qrAs per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology
Volume 10, Issue 02, pages 484-90.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue02.html
DOI: https://doi.org/10.46501/IJMTST1002066

A Novel Solution the Social Media Privacy Checker Designed To Empower Users with the Ability to Assess

Dr.D.Kalyankumar, GottumukkalaVeeraVenkata Naveen, Kalyani Vallapuneni, Nallapaneni Sravan Sudheer

Dept.of CSE-Cyber Security, Chalapathi Institute of Technology,Guntur, Andhra Pradesh, India

To Cite this Article
Dr.D.Kalyankumar, GottumukkalaVeeraVenkata Naveen, Kalyani Vallapuneni, Nallapaneni Sravan Sudheer, A Novel Solution the Social Media Privacy Checker Designed To Empower Users with the Ability to Assess, International Journal for Modern Trends in Science and Technology, 2024, 10(02), pages. 484-490.https://doi.org/10.46501/IJMTST1002066

Article Info
Received: 28 January 2024; Accepted: 19 February 2024; Published: 25 February 2024.

ABSTRACT

With the widespread use of social media platforms, concerns regarding user privacy have become increasingly paramount. This project introduces a novel solution the Social Media Privacy Checker, designed to empower users with the ability to assess and manage their privacy settings across various social media networks. The motivation for this project stems from the growing need for individuals to have greater control over their digital footprint and the potential risks associated with oversharing. The project begins with a comprehensive literature review, analyzing existing social media privacy tools, their functionalities, and user perceptions. Through this analysis, the research identifies gaps in current solutions, paving the way for the development of an innovative and user-centric privacy-checking application. The methodology involves a multifaceted approach, combining data collection from social media APIs, user surveys, and ethical considerations to ensure the responsible handling of personal information. The system design encompasses a robust architecture, database, and user interface, providing a seamless experience for users to assess and enhance their privacy settings. Implemented algorithms and models facilitate the automatic analysis of privacy configurations, offering users insights into potential vulnerabilities and recommendations for improvements. The project's implementation details, including code structure and testing procedures, are discussed, highlighting the reliability and effectiveness of the Social Media Privacy Checker. Implemented algorithms and models facilitate the automatic analysis of privacy configurations, offering users insights into potential vulnerabilities and recommendations for improvements. The project's implementation details, including code structure and testing procedures, are discussed, highlighting the reliability and effectiveness of the Social Media Privacy Checker.

Keywords: Privacy Checker, social media networks,social media API and effectiveness of the Social Media Privacy

1. INTRODUCTION

Social Media Test Drive is an online simulation tool to prepare people for social interaction in the online world. The policy does not indicate if users are able to interact while using the services. The policy clearly states Social Media Test Drive does not collect personal information; however, they do collect anonymous activity log data and usage information. The policy states aggregated data is shared with vendors contracted by the Social Media Lab; however, the policy states data will never be shared with third parties for marketing or advertising purposes. The policy also confirms Social Media Test Drive does not sell or rent user information. The policy clearly states Social Media Test Drive does not display any behavioral or contextual advertising on the service. Furthermore, the policy confirms Social Media Test Drive does not allow third party tracking, targeted advertising, or profiling. The policy does not indicate that users must create an account; instead, the service is used anonymously and users can enter any module as a guest. The policy does not specify the age of Social Media Test Drive's intended users, but does state Social Media Test Drive supports COPPA and does not collect information from children under 13.

Social Media Test Drive can be accessed through its website. The Privacy Policy and Terms of Use used for this evaluation can be found on Social Media Test Drive’s website. This evaluation only considers policies that have been made publicly available prior to an individual using the application or service. SAFETY The policy states users are able to submit textual input after completing a module and that any personal information will be filtered and deleted before the textual input is submitted to the service. PRIVACY The policy does not indicate if any third party or social login is supported to use the product. The policy confirms information may be transferred in the event of a company sale, merger, or bankruptcy.SECURITY The policy states data will be stored in a safe hard drive of the Social Media Lab and in secure Cornell Box folders, only accessible by the research team of the Social Media TestDrive. The policy does not indicate if data encryption is used. COMPLIANCE The policy does not indicate that users can access or modify data; however, the policy does state users may contact Social Media Test Drive to have data removed.

2. LITERATURE SURVEY

A Literature Review on EndUser Role and Evaluation: A. Padyab and A. Ståhlbröst Trends show that privacy concerns are rising, but end users are not armed with enough mechanisms to protect themselves. Privacy enhancing technologies (PETs) or more specifically, tools (PET-tools) are one of the mechanisms that could help users in this sense. These tools, however, reportedly have low adoption rates, and users tend to be reluctant to integrate them into their daily use of the Internet. Detailed scrutiny of current research on PET-tools, however, can guide future research to help overcome low adoption of these tools. We conducted a literature review on PET-tools to enumerate the types of tools available and how they are being evaluated, in order to shed more light on the missing elements in their evaluations. We reviewed and coded 72 articles in the PET-tool literature. Our results highlight two important issues: 1. Evaluation of most tools is performed using only artificial, summative and ex-post strategies.while usability evaluation is quite common, evaluation of enhanced privacy is lacking. This research hopes to contribute to better PET-tool development, and encourage the inclusion of users in the evaluation and design process [1].

On Privacy and Security in Social Media – A Comprehensive Study Senthil Kumar N*, Saravanakumar K, Deepa K In the larger context of data mining, a considerable measure of productive analyzing so as to learn can be found advanced records of human conduct in interpersonal organizations without breaching the users’ privacy. Thus, information ought to be made accessible in a manner that privacy should be safeguarded and protection is extremely scrutinized. On the other hand, the suspicion that any outsider which is intrigued to break down information can be viewed as reliable is truth be told unlikely, because of the key point of preference that the usage of all information, including recognizing and delicate ones, may provide for these gatherings. Due to the specific instance of interpersonal organizations, the most grounded measure that can be received is to make unflinching quality of individual’s privacy who expresses the affiliation [2].

According to the authors [3], who had proposed that any sort of examination about the number of inhabitants in clients who express inclinations, therefore defusing protection dangers as well as vital investigation. The proposition is still to keep connection ready to the interpersonal organization profiles of their users, however to permit clients to partner some guaranteed property estimations with their credentials, by picking each time they express credits that need to uncover. In the sideline perspective of the privacy domain [1], the subject of privacy has been under scrutiny and ensuring the basic importance given by the particular academic group has deemed to be vigilant. To ensure privacy of clients by recognizing characteristics, not by vulnerability based anonymization. Thus, despite the fact that from an only specialized viewpoint our answer is closer to privacy than protection in the long run, individual information of clients is ensured [3].

Assessing User Privacy on Social Media: The Twitter Case Study Giovanni Livraga, Alessandro Motta, Marco Viviani At the time of writing, nearly four billion people worldwide employ social media platforms such as Facebook, Instagram, WeChat, TikTok, etc. to share content of various kinds, which may also include personal data. In addition to this, users interact with members of the virtual community, leaving behind important behavioral traces. In most cases, people do not have a full understanding of who will be able to access and use such a body of information, and for what purposes. Although social platforms provide users with some tools to protect their privacy, the very nature of these technologies and the psychological characteristics of users often lead them to ignore such solutions [4].

To address this issue, in this paper we aim to propose a model for assessing the privacy of users on social media by identifying the critical aspects associated with their content and interactions generated on such platforms. This model, in particular, considers distinct features, of different kinds, that capture the level of users' exposure with respect to privacy. These features, dropped into a vector space, are used to derive a score that expresses, in a measurable way, the privacy risk of users compared to the information available on social media about them. The proposed model is instantiated and tested on data collected from the microblogging platform Twitter, on which the results of the experimental evaluation are analyzed. Specifically, the model is tested by considering both a binary scenario, i.e., where users' privacy is evaluated as at risk or not, a multi-class scenario, i.e., where their privacy is evaluated against different risk ranges, and a ranking scenario, i.e., where the users are ranked according to their privacy assessment [4]

The Use of Social Networks as a Communication Tool between Teachers and Students: ALiterature Review Facundo FROMENT, Alfonso Javier GARCÍA GONZÁLEZ Social networks have drastically changed communication between people, constituting a means of everyday use by which information is created and shared in a simple, instantaneous way with the rest of the world. Although social networks were not initially created for academic purposes, they are gradually being used as a means of communication between teachers and students, making them an extremely important element in the teachinglearning process by offering new possibilities for communication and interaction as well as creating new learning spaces. The purpose of this study is to analyze the use of social networks as a communication tool between teachers and students through a thorough bibliographical review [5]. To do this, a systematic review of scientific documents containing data on teacher-student communication through social networks was carried out, resulting in a total of 96 documents published between 2006 and 2016 indexed in different internationally consulted databases. From the analyzed documents were extracted the educational levels in which research on teacherstudent communication in social networks were carried out; the most addressed social networks in the study of teacher-student interaction through social networks; the research areas that have been developed and the main results [6].

Social media and innovation: A systematic literature review and future research directions Hardik Bhimani, Anne – Laure, Pierre-Jean Barlatier Social media are privileged vehicles to generate rich data created with unprecedented multi-faceted insights to drive faster ideation and commercialisation of client-centric innovations. The essence of data generated through social media is rooted in the connections and relationships it enables between firms and their stakeholders, and represents one of the greatest assets for data-driven innovation. As most of the firms are still experiencing and trailblazing in this matter, the current challenge is therefore to learn how to benefit from social media's potential for innovation purposes. In the last decade, research interest has increased towards understanding social media – innovation interactions. The reliance on the wisdom of the crowd in driving major business decisions and shaping society's way of life is now well acknowledged in academic and business literature. Social media is increasingly used as a tool to manage knowledge flows within and across organisation boundaries in the process of innovation. Yet, conceptualisation of social media and innovation interaction and a systematic review of how far the field has come remain providential.

Therefore, through a systematic literature review we aim to identify research trends and gaps in the field, conceptualise current paradigmatic views and therein provide clear propositions to guide future research. Based on a systematic review, 111 articles published in peer-reviewed journals and found in EBSCO Host® and Scopus® databases are descriptively analysed, with results synthesized across current research trends. Findings suggest social media is seen as enabler and driver of innovation, with behavioural and resource based perspectives being the most popular theoretical lens used by researchers [4]. The originality of the paper is rooted in the comprehensive search and systematic review of studies in the discourse, which have not been unified to date. Implications for advancement of knowledge are embedded in the purposefully proposed theoretical, contextual and methodological perspectives, providing future research directions for exploring social media capability in innovation management [5].

The Impact of Social Networks and Privacyon Electronic Word-of-Mouth in Facebook:Exploring Gender Differences NAMSU PARK, YOOJUNG KIM Using a privacy calculus perspective, this study examines how Facebook users' social networks, privacy concerns, understanding of privacy policies, and privacy protection behaviors influence electronic word-of-mouth (eWOM). It further investigates whether gender difference exists in relationships among variables. The results of an online survey of Korean adults (N = 522, 49.4% females) showed that users' social networks, privacy concerns, and privacy protection behaviors are significant factors in the increase of eWOM. Conversely, understanding privacy policies has no significant impact on eWOM [17]. The findings about gender difference revealed that women, who have more actual friends, were more likely to engage in eWOM than were men, and that women prefer to create eWOM when they have a higher level of privacy protection behavior. Further implications are discussed in light of expanding social networks and effective privacy settings as well as the need for a gender-sensitive social media marketing strategy [7].

Social Media Adoption, Usage And Impact In Business-To-Business (B2B) A State-Of-The-Art Literature Review Yogesh K. Dwivedi, Elvira Ismagilova, Nripendra P. Rana Social media plays an important part in the digital transformation of businesses. This research provides a comprehensive analysis of the use of social media by business-to-business (B2B) companies. The current study focuses on the number of aspects of social media such as the effect of social media, social media tools, social media use, adoption of social media use and its barriers, social media strategies, and measuring the effectiveness of use of social media. This research provides a valuable synthesis of the relevant literature on social media in B2B context by analysing, performing weight analysis and discussing the key findings from existing research on social media. The findings of this study can be used as an informative framework on social media for both, academic and practitioners [23].

A comprehensive review of security threats and solutions for the online social networks industry Naeem A. Nawaz, Kashif Ishaq, Uzma Farooq The term "cyber threats" refers to the new category of hazards that have emerged with the rapid development and widespread use of computing technologies, as well as our growing reliance on them. This article presents an in-depth study of a variety of security and privacy threats directed at different types of users of social media sites. Furthermore, it focuses on different risks while sharing multimedia content across social networking platforms, and discusses relevant prevention measures and techniques. It also shares methods, tools, and mechanisms for safer usage of online social media platforms, which have been categorized based on their providers including commercial, open source, and academic solutions [21].

Social Media, Ethics and the Privacy Paradox Nadine Barrett-Maitland and Jenice Lynch Today's information/digital age offers widespread use of social media. The use of social media is ubiquitous and cuts across all age groups, social classes and cultures [19]. However, the increased use of these media is accompanied by privacy issues and ethical concerns. These privacy issues can have far-reaching professional, personal and security implications. Ultimate privacy in the social media domain is very difficult because these media are designed for sharing information. Participating in social media requires persons to ignore some personal, privacy constraints resulting in some vulnerability [18].

3. SYSTEM MODELLING

Existing system: There were no widely recognized and established standalone tools explicitly named "social media privacy checker." However, there were various tools and services designed to help users manage and enhance their privacy on social media platforms. These tools often focused on features such as reviewing and adjusting privacy settings, monitoring account activity, and providing tips on improving online security. Here are some elements that a social media privacy checker tool might incorporate based on existing trends.

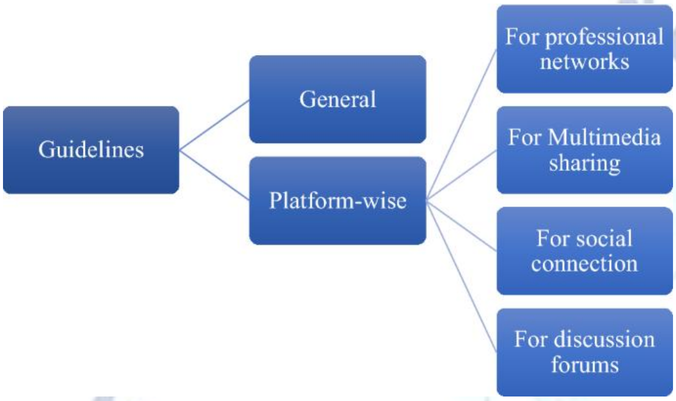

Fig 1: Online social networks security and privacy

Privacy Settings Review: Analyzing and summarizing the privacy settings of the user's social media accounts. Providing recommendations to enhance privacy based on individual preferences.

Security Alerts: Notifying users about any suspicious activities or login attempts on their social media accounts. Offering guidance on how to secure their accounts in case of potential security breaches [23].

Profile Visibility Analysis: Assessing the visibility of a user's profile and content to the public, friends, or custom groups. Suggesting adjustments to ensure the desired level of privacy [22].

Third-Party App Permissions: Reviewing and managing the permissions granted to third-party applications connected to social media accounts. Alerting users about potentially risky or unnecessary app permissions [24].

Activity Monitoring: Tracking and summarizing the user's recent activities on social media.Providing insights into what information is publicly accessible or visible to different groups of people.

Proposed system: A proposed system that could serve as a foundation for my social media privacy checker tool:

User Authentication and Account Linking: Users should authenticate their social media accounts with the tool securely. Allow linking multiple social media accounts to provide a comprehensive privacy analysis.

Privacy Settings Assessment: Conduct a thorough review of privacy settings for each linked social media account. Summarize existing privacy configurations and provide an easy-to-understand report.

Profile Visibility Analysis: Evaluate the visibility of a user's profile, posts, and other information to different audience groups (public, friends, custom lists). Offer suggestions for optimizing privacy based on user preferences.

Security Alerts and Monitoring: Implement real-time monitoring for suspicious activities, login attempts, and changes to account settings. Send security alerts to users if any abnormal or unauthorized activity is detected [21].

Third-Party App Permissions: Display a list of connected third-party applications and the permissions they have. Provide recommendations for revoking unnecessary or high-risk app permissions [18].

Activity Tracking and Historical Data: Track and present recent user activities on social media platforms. Allow users to review historical data to identify patterns or changes in their online behaviour [20].

Custom Privacy Recommendations: Generate personalized recommendations for improving privacy settings based on the user's online behavior and preferences.Offer tips and best practices for maintaining a secure and private online presence.

Educational Resources: Integrate educational materials within the tool to inform users about online privacy risks and best practices. Keep users updated on changes in social media platforms' privacy policies.

4. SYSTEM DESIGN

Designing system architecture for a social media privacy checker tool involves several components to ensure efficient and accurate analysis of privacy settings across various social media platforms. Here's a high-level overview of the architecture:

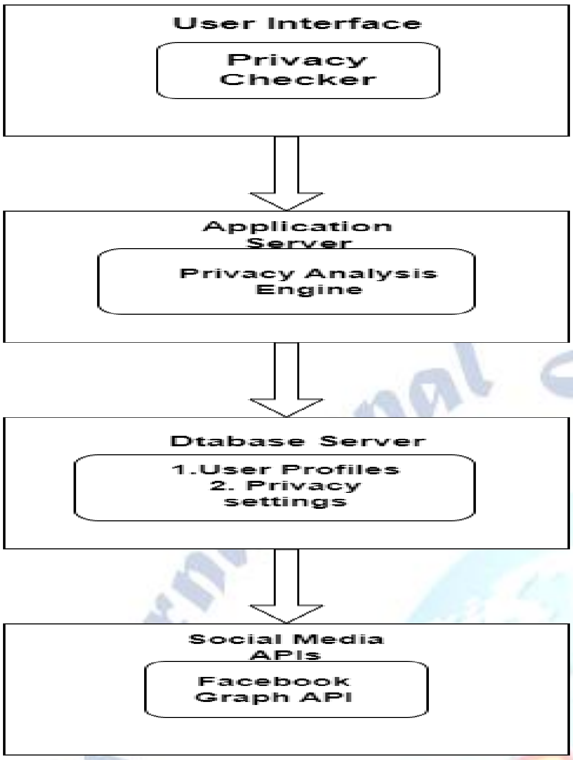

Fig 1: System Architecture

Frontend Interface: This component interacts directly with users, providing a user-friendly interface for inputting social media account details and viewing privacy analysis results [19].

Backend Interface: Handles communication between the frontend and backend systems, processing user requests and displaying results [18]**.**

Authentication and Authorization: Handles user authentication and authorization to ensure only authorized users can access the tool and analyze social media accounts [17].

Data Ingestion: Responsible for collecting social media data from various platforms. This could involve utilizing APIs provided by social media platforms or using web scraping techniques to gather relevant information.

5. CONCLUSIONS

In conclusion, the development of a social media privacy checker tool represents a significant step towards empowering users to better understand and manage their online privacy. By analyzing the privacy settings and configurations across multiple social media platforms, this tool provides users with valuable insights into their digital footprint and helps them make informed decisions to protect their personal information. Throughout the project, we have designed a comprehensive system architecture that encompasses various components, including user interface, authentication, data ingestion, processing, privacy analysis engine, storage, notification system, reporting, scalability, security, compliance, and maintenance. Each of these components plays a crucial role in ensuring the effectiveness, security, and scalability of the tool.

6. FUTURE SCOPE

The future scope for your social media privacy checker tool project is vast and includes several avenues for expansion and improvement. Continuously update the tool to integrate with emerging social media platforms and stay relevant as users adopt new platforms. Invest in research and development to improve the accuracy and depth of privacy analysis algorithms, allowing for more comprehensive evaluations of privacy settings. Implement machine learning techniques to provide personalized recommendations based on users' online behavior and preferences, helping them tailor their privacy settings to their specific needs. By exploring these future scope areas and remaining responsive to evolving user needs and technological advancements, your social media privacy checker tool can continue to make a meaningful impact in promoting online privacy awareness and empowering users to protect their personal information effectively.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] S. Shaham, M. Ding, B. Liu, Z. Lin, and J. Li, "Machine learning aided anonymization of spatiotemporal trajectory datasets," arXiv preprint arXiv:1902.08934, 2019.

[2] A. Government, "New australian government data sharing and release legislation," 2018.

[3] A. Tamersoy, G. Loukides, M. E. Nergiz, Y. Saygin, and B. Malin, "Anonymization of longitudinal electronic medical records," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 3, pp. 413–423, 2012.

[4] F. Xu, Z. Tu, Y. Li, P. Zhang, X. Fu, and D. Jin, "Trajectory recovery from ash: User privacy is not preserved in aggregated mobility data," in Proceedings of the 26th International

Conference on World Wide Web. International World Wide Web Conferences Steering Committee, 2017, pp. 1241–1250.

[5] Y. Dong and D. Pi, “Novel privacy-preserving algorithm based on frequent path for trajectory data publishing,” Knowledge-Based Systems, vol. 148, pp. 55–65, 2018.

[6] M. Gramaglia, M. Fiore, A. Tarable, and A. Banchs, “Towards privacy-preserving publishing of spatiotemporal trajectory data,” arXiv preprint arXiv:1701.02243, 2017.

[7] . Terrovitis, G. Poulis, N. Mamoulis, and S. Skiadopoulos, “Local suppression and splitting techniques for privacy preserving publication of trajectories,” IEEE Trans. Knowl. Data Eng, vol. 29, no. 7, pp. 1466–1479, 2017.

[8] . E. Nergiz, M. Atzori, and Y. Saygin, “Towards trajectory anonymization: a generalization-based approach,” in Proc. of the SIGSPATIAL ACM GIS. ACM, 2008, pp. 52–61.

[9] . Gurung, D. Lin, W. Jiang, A. Hurson, and R. Zhang, “Traffic information publication with privacy preservation,” ACM Transactions on Intelligent Systems and Technology (TIST), vol. 5, no. 3, p. 44, 2014.

[10] R. Yarovoy, F. Bonchi, L. V. Lakshmanan, and W. H. Wang, “Anonymizing moving objects: How to hide a mob in a crowd?” in Proc. of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 72– 83.

[11] B. Liu, W. Zhou, T. Zhu, L. Gao, and Y. Xiang, “Location privacy and its applications: A systematic study,” IEEE Access, vol. 6, pp. 17 606–17 624, 2018.

[12] G. Poulis, G. Loukides, S. Skiadopoulos, and A. GkoulalasDivanis, “Anonymizing datasets with demographics and diagnosis codes in the presence of utility constraints,” Journal of biomedical informatics, vol. 65, pp. 76–96, 2017.

[13] T. Takahashi and S. Miyakawa, “Cmoa: Continuous moving object anonymization,” in Proceedings of the 16th International Database Engineering & Applications Sysmposium. ACM, 2012, pp. 81–90.

[14] X. Zhou and M. Qiu, “A k-anonymous full domain generalization algorithm based on heap sort,” in International Conference on Smart Computing and Communication. Springer, 2018, pp. 446–459.

[15] Kalyan Kumar Dasari&amp; Dr, K.Venkatesh Sharma, “Mobile Agent Applications in Intrusion Detection System (IDS)”-JASC, Volume 4, Issue 5, October/2017, ISSN NO:1076-5131, Pages: 97-103.

[16] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, “Analyzing the Role of Mobile Agent in Intrusion Detection System”-JASRAE, Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540, Pages: 566-573.

[17] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, “A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework”-JASRAE, Vol. XI, Issue No. 22, July-2016, ISSN 2230-7540, Pages: 209-214

[18] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[19] Anderson, K. (2023). Phishing Threats and Trends: A Comprehensive Analysis. Journal of Cybersecurity Research, 7(2), 213-230.

[20] Smith, M., & Johnson, R. (2022). Behavioral Aspects of Phishing Attacks: An Empirical Study. Proceedings of the International Conference on Cybersecurity (ICC), 2022, 112-126.

[21] Brown, A. (2021). Machine Learning Approaches for Phishing Detection: A Review. Journal of Information Security, 14(4), 421-438.

[22] Wilson, L. (2020). Social Engineering in Phishing Attacks: An Overview of Tactics and Countermeasures. International Journal of Human-Computer Interaction, 33(1), 89- 104.

[23] Martinez, J. (2019). Phishing Simulation Effectiveness: A Comparative Analysis. ACM Transactions on Information and System Security, 24(3), 345-362.

[24] Thompson, S. (2018). Email Security Protocols and their Role in Phishing Prevention. Journal of Network Security, 19(2), 178-193.

[25] Garcia, D., & Adams, E. (2017). The Evolution of Phishing Techniques: A Historical Perspective. Journal of Cyber Threat Intelligence, 28(4), 432-447.

[26] Kalyan Kumar Dasari & Dr, K.Venkatesh Sharma, “Mobile Agent Applications in Intrusion Detection System (IDS)”-JASC, Volume 4, Issue 5, October/2017, ISSN NO:1076-5131, Pages: 97-103.

[27] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, “Analyzing the Role of Mobile Agent in Intrusion Detection System”-JASRAE, Vol. XV, Issue No. 1, April-2018, ISSN 2230-7540, Pages: 566-573.

[28] Kalyan Kumar Dasari& Dr, K.Venkatesh Sharma, “A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework”-JASRAE, Vol. XI, Issue No. 22, July-2016, ISSN 2230-7540, Pages: 209-214

[29] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[30] . K. .Kommineni and A. . Prasad, “A Review on Privacy and Security Improvement Mechanisms in MANETs”, Int J IntellSystApplEng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

[31] alyan Kumar Dasari&amp; M.Prabhakar “Professionally Resolve the Password Security knowledge in the Contexts of Technology”-IJCCIT, Vol. 3, Issue. 1, April’ 2015;ISSN: 2345 – 9808 (2015).

[32] .Mounika D. Kalyan Kumar “Background Subtraction by Using DE Color Algorithm” -IJATCSE, ISSN 2278-3091 Vol: 3, No: 1, Pages: 273-277(2014).

[33] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023- 15926-5

[34] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., &Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.