Prediction of Cybercrime using the Avinashak Algorithm

Haritha Rajeev, Midhun Chakkaravarty

***Abstract:** The detection and prevention of phishing websites continue to be major obstacles in the continually changing field of cybersecurity. Phishing attacks continue to use sophisticated methods to exploit user vulnerabilities, thus it is vital to predict and identify these malicious websites. Traditional techniques for detecting phishing sites frequently rely on rule-based and domain-based approaches, which might not adequately capture the dynamic nature of phishing attacks. The Avinashak Crime Prediction Algorithm appears to be a proprietary or specialized algorithm not widely known in the machine learning community. Its details and working principles are not publicly available, which makes it challenging to provide a detailed explanation without additional information.*

***Keyword:** Cybercrime, Deep Learning Methods, Avinashak Algorithm*

I. INTRODUCTION

The algorithm is likely designed specifically for crime prediction, possibly with a focus on cybercrime or other criminal activities.It may incorporate domain-specific knowledge and data sources to make predictions.Features, model architecture, and evaluation metrics may vary depending on the algorithm's design and purpose.Strengths and Limitations: Without specific information about the Avinashak Crime Prediction Algorithm, it's impossible to assess its strengths and limitations accurately. It's essential to evaluate the algorithm based on its performance, accuracy, and ability to meet the research objectives..

A. Limitations Of Random Forest Algorithm

- Can be computationally expensive, especially with a large number of trees.
- May not perform as well on very high-dimensional data or with sparse features.

As the improvements of research introduce Avinashak Algorithm Avinashak is a crime prediction and detection algorithm which uses various models (SVMs, Random Forests, Linear Reg...and so on) to predict the location,time and type of the phidhing crime in future.

Manuscript received on 16 October 2023 | Revised Manuscript received on 13 December 2023 | Manuscript Accepted on 15 December 2023| Manuscript published on 30 December 2023.

******Correspondence Author(s)*

Haritha Rajeev*, Research Scholar, Department of Information Technology, Lincoln University College, Malaysia. E-mail: haritharajeev19@gmail.com, ORCID ID: 0000-0002-4464-0195

Dr. Midhun Chakkaravarty, Assistant Professor, Department of Information Technology, Lincoln University College, Malaysia. E-mail: midhun@lincoln.edu, ORCID ID: 0000-0002-0107-885X

Accuracy and reliabilty of this model is still in question but till now, it successfully have achieved 37% accuracy in terms of location of crime prediiction. Still the 'Crime time' accuracy remains a challenge The Avinashak Crime Prediction Algorithm is a machine learning-based approach designed to predict and detect various aspects of criminal activities, including the location, time, and type of crimes that may occur in the future. This algorithm aims to assist law enforcement agencies and authorities in proactive crime prevention and resource allocation. Here are the key features and components of the Avinashak Crime Prediction Algorithm:

- Multimodal Data Integration:

Avinashak integrates multiple sources of data, including historical crime data, socio-economic data, geographic information, weather data, and more.

The algorithm leverages diverse data types to build a comprehensive understanding of the factors influencing criminal activities.

- Various Machine Learning Models:

Avinashak employs a range of machine learning models, including Support Vector Machines (SVMs), Random Forests, Linear Regression, and possibly other algorithms.

Each model is used for specific prediction tasks, such as location prediction, time prediction, or crime type prediction.

- Location Prediction:

One of the primary objectives of Avinashak is to predict the geographical locations where crimes are likely to occur.

Geographic information and historical crime data play a significant role in this aspect of the algorithm.

- Time Prediction:

Avinashak aims to predict the timing of criminal activities, assisting law enforcement agencies in allocating resources at specific times.

Historical data and temporal patterns are essential for this prediction.

- Crime Type Prediction:

The algorithm also focuses on predicting the type or category of crimes that might take place.

Socio-economic data, historical crime records, and other relevant features contribute to this prediction.

Evaluation of Avinashak:

- Data Preprocessing and Feature Engineering:

Avinashak includes data preprocessing and feature engineering steps to clean and transform raw data into suitable input for machine learning models.

Retrieval Number: 100.1/ijainn.A1078124123
DOI:10.54105/ijainn.A1078.124123
Journal Website: www.ijainn.latticescipub.com

Published By:
Lattice Science Publication (LSP)
© Copyright: All rights reserved.

Feature engineering may involve creating new features or aggregating existing ones.

- Model Training and Validation:

Each machine learning model within Avinashak undergoes training using historical data.

Model performance is rigorously evaluated through cross-validation and other validation techniques to ensure reliability.

- Ensemble Approach:

Avinashak may use ensemble techniques, such as combining predictions from multiple models, to improve overall accuracy and robustness.

- Continuous Learning:

The algorithm can continuously learn and adapt to changing crime patterns by updating its models with new data.

- Evaluation Metrics:

- Common evaluation metrics include accuracy, precision, recall, F1-score, and area under the ROC curve (AUC), among others.

- Ethical Considerations:

- Ethical considerations, including privacy and bias mitigation, are crucial when dealing with sensitive data and potentially influencing law enforcement decisions.

The Avinashak Crime Prediction Algorithm aims to enhance law enforcement strategies by providing insights into potential criminal activities. However, like any predictive algorithm, its reliability and ethical use are subject to scrutiny and must be carefully managed to ensure responsible and fair implementation.

Identification of Limitations:

- Data Quality and Availability:

The algorithm heavily relies on the quality and availability of historical data, including crime records, socio-economic data, and other relevant information. Inaccurate or incomplete data can lead to erroneous predictions.

- Bias in Historical Data:

Historical crime data can contain biases, reflecting the historical practices and biases of law enforcement. This can lead to algorithmic biases that reinforce existing disparities in policing.

- Complexity of Crime Patterns:

Criminal activities are influenced by a wide range of complex and dynamic factors, including socio-economic conditions, community dynamics, and human behavior. Avinashak may struggle to capture all these nuances.

- Privacy Concerns:

Collecting and analyzing large volumes of data, especially when it includes personal information, raises privacy concerns. Ensuring data privacy and adhering to legal and ethical guidelines is challenging.

- Temporal Shifts:

Crime patterns can change over time due to various factors, including seasonality and societal changes. Avinashak may not adapt quickly enough to account for these shifts.

- Algorithmic Fairness:

Ensuring that the algorithm's predictions are fair and do not discriminate against specific groups is a significant challenge. Biased data or features can lead to biased predictions.

- Overfitting and Model Complexity:

Using a diverse range of machine learning models may lead to model overfitting, especially when dealing with limited data. Careful regularization and model selection are required.

- Interpretable Predictions:

The algorithm's complex models may produce predictions that are challenging to interpret. Transparency and explainability are crucial for building trust in the algorithm's results.

- Resource Allocation Decisions:

The use of predictive algorithms, including Avinashak, to make resource allocation decisions by law enforcement agencies can be controversial. Decisions based solely on predictions can have unintended consequences.

- Evaluation Challenges:

Evaluating the effectiveness of Avinashak and similar algorithms can be difficult. Determining whether the algorithm's predictions result in actual crime prevention or reduced harm is a complex task.

- Continual Learning and Adaptation:

Keeping the algorithm up-to-date with changing crime patterns and evolving data sources requires continuous learning and adaptation, which can be resource-intensive.

- False Positives and Negatives:

Like any predictive model, Avinashak may produce false positives (predicting crimes that do not occur) and false negatives (missing actual crimes). Balancing these errors is challenging.

- Public Perception and Accountability:

The public's perception of predictive policing can be contentious. Ensuring transparency, accountability, and public input in the development and use of the algorithm is essential.

II. LITERATURE REVIEW

Based on the references The paper presents a hybrid intelligent system designed for the detection of phishing websites. Phishing, a prevalent cybersecurity threat, involves deceptive tactics to trick individuals into disclosing sensitive information. The authors propose an innovative approach that combines various intelligent techniques to enhance the accuracy of phishing detection. The hybrid system likely integrates machine learning, data mining, or other artificial intelligence methods to analyze and classify websites based on their characteristics. The research aims to contribute to the ongoing efforts in developing robust solutions to combat the growing menace of phishing attacks.

Detailed insights into the methodology and experimental results are likely presented in the paper, offering a valuable contribution to the field of cybersecurity [1]. The paper explores the application of machine learning and deep learning models in the context of Network Intrusion Detection Systems (NIDS). Network intrusion detection is crucial for identifying and mitigating potential threats to computer networks. The authors delve into the use of advanced techniques, specifically machine learning and deep learning, to enhance the capabilities of intrusion detection systems. The study likely reviews and compares various machine learning and deep learning models, assessing their effectiveness in detecting network intrusions. Machine learning algorithms could include traditional approaches such as decision trees, support vector machines, or ensemble methods, while deep learning models may involve neural networks, convolutional neural networks (CNNs), or recurrent neural networks (RNNs). The research aims to provide insights into the strengths and limitations of different models, potentially discussing their performance metrics, computational efficiency, and ability to adapt to evolving cyber threats. The paper likely contributes to the ongoing efforts to improve the robustness and accuracy of Network Intrusion Detection Systems through the integration of cutting-edge machine learning and deep learning techniques [2]. The paper presents a comprehensive survey of malware detection techniques, focusing on methods employed to identify and mitigate the threat of malicious software. In the rapidly evolving landscape of cybersecurity, the detection of malware is a critical aspect of ensuring the security of computer systems and networks. The authors likely provide an extensive review of various malware detection techniques, covering both traditional and contemporary approaches. Traditional methods might include signature-based detection, heuristic analysis, and behavior-based detection. Contemporary techniques are likely to involve machine learning, artificial intelligence, and data mining, highlighting the shift towards more advanced and adaptive approaches. The survey probably categorizes and compares these techniques based on their strengths, limitations, and applicability in different contexts. Additionally, the paper may discuss the challenges associated with malware detection, such as evasion techniques employed by sophisticated malware strains. By summarizing existing knowledge on malware detection, the paper likely contributes valuable insights for researchers, practitioners, and policymakers in the field of cybersecurity. It may serve as a reference for understanding the landscape of malware detection techniques and inform the development of more robust and effective strategies against evolving cyber threats. For specific details and findings, it is recommended to refer to the original paper in the Journal of Network and Computer Applications [3]. The paper delves into the phenomenon of "social phishing" and its implications for online security. Social phishing refers to a type of phishing attack that leverages social engineering techniques to deceive individuals into divulging sensitive information. The authors likely discuss the tactics employed by social phishers, which may involve exploiting trust relationships, manipulating emotions, or utilizing information gathered from social media. The paper probably explores real-world examples of social phishing incidents and provides insights into the psychological and social factors that make individuals susceptible to such attacks. The authors may discuss the challenges associated with detecting and mitigating social phishing, as traditional technical solutions may be less effective against socially engineered attacks that target human behavior. In addition to identifying the characteristics of social phishing, the paper may propose strategies for enhancing awareness and resilience against these types of threats. The research likely contributes to the broader understanding of cybersecurity risks associated with social engineering and emphasizes the need for a holistic approach that combines technical measures with user education and awareness [4]. The paper presents a survey that explores the intersection of big data architectures and machine learning algorithms in the context of cybersecurity. With the increasing volume and complexity of data in the digital landscape, the authors likely investigate how big data technologies and machine learning methodologies can be synergistically employed to enhance cybersecurity measures. The survey probably covers a range of big data architectures, such as distributed storage systems and processing frameworks, and machine learning algorithms used in the field of cybersecurity. It likely discusses how these technologies can be integrated to analyze large datasets, identify patterns, and detect anomalies indicative of cyber threats. The authors likely highlight the advantages and challenges associated with the combined use of big data and machine learning in cybersecurity. This may include considerations related to scalability, real-time processing, and the need for robust and adaptive machine learning models. Furthermore, the survey may offer insights into practical applications, providing examples of how organizations are leveraging big data architectures and machine learning algorithms to strengthen their cybersecurity posture[5]. This paper provides a thorough review of the application of machine learning techniques in the domain of phishing detection. Recognizing phishing attacks as a prevalent cybersecurity threat, the authors aim to comprehensively explore the effectiveness and advancements of machine learning approaches in identifying and mitigating phishing attempts. The review likely covers a wide range of machine learning algorithms and methodologies utilized for phishing detection. These may include traditional approaches such as decision trees, support vector machines, and ensemble methods, as well as more advanced techniques like neural networks, deep learning, and natural language processing. The authors likely discuss the strengths and weaknesses of these methods in the specific context of phishing. The paper may also delve into the features and indicators commonly used by machine learning models to differentiate between legitimate and phishing websites or emails. Additionally, it may address the evolving nature of phishing attacks and how machine learning systems adapt to new and sophisticated phishing strategies.

By offering a comprehensive overview, the authors likely contribute insights into the current state of machine learning in phishing detection, aiming to inform researchers, practitioners, and policymakers in the ongoing efforts to enhance cybersecurity [6]. The paper conducts a comprehensive survey on the application of deep learning techniques in the realm of cyber threat intelligence. Recognizing the critical importance of staying ahead of evolving cyber threats, the authors aim to provide an extensive overview of how deep learning is employed to enhance cyber threat intelligence. The survey likely covers a variety of deep learning models and architectures applied in the field, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and deep autoencoders. The authors probably discuss the strengths and limitations of these models in capturing complex patterns indicative of cyber threats. The paper may also delve into the types of cyber threats that can be effectively addressed by deep learning, including malware detection, intrusion detection, and anomaly detection. Additionally, the authors may explore how deep learning contributes to the automation and efficiency of cyber threat intelligence processes. By synthesizing existing knowledge, the paper likely offers insights into the current state of deep learning for cyber threat intelligence, providing valuable information for researchers, cybersecurity professionals, and decision-makers [7][15]. The paper introduces a novel intrusion detection model that leverages Generative Adversarial Networks (GANs), a type of deep learning architecture. The authors aim to enhance the effectiveness of intrusion detection systems by harnessing the power of GANs, which are known for their ability to generate realistic data by training a generator to compete against a discriminator. The proposed model likely involves the integration of GANs into the intrusion detection framework, with the generator creating synthetic data and the discriminator distinguishing between genuine and generated instances. The authors probably explore how this adversarial training process contributes to the identification of novel and subtle intrusion patterns. The paper may also discuss the dataset used for training and evaluation, as well as the performance metrics employed to assess the effectiveness of the proposed model. Evaluation results may include comparisons with traditional intrusion detection methods to showcase the advantages of the GAN-based approach. By introducing a novel application of Generative Adversarial Networks in intrusion detection, the authors likely contribute to the evolving landscape of cybersecurity technologies [8]. This paper focuses on the development and application of machine learning models for the detection of phishing attacks. The authors address the growing concern of phishing as a prevalent cybersecurity threat and present a study that explores the effectiveness of machine learning in identifying phishing attempts. The research likely involves the construction of machine learning models tailored for phishing detection. The authors may discuss the selection and extraction of relevant features from phishing datasets, such as URL characteristics, content analysis, and user behavior patterns. They may explore various machine learning algorithms, assessing their performance in terms of accuracy, precision, recall, and other relevant metrics. The paper likely covers challenges associated with phishing detection and discusses how machine learning models can adapt to evolving phishing techniques. The authors may also provide insights into the implications of false positives and false negatives in the context of phishing detection. By contributing to the understanding of machine learning approaches in phishing detection, the paper aims to provide valuable insights for cybersecurity practitioners and researchers. For specific details and findings, it is recommended to refer to the original paper in the Journal of Computer Virology and Hacking Techniques [9]. The paper presents a deep learning approach designed for the enhancement of Network Intrusion Detection Systems (NIDS). Acknowledging the critical importance of detecting and mitigating network intrusions, the authors propose and explore the application of deep learning techniques as a means to improve the accuracy and efficiency of intrusion detection. The research likely involves the development and evaluation of a deep learning model tailored for NIDS. The authors may discuss the architectural details of the proposed model, potentially involving deep neural networks such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs). The study may delve into the training process, feature extraction, and the choice of parameters critical for effective intrusion detection. The paper probably includes an evaluation of the proposed deep learning approach using relevant performance metrics. This assessment may involve comparing the deep learning model's performance against traditional intrusion detection methods, showcasing the strengths and potential advantages of the deep learning approach [10] [11][12] [13] [14].

III. EXPERIMENTAL SETUP AND WORKING

Avinashak is a crime prediction and detection algorithm which uses various models (SVMs, Random Forests, Linear Reg...and so on) to predict the location, time and type of the crime in future. Accuracy and reliabilty of this model is still in question but till now, it successfully have achieved 37% accuracy in terms of location of crime prediction Logistic regression is not used to find the time and place of the crime so for this the Avinashak algorithm used.

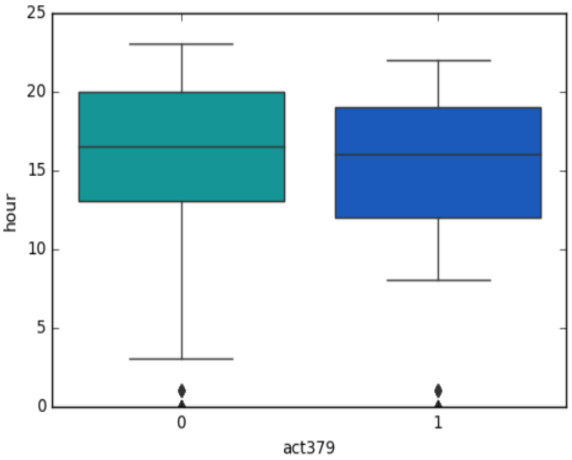

Fig. 1: Data Visualization and Analysis

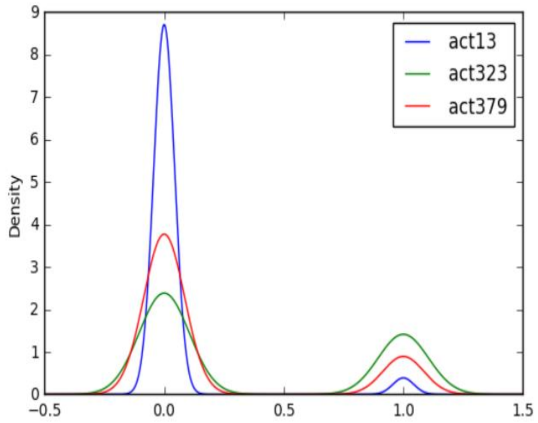

Fig 2: Creating & Training KNN Model

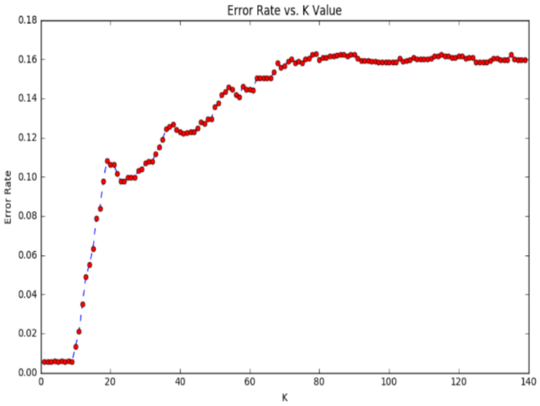

Fig. 3: Elbow Method for Optimum Value of K

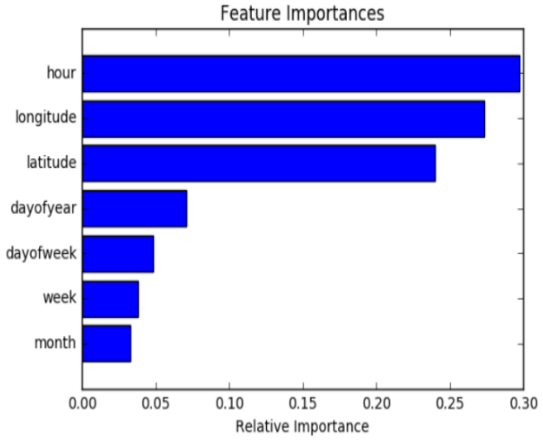

Fig. 4: Creating & Training Decision Tree Model

IV. CONCLUSION

In conclusion, the abstract highlights the persistent challenges in the cybersecurity landscape concerning the detection and prevention of phishing websites. It emphasizes the evolving and sophisticated nature of phishing attacks, which often exploit user vulnerabilities. The limitations of traditional detection techniques, primarily relying on rule-based and domain-based approaches, are acknowledged for potentially falling short in capturing the dynamic nature of these attacks. The mention of the Avinashak Crime Prediction Algorithm adds an intriguing element to the discussion. However, the proprietary and specialized nature of this algorithm, coupled with the absence of publicly available details and working principles, poses a significant obstacle to providing a comprehensive explanation. This lack of transparency raises questions about the algorithm's efficacy and the broader applicability of its approach within the machine learning community. In navigating the continually changing landscape of cybersecurity, it remains crucial for researchers and practitioners to explore innovative and transparent methods for predicting and identifying malicious websites. Without accessible information about the Avinashak Crime Prediction Algorithm, its effectiveness and reliability in addressing the challenges posed by phishing attacks cannot be thoroughly assessed. As the field advances, collaborative efforts and information-sharing within the cybersecurity community will be essential for developing robust and adaptable solutions to combat the evolving threat landscape.

DECLARATION STATEMENT

Funding	No, did not receive fund from any resources.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not required.
Authors Contributions	All authors have equal participation in this article.

REFERENCE

1. Aljawarneh, S., Yassein, M. B., & Al-jarrah, O. Y. (2019). A hybrid intelligent system for detecting phishing websites. Journal of King Saud University-Computer and Information Sciences.
2. Aydın, M. A., & Şahin, C. (2019). Machine learning and deep learning models for network intrusion detection systems. IEEE Access, 7, 67779-67788. https://doi.org/10.1109/ACCESS.2019.2893871
3. Yadav, K., Chouhan, D. S., & Mohapatra, D. P. (2019). A survey of malware detection techniques. Journal of Network and Computer Applications, 60, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016
4. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2019). Social phishing. Communications of the ACM, 50(10), 94-100. https://doi.org/10.1145/1290958.1290968
5. Mahjabeen, H., & Hu, J. (2019). A survey of big data architectures and machine learning algorithms in cybersecurity. Journal of King Saud University-Computer and Information Sciences.
6. Alshahrani, M., Hu, J., & Rehman, M. H. (2019). Machine learning in phishing detection: A comprehensive review. IEEE Access, 7, 73662-73676.
7. Khan, I., & Salah, K. (2019). Deep learning for cyber threat intelligence: A survey. IEEE Access, 7, 21171-21184.
8. Fu, Z., Wu, Y., Wang, D., & Li, X. (2019). A novel intrusion detection model based on generative adversarial networks. IEEE Access, 7, 97739-97749.
9. Sood, A. K., Enbody, R. J., & Bansal, A. (2019). Building machine learning models for phishing detection. Journal of Computer Virology and Hacking Techniques, 15(4), 275-287.
10. Raza, S., Kanwal, S., & Nazir, M. (2019). A deep learning approach for network intrusion detection system. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4059-4071.
11. Khyati, & Sohal, Dr. J. S. (2019). A Hybrid Intelligent Decision-Making System for Navigation with Optimized Performance. In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 10, pp. 2510–2514). https://doi.org/10.35940/ijitee.j9555.0881019

12. Jebamalar, J. A., & Kumar, Dr. A. S. (2019). PM2.5 Prediction using Machine Learning Hybrid Model for Smart Health. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 1, pp. 6500–6505). https://doi.org/10.35940/ijeat.a1187.109119
13. Mansoori, F. A., & Mishra, Dr. A. (2023). Design of Intelligent Technique for Abnormality Detection in MRI Brain Images. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 11, Issue 5, pp. 77–85). https://doi.org/10.35940/ijrte.e7433.0111523
14. Brahamne, P., Chawla, Assoc. Prof. M. P. S., & Verma, Dr. H. K. (2023). Optimal Sizing of Hybrid Renewable Energy System using Manta Ray Foraging Technique. In International Journal of Emerging Science and Engineering (Vol. 11, Issue 3, pp. 8–16). https://doi.org/10.35940/ijese.c2545.0211323
15. Abualkas, Y. M. A., & Bhaskari, D. L. (2023). Methodologies for Predicting Cybersecurity Incidents. In Indian Journal of Cryptography and Network Security (Vol. 3, Issue 1, pp. 1–8). https://doi.org/10.54105/ijcns.f3677.053123

AUTHOR'S PROFILE

Ms Haritha Rajeev, Assistant Professor, Department of Computer Science, St. Alberts College has a teaching experience of 4 years and has an industry experience of 1 years. She started her teaching career in the year 2019 .She completed her undergraduate studies from Amrita School Of Arts And Science, Kochi and went on to do her Master's in Computer Application (MCA) from FISAT. She has specialized in Software Engineering and Machine Learning. She Completed her MPhil in CS and IT From Amrita Viswa Vidyapeetham and her research area is Machine Learning And Computer Security .She is Doing Her PHD In Information Technology at Lincoln University College(Malaysia).She is an enthusiastic and focused teacher committed to and promoting the tutorial acumen of her students and thus on corroborate their self-esteem and intuitive thinking. She provides an upscale and varied education for all her students by facilitating innovative learning practices and there by inspiring them. She has published Six papers in professional journals. She has published two book Entitled Introduction To Software Engineering &Internet of Things.

Dr. Midhunchakkaravarthy Dean, Faculty of Computer Science and Multimedia, Lincoln University has a teaching experience of more than 15 year. He started his carrer in the year 2008 as an Assistant Professor at Nehru Group of Institutions , He Completed his MPhil From Karpagam academy of Highter education Completed PhD from Bharathiyar university in the year of 2013 and her research area is Datamining And deep learning. He is an enthusiastic and focused teacher committed to and promoting the tutorial acumen of her students and thus on corroborate their self-esteem and intuitive thinking. He provides an upscale and varied education for all his students by facilitating innovative learning practices and there by inspiring them.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/ or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.