system's mutation process replicates the immature detectors. To the best of our knowledge, this is the first time a system of this kind has ever been predicted. They believed that compared to existing active phishing detection methods, the system is more adaptable. In [20], Uppu Lokesh et al. presented a single-layer neural network-based effective method for identifying phishing websites. In particular, the suggested method determines the heuristics' value in an unbiased manner. A single-layer neural network then generates the heuristic weights. A dataset of 10,000 authentic websites and 11,660 phishing sites is used to evaluate the suggested method. In [9], Umar et al. suggested a method for taking identification claims on websites into account. This human expert behaviour is replicated by their phishing detection technology. Their approach analyses a website's claimed identity and determines the documentary importance of the relationship between the claimed identity and other descriptions on the page. This textual relevance is then used as one of the classification criteria by their phishing detection system. As a preliminary step, DeBarr et al. [3] suggested using Spectral Clustering to analyse messages according to traffic patterns. Specifically, for websites that originate in the message contents, Spectral Clustering examines the relationship between URL substrings. A Random Forest classifier for phishing is then assembled using cluster membership. This method is evaluated using data from the Phishing Email quantity and the Spam Killer Email quantity. Metrics for performance evaluation include the region Along with the (harmonic mean) F measure, accuracy, exactness, evoke, and receiver operating characteristic curve (AUC). When compared to a satisfied filtering technique like LDA combined with text message deletion carried out arbitrarily or adaptively using adversarial learning, the presentation of the integrated Spectral Clustering and Random Forest loom is found to provide significant improvements in all the metrics listed. The Spectral Clustering method works well when there is insufficient content. In a study proposed by Gowtham et al. [2], the characteristics of phishing and legitimate websites were thoroughly analysed. To complement this analysis, heuristics were proposed to remove 15 characters from these websites. In order to detect phishing sites, a trained machine learning system was fed these heuristic results. This method used two first screening modules in this system to the webpages prior to alarmed heuristics. The preapproved site identifier, the first component, checks websites against a user-maintained whitelist, and the Login Form Finder, the second component, classifies websites as authentic when no login

appearances are found. Since cybercrime is a technology-based error committed by technocrats, R. Gnanakumaran et al. [14] suggested a method. The modification of cybercrimes such as bot networks, salami attacks, packet sniffing, and temperate attacks are covered in this study. It also includes actual cybercrime instances, their circumstances, and their methods of operation. Malware, spam, and phishing rates are rapidly increasing globally. Additionally, there is a latent shock of cybercrime on production time, economics, and consumer trust. The GPRS Security architecture, Agent Based Distributed Intrusion Detection System, and prevention system are used for safety purposes in methods that are comparable to intrusion detection. D. M. Krishnan et al. [21] suggest a strategy that combines machine learning techniques with statistical analysis of website URLs to provide an extra accurate classification of phishing URLs. using a two-sample Kolmogorov-Smirnov test in addition to other explanations. Therefore, using these statistical measures can greatly increase the accuracy of phishing URL classification.

III. METHODOLOGY

The purpose of the suggested problem is to investigate phishing detection through the use of online logos. The following two procedures make up the methodology:
The first step will take a screenshot and use a direct way to extract the logo. There are several benefits to this strategy. Since the goal of the study project is to replace the process of locating the logo image among a collection of downloaded photos (the image income of a query webpage), a screenshot will be taken and the logo will be extracted straight from it. There are several benefits to this strategy. There isn't another secret image because the screenshot that was taken is a real offer of the online material. The real web content, which is typically used to enhance page loading time, can be obtained by directly taking a screenshot. Even if the logo was present in the sprite image, Google Image Search will still provide the undesirable result when it uses sprite images as a query result. Another benefit is that the brand will be more accurately removed from a website's poster image. In other words, no non-logo images will be produced by simply removing the logo images. To find the true identity, the second procedure will use a Google picture search. It is reasonable to treat the domain name as the identity because of the unique connection between the logo and the domain name. We can distinguish between a phishing website and a legal website by comparing the domain name that Google returns with the one from the inquiry website. identifying a phishing website by looking for a graphical element, like a logo. To improve phishing detection accuracy, the website's Alexa rank is taken and matched within the range of less than 10,000.
A phishing website is identified by inconsistent identification, while a valid website is identified by consistent identity.

Design

The suggested method took the data flow structure into account when designing the experimental setting. We began by examining the specifications. The following is a list of requirements:
1. Phishing and non-phishing website database.
2. Screenshots of the website in question.
3. A tool for processing website logo images.
4. An automated tool that uses screenshots of logo images to identify phishing sites.

We began by compiling a database of phishing and non-phishing websites in order to validate these design choices. The work has made use of the open-source database Phishload [5]. Webpage screenshots are gathered from PhishTank [6]. If a snapshot of the webpage is available, it is returned via a URL from PhishTank. Java was used to create a processing tool for extracting website logo images. The user must draw a rectangle around the logo image in order for the image to be retrieved using this assisted cropping tool. Another Java-based program is used to identify phishing sites.

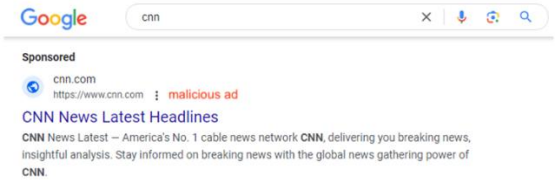

Figure 2: Google Image Search Result

In figure 2 shows that after searing the logo image of a website in the google image search,it shows the result that whether it is a phishing website or a legitimate website.It shows the best guess of the searched logo image.

© MAY 2024 | IRE Journals | Volume 7 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I11-1712451

Flowchart

Figure 3 makes reference to the concept's flowchart. We will load a phishing URL (known only to us) in accordance with the code flow. To obtain its screenshot image, we will load a Phishtank ID from a database and run a search. We will launch the Crop Image Tool and Crop the Logo Region after we get the screenshot image. A logo image is extracted from the database, cropped, and saved in a database for each phase. The picture has been posted to the Google image search engine. Google provides the results in the form of a number of urls (website search results) and a best guess value. The website is identified as valid if the URL of the query logo is in the list of URLs that Google Image Search returns; else, the website's Alexa rank is extracted and matched within the range of less than 10,000.

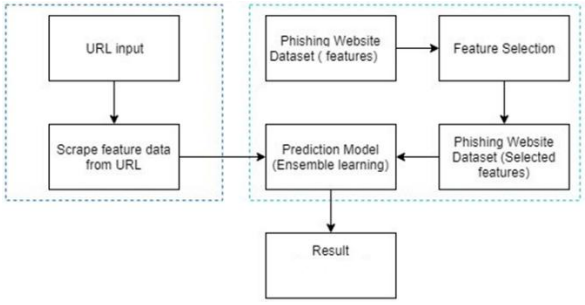

Figure 3: Flowchart of the Proposed Work

To detect various chest diseases, the contribution that has been made to conduct the research work (figure 3) has been shown as under:

1. The data has been collected from two datasets such as NIH chest xray and Malignant Lymphoma Classification.
2. The study employed a novel strategy that combines transfer learning with deep and federated learning techniques to effectively classify chest conditions.
3. Data preprocessing procedures were undertaken to ensure data integrity, alignment with the .csv dataset, handling of missing values (NAN), and data encoding.
4. After preprocessing, the data was visually represented and summarized graphically. This aided in extracting features such as area, perimeter, aspect ratio, and solidity from the data."
5. The dataset was partitioned into training and testing subsets, with a division ratio of 75% for training and 25% for testing. Various augmentation techniques, including flipping and rotation, were applied to enhance dataset diversity.
6. Finally, pre-trained models such as DenseNet-161, Inception V3, ResNet50,MobileNet V2, VGG16, and VGG19 were leveraged for classification tasks. The performance evaluation of these models was conducted using precision rate and recall rate metrics.

IV. RESULTS AND ANALYSIS

A logo image is extracted from the database, cropped, and saved in a database for each phase. The picture has been posted to the Google image search engine. Google provides the results in the form of a number of urls (website search results) and a best guess value. The website is certified as authentic if the URL for the query logo appears in the list of URLs that Google Image Search returns; if it does not appear directly in the list of URLs, the website's Alexa rank is extracted and matched under the range less than 10,000.

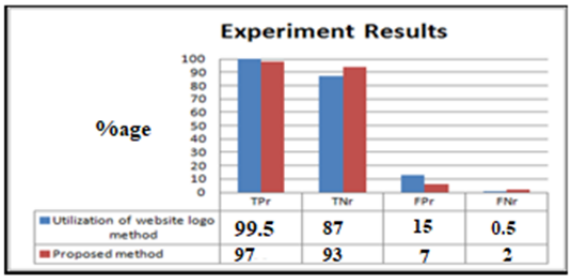

Figure 4: Bar Chart Comparison Analysis of Our System compared to Utilization of website

In Figure 4 the True Positive rate of our system is 97% while the True Positive rate of Utilization of logo image based mehod is 99.5 %, further, the True Negative rate of our system is 93% whereas the true negative rate of Utilization of logo image based mehod is 87 %.

Table 1: Table Comparison Analysis of Our System compared to Utilization of website

Models	TP	TN	FP	FN
Logo Technique	99.5	87	15	0.5
Proposed Technique	97	93	7	2

V. CONCLUSION

The medical industry is seeing rapid growth in the field of AI-based chest disease detection. AI systems are taught to look for patterns or anomalies in medical images like chest X-rays or CT scans that might point to the presence of a chest disease. Convolutional Neural Networks are one of the AI methods for detecting chest diseases that are most frequently employed (CNNs). CNNs are deep learning algorithms that examine the pixels in an image to identify patterns. Another AI method that can be used to identify chest diseases is SVMs. Using features taken from the images, SVMs are machine learning algorithms that can categorise images into various groups. These AI methods allow physicians and other healthcare professionals to diagnose chest diseases more quickly and accurately, which can improve patient outcomes. In this part, we've examined about standing out the proposed model i.e VGG16 from the techniques that researchers have used to distinguish different chest diseases. The correlation has been acted in two situations where the primary case depends on the equivalent dataset and the subsequent case is for various dataset based on their accuracy.

REFERENCES

[1] Chiew, K.L., Chang, E.H. and Tiong, W.K., 2015. Utilisation of website logo for phishing detection. Computers & Security, 54, pp.16-26.

[2] Gowtham, R. and Krishnamurthi, I., 2014. A comprehensive and efficacious architecture for detecting phishing webpages. Computers & Security, 40, pp.23-37.

[3] DeBarr, D., Ramanathan, V. and Wechsler, H., 2013, June. Phishing detection using traffic behavior, spectral clustering, and random forests. InIntelligence and Security Informatics (ISI), 2013 IEEE International Conference on (pp. 67-72). IEEE.

[4] Tout, H. and Hafner, W., 2009, August. Phishpin: An identity-based anti-phishing approach. In Computational Science and Engineering, 2009. CSE'09. International Conference on (Vol. 3, pp. 347-352). IEEE.

[5] Phishload. 2016. Phishload. [ONLINE] Available at: http://www.medien.ifi.lmu.de/team/max.maurer/files/phishload. [Accessed 01 July 2016].

[6] PhishTank | Join the fight against phishing. 2016. PhishTank | Join the fight against phishing. [ONLINE] Available at: http://www. K. L. Chiew, E. H. Chang, S. N. Sze, and W. K. Tiong, “Utilisation of website logo for phishing detection,” Comput. Secur., pp. 1–11, 2015.

[7] J. Hong and L. Cranor, “CANTINA : A Content-Based Approach to Detecting Phishing Web Sites,” pp. 639–648, 2007.

[8] Mr DD Sarpate, "Design of Dual Band Microstrip for satellite Applications", 2nd International Conference on Recent Innovations in Engineering & Technology 2020.

[9] Umar, Syed, Bommina Naveen Sai, Nagineni Sai Lasya,Doppalapudi Asutosh, and LohithaRani. "Machine Learning based Sentiment Analysis of Product Reviews Using DeepEmbedding." Journal of Optoelectronics Laser 41, no. 6(2022): 108-113.

[10] Habeeb, M. S., & Babu, T. R. (2022). Network intrusion detection system: a survey on artificial intelligence-based techniques. Expert Systems, 39(9), e13066

[11] Mr. Dikshendra Daulat Sarpate, and Dr. B.G Nagaraja, "CONVOLUTION NEURAL NETWORK-BASED SPEECH EMOTION RECOGNITION USING MFCCS", International Journal of Communication Networks and Information Security, 2023/12/10

[12] Usman, M., Zubair, M., Hussein, H. S., Wajid, M., Farrag, M., Ali, S. J., ... & Habeeb, M. S. (2021). Empirical mode decomposition for analysis and filtering of speech signals. IEEE Canadian Journal of Electrical and Computer Engineering, 44(3), 343-349.

[13] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimized AI Models for Real-Time Cyberattack Detection in Smart Homes and Cities", International Journal of Applied Engineering & Technology, Vol. 4 No.1, June, 2022.

[14] R. Gnanakumaran, Divya Rohatgi, A K Sampath, Nidhi Nagar, D. Amuthaguka, Raj Kumar Gupta, "Robust Extreme Learning Machine based

Sentiment Analysis and Classification", 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), (2023), DOI: 10.1109/ICSSIT55814.2023.10061017.

[15] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Privacy-Preserving Federated Learning for IoT Devices with Secure Model Optimization", International Journal of Communication Networks and Information Security (IJCNIS), (2021), 13(2), 396–405.

[16] K. Kartheeban, K. Kalyani, S. K. Bommavaram, D. Rohatgi, M. N. Kathiravan, and S. Saravanan, “Intelligent Deep Residual Network based Brain Tumor Detection and Classification,” in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Dec. 2022, pp. 785–790. doi:10.1109/ICACRS55517.2022.10029146.

[17] Nandipati Sai Akash, Naveen Sai Bommina, Uppu Lokesh, Hussain Syed, Syed Umar, "Optimized Block Chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization", International Journal on Recent and Innovation Trends in Computing and Communication, (2023), 11(10), 1226–1233.

[18] D Veerendra, BN Umesh, A Khandare, D Rohatgi, K Tiwari, S Datta, "ECA-MURE algorithm and CRB analysis for high-precision DOA estimation in coprime sensor arrays", IEEE Sensors Letters 7 (12), 1-4.

[19] Naveen Sai Bommina , Nandipati Sai Akash, Uppu Lokesh , Dr. Hussain Syed , Dr. Syed Umar, "Multi-Objective Genetic Algorithms for Secure Routing and Data Privacy in IoT Networks", International Journal of Communication Networks and Information Security (IJCNIS), (2020), 12(3), 632–643.

[20] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[21] D. M. Krishnan and V. Subramaniyaswamy, “Phishing website detectionsystem based on enhanced itree classifier,” ARPN J. Eng. Appl. Sci.,vol. 10, no. 14, pp. 5688–5699, 2015