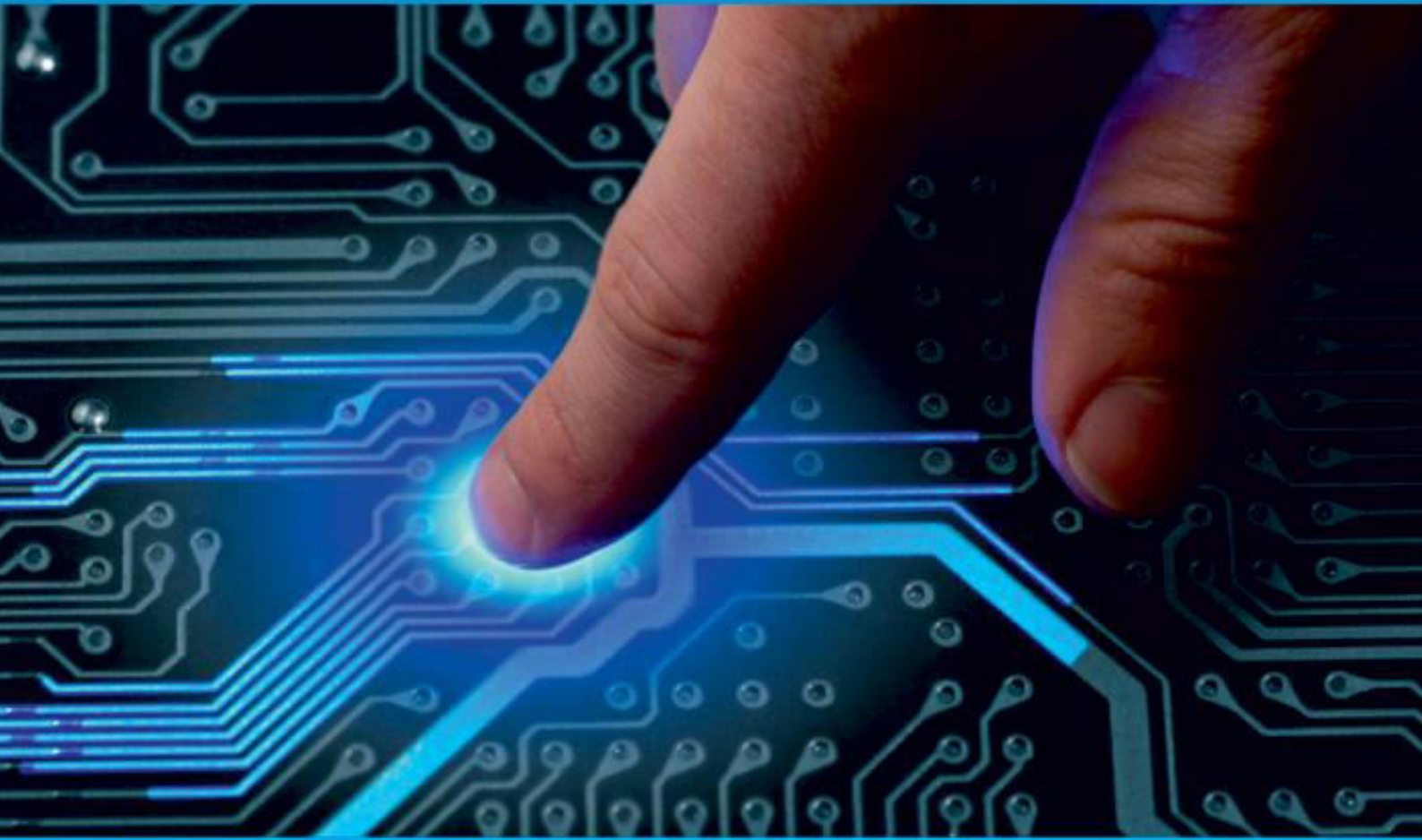




IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798




INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

 9940 572 462

 6381 907 438

 ijircce@gmail.com

 www.ijircce.com

Multi-Modal Hierarchical Attention Model for Enhanced Phishing Website Detection

¹Rakshith K R, ²Murugan R

¹Student of MCA, Department of CS & IT, Jain (Deemed-to-be) University, Bangalore, India

²Professor, Department of CS & IT, Jain (Deemed-to-be) University, Bangalore, India

ABSTRACT: Phishing website attacks persist as a major cyber threat, continually evolving to evade detection. Existing detection methods, such as lookup systems and fraud cue-based approaches, have limitations, prompting the need for advanced techniques capable of addressing these challenges. This paper introduces a novel approach, the Multi-Modal Hierarchical Attention Model (MMHAM), designed to enhance phishing website detection by jointly analysing three crucial modalities: URLs, textual information, and visual design. Traditional lookup systems often fall short in addressing newly created attacks, while fraud cue-based methods may rely heavily on feature engineering, limiting their effectiveness. Deep representation-based methods have shown promise in learning intricate fraud cues, primarily focusing on URLs. However, they neglect the analysis of textual content and visual design, two equally important aspects of website content. MMHAM integrates information from URLs, textual content, and visual design through a shared dictionary learning approach. This innovative mechanism aligns representations from different modalities within the attention model, enabling the model to learn deep fraud cues comprehensively. The proposed MMHAM not only improves phishing detection capabilities but also introduces a hierarchical interpretability system. This system enhances model trustworthiness and provides actionable intelligence for informed decision-making at various levels of phishing threat detection. In our evaluation experiments, MMHAM demonstrated superior performance compared to existing methods, showcasing its ability to learn enhanced deep cues for phishing detection. Furthermore, the hierarchical interpretability system enabled the extraction of valuable phishing threat intelligence. This intelligence can be leveraged to inform phishing website detection strategies at different levels, empowering cybersecurity professionals with a more robust and adaptable defense against phishing attacks. The MMHAM model represents a significant step forward in the ongoing effort to combat the evolving landscape of cyber threats, particularly in the realm of phishing website detection.

I. INTRODUCTION

Phishing threat intelligence plays a pivotal role in the realm of Cyber Threat Intelligence (CTI), especially within Security Operations Centres (SOC) of organizations. The persistent nature of phishing attacks poses a significant and widespread cybersecurity concern, particularly affecting electronic commerce (e-commerce) platforms. Industry reports highlight the substantial time invested by SOC analysts in responding to phishing attacks, underscoring the critical need for effective solutions in this domain. Among the various phishing attack types, phishing website attacks stand out as one of the most prevalent and insidious forms. These attacks involve the use of fraudulent websites to illicitly capture sensitive information from unsuspecting users, including account credentials, passwords, and credit card details. Recognizing the severity of this threat, the automation of phishing website detection becomes imperative for robust phishing threat intelligence. Artificial intelligence methods, notably machine learning, have emerged as crucial tools in the analysis of website information to ascertain the legitimacy of websites. This paper explores the application of artificial intelligence in phishing website detection, categorizing the methods into three overarching groups: lookup systems, fraud cue-based methods, and deep representation-based methods. The utilization of these advanced techniques aims to enhance the efficiency and accuracy of phishing threat intelligence, allowing SOC professionals to proactively defend against the evolving landscape of phishing attacks in the dynamic cybersecurity environment.

II. SYSTEM ANALYSIS

The System analysis is a vital process encompassing the systematic collection and interpretation of information, problem identification, and the decomposition of a system into its constituent components. The primary objective of system analysis is to study the entirety of a system or its individual parts to discern and define its objectives. It operates as a problem-solving technique, enhancing system functionality and ensuring optimal performance by coordinating the efficient operation of all system components. This analytical process serves to specify the intended functionalities of the system. In the context of software engineering, the term "module" refers to distinct software components created through the division of software. Software is partitioned into various components that collaborate to form a unified and functioning whole. However, these components can also operate independently as standalone functions when not interconnected. This systematic creation of software modules is known as Modularity, a critical concept in software engineering. Modularity measures the extent to which these components can be independently created and combined. In cases where projects or software designs become inherently complex, making it challenging to comprehend their workings, modularity becomes an essential tool for reducing complexity. The fundamental principle guiding Modularity is that systems should be constructed from cohesive, loosely coupled components or modules. This implies that a system should consist of diverse components that are interconnected and function seamlessly, each serving a well-defined purpose. To define a modular system, several properties and criteria are considered to evaluate a design method in terms of its capabilities and effectiveness. The proposed system under analysis consists of two core modules: Admin and User. These modules are designed to fulfil distinct functionalities, catering to the needs of both administrators and end-users, and they play a crucial role in achieving the overall efficiency and effectiveness of the system.

There are two modules in the proposed system. They are : Admin & User

Admin Module: The Admin module of the proposed system encompasses essential functionalities tailored for administrators. Admins can initiate their sessions through a secure login process, ensuring controlled access. The module provides the capability to view and authorize users, allowing administrators to manage user permissions effectively. Admins can also oversee the entirety of data sets within the system, including viewing all data sets and categorizing them based on attacker types. Monitoring reviews, examining threat results, and reviewing outcomes for both data sets and user reviews are crucial features embedded in this module. The Admin module is designed for seamless navigation, ensuring administrators can efficiently interact with the system and maintain a comprehensive overview of its functionalities. To conclude their sessions securely, administrators have the option to logout.

User Module: In contrast, the User module is tailored to meet the specific needs of end-users interacting with the system. Users can initiate their engagement by registering an account, followed by a secure login process for access. Once logged in, users can view and manage their profiles within the system. The module enables users to contribute to the system by uploading data sets and subsequently accessing and managing their uploaded data sets. Users can leverage the system to identify phishing threat types, providing a valuable contribution to threat intelligence. Additionally, the User module allows users to review feedback provided by other users within the system. To conclude their sessions securely, users have the option to logout, ensuring controlled access to the system. This separation of functionalities ensures a user-friendly interface for both administrators and end-users, fostering efficient interaction within the system.

III. BACKGROUND

The foundation of the research methodology is grounded in the escalating and persistent threat of phishing attacks within the expansive cybersecurity landscape, with a particular emphasis on the vulnerability of electronic commerce (e-commerce) platforms. Phishing attacks, specifically those involving deceptive websites, have arisen as a significant cause for concern, presenting substantial risks to sensitive information such as account credentials, passwords, and credit card details. Recognizing the crucial role of Security Operations Centres (SOC) in organizations, the study acknowledges their pivotal responsibility in responding to and mitigating the evolving threats posed by phishing attacks. The introduction highlights the considerable time invested by SOC analysts in responding to phishing attacks, accentuating the urgent need for effective solutions in this domain. It sheds light on the pervasive and adaptive nature of phishing attacks, particularly underscoring their impact on e-commerce platforms, where financial transactions and

sensitive data exchanges are commonplace. Importantly, the paper identifies phishing website attacks as one of the most prevalent and insidious forms, involving the utilization of fraudulent websites to illicitly capture sensitive information.

In response to the severity of this evolving threat landscape, the paper advocates for the imperative automation of phishing website detection to fortify robust phishing threat intelligence. Artificial intelligence, specifically the application of machine learning, is identified as a critical tool in the analysis of website information to discern the legitimacy of online platforms. The introduction categorizes these AI-driven methods into three overarching groups: lookup systems, fraud cue-based methods, and deep representation-based methods, providing a structured framework for subsequent exploration. Building upon this background, the research methodology is meticulously crafted to systematically delve into the challenges and potentials associated with the application of AI in phishing website detection. The primary objective is to assess the efficiency and accuracy of phishing threat intelligence methods, particularly those harnessing artificial intelligence, in reinforcing SOC defence capabilities. The methodology incorporates key elements, including an extensive literature review, specific research questions, hypotheses formulation, a mixed-methods research design, diverse data sources encompassing real-world phishing attack datasets and SOC practices, a targeted sampling strategy to ensure relevance and representativeness, ethical considerations to uphold research integrity, and a comprehensive data analysis approach employing both statistical techniques and thematic analysis. Ultimately, the overarching aim of this research methodology is to provide a thorough and nuanced investigation into the practical application of artificial intelligence in phishing website detection. By doing so, the research endeavours to offer valuable insights that can inform and fortify cybersecurity practices in the face of the ever-evolving threat landscape, particularly within the context of e-commerce platforms and their susceptibility to phishing attacks.

IV. RESEARCH METHODOLOGY

In order to comprehensively investigate the application of artificial intelligence (AI) in phishing website detection within the realm of Cyber Threat Intelligence (CTI), this research will deploy a multifaceted methodology designed to yield nuanced insights into the efficacy and accuracy of phishing threat intelligence methods. The primary objective is to evaluate the tangible impact of these methods on the defence capabilities of Security Operations Centres (SOC). Establishing a robust foundation for the study, an exhaustive literature review will be conducted to discern prevailing gaps, challenges, and recent advancements in the spheres of phishing attacks, threat intelligence, and AI applications in cybersecurity. The study will be guided by specific research questions derived from the key aspects highlighted in the introduction. These questions will delve into the landscape of prevalent phishing attack types, the nuanced responses of SOC analysts to phishing incidents, and the effectiveness of existing detection methods. Hypotheses will be formulated based on these research questions, aiming to predict outcomes related to the enhancement of efficiency through automation and the superiority of machine learning-based methods in comparison to traditional approaches.

To ensure a comprehensive understanding, a mixed-methods research design will be employed, harmonizing quantitative analyses of detection accuracy with qualitative examinations of SOC response strategies. Diverse and representative data sources will be curated, encompassing real-world phishing attack datasets and detailed information on SOC practices. A targeted sampling strategy will be implemented to ensure the relevance and representativeness of the study population, allowing for a nuanced exploration of the subject matter. Addressing ethical considerations is paramount, with measures in place to safeguard participant confidentiality and handle sensitive information responsibly. The data analysis phase will encompass both statistical techniques for quantitative data, evaluating the performance of AI-based methods, and thematic analysis for qualitative insights, extracting valuable information from SOC professionals' experiences and perspectives. The research methodology will culminate by offering a comprehensive summary of the planned approach, accentuating its alignment with the predefined objectives. Additionally, potential limitations will be acknowledged, and strategies to mitigate these constraints will be detailed. This meticulous methodology aims to provide a holistic and nuanced understanding of the role and impact of AI in phishing website detection, offering valuable insights for the evolving landscape of cybersecurity.

V. DIFFERENT APPROACHES IN MULTI-MODAL HIERARCHICAL ATTENTION MODEL FOR ENHANCED PHISHING WEBSITE DETECTION

1. Text Modality:

- Use word embeddings or train them on the dataset.
- Employ RNNs, CNNs, or transformers for text processing.
- Implement attention mechanisms to weigh word importance dynamically.

2. Image Modality:

- Utilize CNN architectures to extract features from screenshots or logos.
- Fine-tune pre-trained CNN models or use transfer learning.
- Combine features from different CNN layers for comprehensive visual cues.

3. Hierarchical Attention Mechanisms:

- Design hierarchical structures to attend to different abstraction levels.
- Apply attention mechanisms within each modality and across modalities.
- Emphasize both fine-grained and coarse-grained features.

4. Fusion Strategies:

- Consider early fusion by combining modalities at input levels.
- Explore late fusion for more flexible integration.
- Incorporate multi-modal attention for dynamic modality contribution.

5. Training Strategies:

- Implement multi-task learning for related tasks.
- Introduce adversarial training to enhance robustness.
- Augment training data to improve generalization across diverse scenarios.

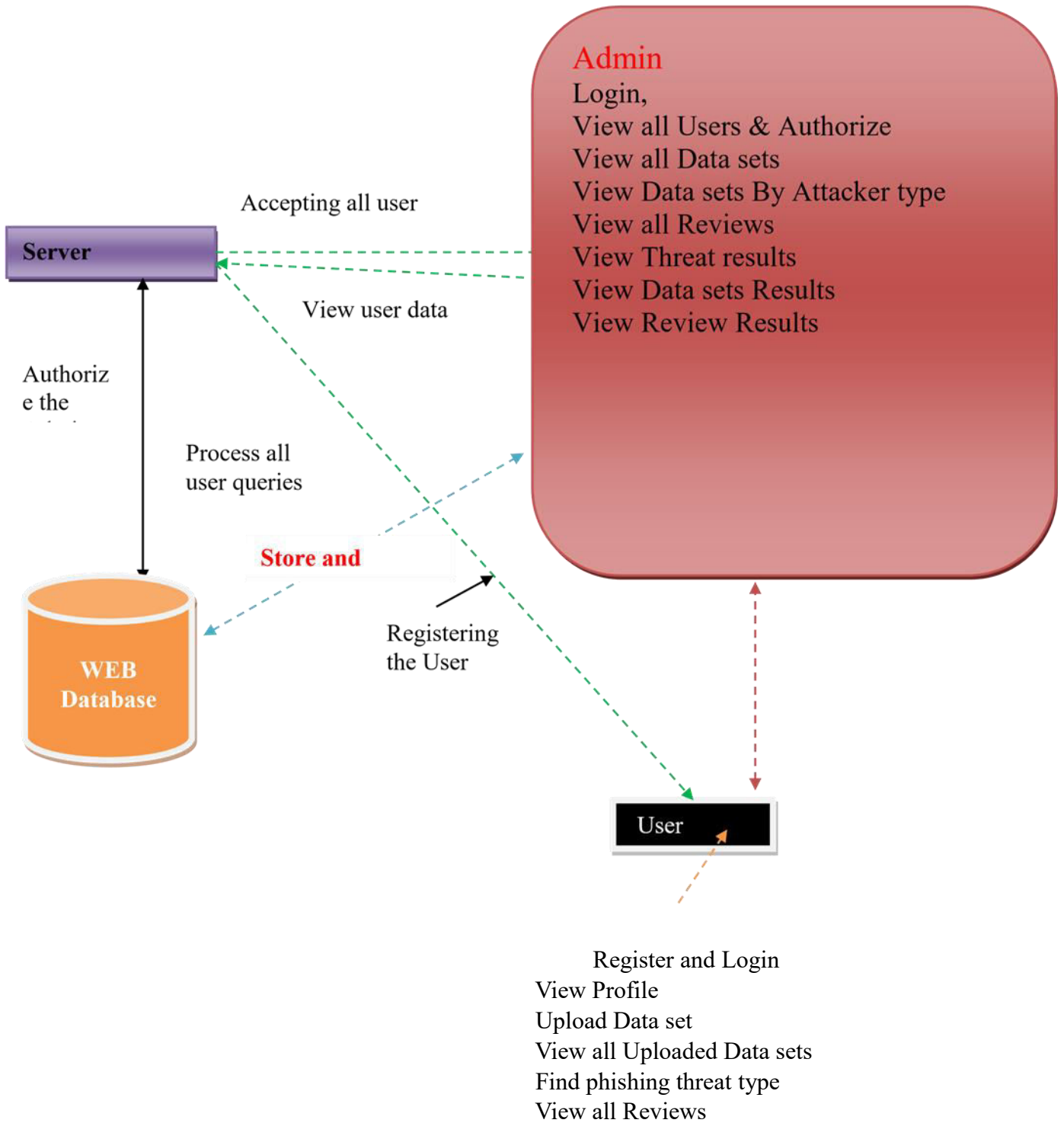
VI. SYSTEM DESIGN AND ARCHITECTURE

Business system analysis is a meticulous process involving the planning of a new business system or upgrading an existing one by defining its components or modules to meet specific requirements and optimize operational efficiency. Prior to the planning phase, a comprehensive understanding of the current system is imperative, encompassing an analysis of its strengths, limitations, and functionalities. Stakeholder engagement is crucial for gathering insights into user needs and preferences.

The planning process revolves around delineating components or modules that align with the organization's unique requirements. This encompasses a strategic evaluation of how computers and technology can be optimally integrated to enhance overall efficiency. Collaboration and communication with stakeholders remain central to ensuring the proposed system aligns with organizational goals.

In summary, business system analysis is a holistic approach that combines a profound understanding of the existing system, stakeholder engagement, and strategic planning to create a tailored and efficient business system. The objective is to drive innovation, enhance operational effectiveness, and position the organization for sustained success in the dynamic business landscape.

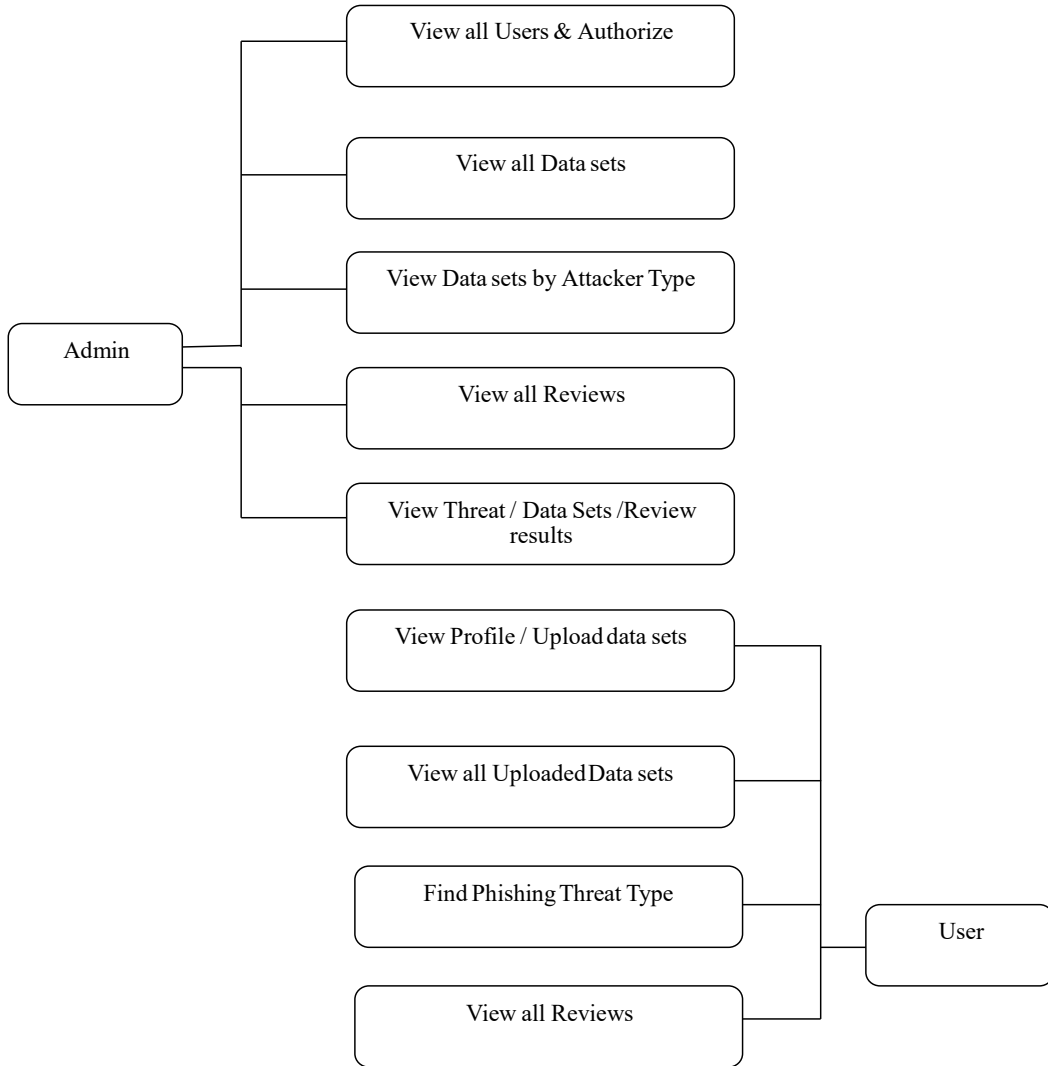
ARCHITECTURE DIAGRAM



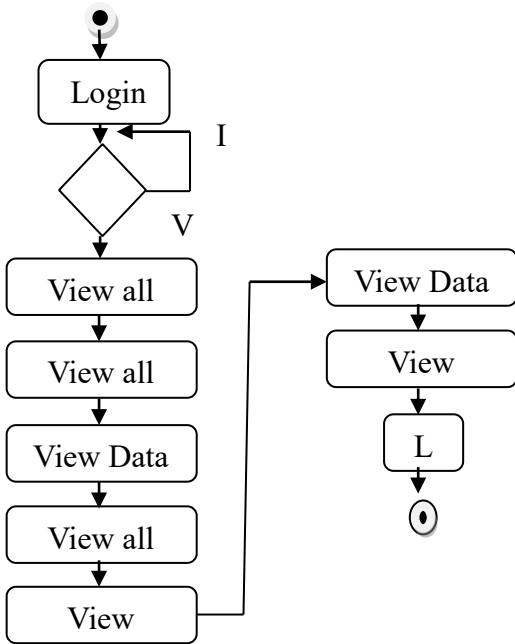


DATA FLOW DIAGRAM

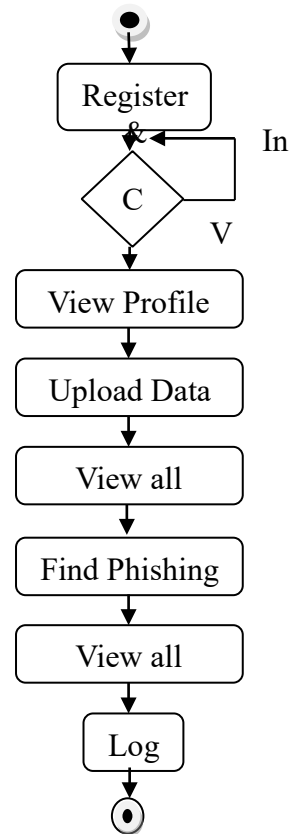
A data flow diagram (DFD) maps out the flow of information for any process or system. It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination. Data flowcharts can range from simple, even hand-drawn process overviews, to in-depth, multi-level DFDs that dig progressively deeper into how the data is handled. They can be used to analyse an existing system or model a new one.



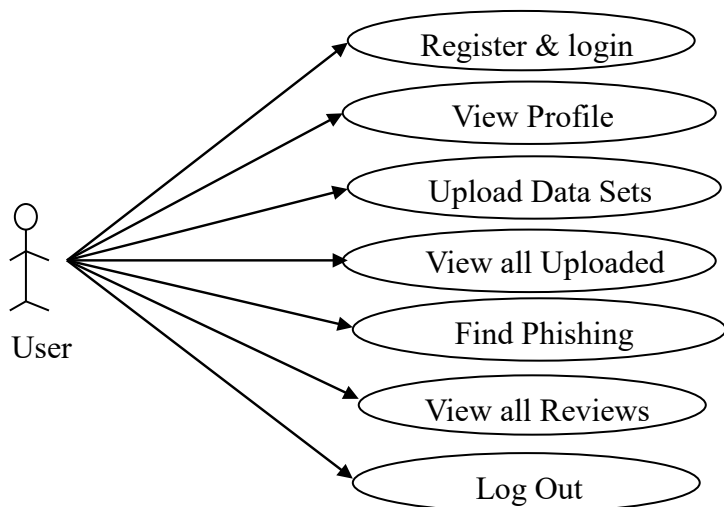
Activity diagram for Admin



Activity diagram for User



Use case diagram



VII. REQUIREMENT ANALYSIS

The hardware specifications for the system consist of an Intel (R) Core (TM) i3-4200U processor operating at 1.6GHz, 4 GB RAM, and a 500 GB hard disk. On the software side, the system runs on the Windows 10 operating system, employs Apache Tomcat as the server, and utilizes MYSQL Server 5.0 for database management. For frontend development, HTML, CSS, and JavaScript are employed, while the backend is implemented using Java Server Pages (JSP). The Integrated Development Environment (IDE) chosen for this system is Notepad++, offering a comprehensive and functional platform for development and execution. This amalgamation of hardware and software components establishes a robust foundation for the effective implementation and operation of the system.

VIII. HOW THE MECHANISM IS HELPFUL

1. **Feature Fusion:** By integrating data from various modalities such as text and images, this mechanism creates a more comprehensive view of phishing website attributes, thereby enhancing the model's ability to identify subtle indicators of phishing.
2. **Selective Attention:** Through hierarchical attention, the model can concentrate on pertinent features across different levels of detail. This selective focus enables prioritization of relevant information while disregarding irrelevant or noisy input, thereby enhancing the model's ability to differentiate between legitimate and malicious websites.
3. **Contextual Understanding:** The dynamic adjustment of attention weights enables the model to understand the context of phishing indicators within webpage content and structure. This contextual comprehension improves the model's interpretability and its capability to distinguish between benign and harmful websites.
4. **Robustness:** By identifying and filtering out irrelevant or adversarial features introduced by attackers, the attention mechanism enhances the model's resilience against evasion techniques commonly used by phishing websites, making it more resistant to sophisticated attacks.
5. **Efficiency:** The attention mechanism optimizes computational resources by focusing on salient features, thereby enhancing inference speed and reducing computational overhead. This improvement in efficiency is crucial for realtime applications and scalability.
6. **Generalization:** The mechanism facilitates learning from diverse datasets and adapts to evolving phishing tactics. By attending to relevant features across different modalities and levels of abstraction, the model can generalize well to new phishing scenarios, thereby improving its effectiveness in real-world settings.

IX. CONCLUSION AND FUTURE WORK

The multi-modal capability of EMMHAM enables it to analyse a wide array of data types, including text, images, and potentially other modalities, thereby offering a comprehensive insight into phishing attacks. The inclusion of a hierarchical attention mechanism allows the model to concentrate on pertinent information across various levels, capturing both global and local patterns within the dataset. This not only enhances the accuracy of the model but also promotes interpretability by spotlighting essential features that influence the decision-making process. One of the notable strengths of EMMHAM is its emphasis on explainability, addressing the inherent opacity of many deep learning models. The significance of interpreting and comprehending the decision-making process cannot be overstated for cybersecurity professionals and analysts, fostering trust and informed decision-making based on the model's outcomes. The hierarchical attention mechanism plays a crucial role in offering insights into the primary features or modalities that significantly contribute to the final prediction, empowering users to grasp the rationale behind the model's decisions.

ACKNOWLEDGMENT

The authors extend heartfelt appreciation to the collaborative efforts and valuable insights contributed by the research team. Each member's dedicated work has played a pivotal role in shaping the conclusions of this study. Special thanks go to the team for their diverse expertise, fostering a comprehensive understanding of the subject matter. This acknowledgment reflects gratitude not only for individual contributions but also for the collective synergy that

characterized the team's interactions. The collaborative environment, encouraging open dialogue and shared insights, has been integral to refining ideas and influencing the outcomes of this study.

In summary, the authors express deep appreciation for the commitment, dedication, and intellectual contributions of the entire research team, enhancing both the quality of this study and the broader field of knowledge.

REFERENCES

1. B. Barth, "SOC teams spend nearly a quarter of their day handling suspicious emails." Accessed: Feb. 3, 2021. [Online]. Available: <https://www.scmagazine.com/home/email-security/soc-teams-spendnearly-a-quarter-of-their-dayhandling-suspicious-emails>
2. C. Hassold, "Employee-reported phishing attacks climb 65%, clob bering SOC teams." Accessed: Aug. 25, 2020. [Online]. Available: <https://www.agari.com/email-security-blog/employee-reported-phishing-attacks-soc/>
3. C. N. Gutierrez et al., "Learning from the ones that got away: Detecting new forms of phishing attacks," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 6, pp. 988–1001, Nov./Dec. 2018.
4. M. A. Adebowale, K. T. Lwin, and M. A. Hossain, "Deep learning with convolutional neural network and long short-term memory for phishing detection," in *Proc. 13th Int. Conf. Softw. Knowl. Inf. Manage. Appl.*, 2019, pp. 1–8. [5] Anti-Phishing Working Group, "Phishing activity trends report Q2 2020." Accessed: Aug. 27, 2020. [Online]. Available: www.apwg.org
6. [6] X. Xiao, D. Zhang, G. Hu, Y. Jiang, and S. Xia, "CNN-MHSA: A convolutional neural network and multi-head self-attention com bined approach for detecting phishing websites," *Neural Netw.*, vol. 125, pp. 303–312, 2020, doi: 10.1016/j.neunet.2020.02.013. [7] ENISA threat landscape," European Union Agency for Network and Information Security, Athens, Greece, Tech. Rep., 2020. 802 *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, VOL. 19, NO. 2, MARCH/APRIL 2022
8. H. Yuan, Z. Yang, X. Chen, Y. Li, and W. Liu, "URL2Vec : URL modeling with character embeddings for fast and accurate phishing website detection," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl. Ubiquitous Comput. Commun. Big Data Cloud Comput. Social Comput. Netw. Sustain. Comput. Commun.*, 2018, pp. 265–272, doi: 10.1109/BDCloud.2018.00050.
11. F. Feng, X. He, J. Tang, and T. -S. Chua, "Graph adversarial train ing: Dynamically regularizing based on graph structure," *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 6, pp. 2493–2504, Jun. 2021.
12. M. A. Adebowale, K. T. Lwin, and M. A. Hossain, "Intelligent phish ing detection scheme using deep learning algorithms scheme," *J. Enterp. Inf. Manag.*, to be published, doi: 10.1108/JEIM-01-2020-0036.
13. S. Sountharajan, M. Nivashini, S. K. Shandilya, E. Suganya, A. B. Banu, and M. Karthiga, "Dynamic recognition of phishing URLs using deep learning techniques," in *Proc. Conf. Cyber Secur. Anal. Decis. Syst.*, 2020, pp. 27–56, doi: 10.1007/978-3-030-19353-9.
14. P. Yang, G. Zhao, and P. Zeng, "Phishing website detection based on multidimensional features driven by deep learning," *IEEE Access*, vol. 7, pp. 15196–15209, 2019.



INNO  **SPACE**
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 **9940 572 462**  **6381 907 438**  **ijircce@gmail.com**



www.ijircce.com

Scan to save the contact details