**Critique Papers on Information Assurance and Security Research Articles**

**Limpangog, Anna Rose G.**

Third Year – BSIT

January 11, 2023

**"A Survey on Security and Privacy Issues in Internet-of-Things"**

Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao

The research "A Survey on Security and Privacy Issues in Internet-of-Things" discusses the security and privacy challenges posed by the Internet of Things (IoT) and surveys various approaches that have been proposed to address these issues. The authors argue that the Internet of Things has the potential to revolutionize various aspects of our lives, but the security and privacy risks associated with it must be carefully managed.

The main findings of the research are that security and privacy are critical issues in the IoT and that various approaches have been proposed to address these issues. The authors classify these approaches into three categories: technical solutions, security protocols, and security and privacy frameworks. They also discuss the challenges and limitations of each approach and provide a summary of the research on the effectiveness of these approaches.

One of the strengths of this research is that it provides a comprehensive overview of the security and privacy issues in the IoT, and surveys a wide range of approaches that have been proposed to address these issues. The authors also do a good job of discussing the challenges and limitations of each approach, which helps to provide a balanced view of their effectiveness. Additionally, the research is well-written and clearly structured, which makes it easy to understand and follow. On the other hand, one potential weakness of this research is that it focuses primarily on the security and privacy issues in the IoT, and does not consider other factors that may also be relevant, such as technological or organizational factors. Moreover, the authors do not provide a detailed analysis of the empirical evidence on the effectiveness of the various approaches discussed in the research, which could be useful for practitioners seeking to implement these approaches in real-world settings.

The research has implications for both practitioners and researchers working in the field of IoT. For practitioners, the research provides a useful overview of the different approaches that have been proposed to address the security and privacy issues in IoT systems and can help to inform the development of effective security and privacy strategies and technologies. For researchers, the research highlights areas where further research is needed, such as the effectiveness of different approaches in real-world settings, and the role of other factors beyond security and privacy in the IoT.

Overall, the research "A Survey on Security and Privacy Issues in Internet-of-Things" is a valuable resource for practitioners and researchers working in the field of IoT. It provides a useful overview of the security and privacy issues in the Internet of Things (IoT) and surveys a range of approaches that have been proposed to address these issues. While there are some limitations to the scope of the research, the authors do a good job of discussing the challenges and limitations of each approach, and the research is well-written and clearly structured.

**"Phishing website prediction using base and ensemble classifier techniques with cross-validation"**

Anjaneya Awasthi and Noopur Goel

The research “Phishing website prediction using base and ensemble classifier techniques with cross-validation” aims to address an important problem in the field of cybersecurity: the ability to predict and prevent phishing attacks. The authors propose using a combination of base classifier techniques (such as support vector machines and k-nearest neighbors) and ensemble classifier techniques (such as bagging and boosting) to improve the accuracy of phishing website prediction. The use of cross-validation is also described as a means of evaluating the performance of the proposed methods.

The main findings of the research are that it is possible to develop a machine learning algorithm for predicting phishing websites using base and ensemble classifier techniques, and that cross-validation can be used to improve the accuracy of the model. The authors demonstrate the effectiveness of their approach using a dataset of phishing and legitimate websites and compare the performance of different classifier techniques. They also discuss the limitations of their approach, including the need for a large and diverse dataset to achieve good results.

One of the strengths of this research is that it provides a thorough overview of the various classifier techniques that were tested, as well as a detailed description of the dataset used in the experiments. The use of cross-validation is also a strength, as it helps to improve the reliability of the results and reduce the risk of overfitting. Additionally, the authors provide a detailed analysis of the results, which helps to understand the underlying factors that contribute to the performance of the different techniques. However, there are a few areas in which the paper could be improved. First, it would be helpful to have a more in-depth discussion of the results of the experiments. While the authors do provide some summary statistics and graphs, it would be useful to have more detailed information on the performance of the different classifiers, particularly in terms of false positive and false negative rates. Also, a more thorough review of the literature would provide a stronger foundation for the proposed methods and help to contextualize the contribution of the current work.

The research has implications for both practitioners and researchers working in the field of cybersecurity. For practitioners, the research provides a valuable tool for predicting phishing websites, which can help to mitigate the impact of these attacks. For researchers, the research highlights the importance of using base and ensemble classifier techniques and cross-validation to improve the accuracy of machine learning algorithms and suggests areas where further research is needed, such as the generalizability of the approach to other types of phishing attacks or other domains.

Overall, the research "Phishing website prediction using base and ensemble classifier techniques with cross-validation" is a promising approach to predicting and preventing phishing attacks. It provides an evaluation of the effectiveness of different classifier techniques for predicting phishing websites and demonstrates the usefulness of cross-validation to improve the accuracy of the model. However, more detailed results and a more comprehensive review of related work would strengthen the paper and further advance the field.

**SOURCES**

Awasthi, A., & Goel, N. (2022, November 2). *Phishing website prediction using base and ensemble classifier techniques with cross-validation*. SpringerOpen. Retrieved January 6, 2023, from <https://cybersecurity.springeropen.com/articles/10.1186/s42400-022-00126-9>

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017, April 17). *A Survey on Security and Privacy Issues in Internet-of-Things*. Research Gate. Retrieved January 6, 2023, from <https://www.researchgate.net/publication/316173391_A_Survey_on_Security_and_Privacy_Issues_in_Internet-of-Things>