ISAA 2

| **Paper Title** | **Authors** | **Year** | **Conference/Journal** | **Pros** | **Cons** |
| --- | --- | --- | --- | --- | --- |
| Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools | Tariq Mahmood, U. Afzal | 2013 | 2nd National Conference on Information Assurance (NCIA) | 1. In-depth survey of Security Analytics. 2. Recognition of the impact of Big Data on cybersecurity. 3. Emphasis on real-time monitoring and detection. | 1. Limited focus on specific tools and techniques. 2. Lacks detailed case studies or empirical validation. 3. Limited exploration of potential challenges in implementing Security Analytics. |
| A Comprehensive Survey on Big Data Technology Based Cybersecurity Analytics Systems | S. Saravanan, G. Prakash | 2021 | Lecture notes in networks and systems | 1. Comprehensive coverage of BDTCA systems. 2. Identification of key technologies and algorithms. 3. Exploration of methods for handling large packet captures. | 1. Limited discussion on specific implementation challenges. 2. Lacks empirical validation or case studies. 3. Could provide more insights into real-world applications of BDTCA systems. |
| A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks | Chuanlong Yin, Yuefei Zhu, Jin-long Fei, Xin-Zheng He | 2017 | IEEE Access | 1. Novel approach using recurrent neural networks (RNN) for intrusion detection. 2. Detailed exploration of model performance in binary and multiclass classification. 3. Comparative analysis with traditional machine learning methods. | 1. Limited discussion on the interpretability of the RNN-IDS model. 2. The paper could benefit from more in-depth analysis of the impact of hyperparameters. 3. Specifics on the benchmark dataset used are not extensively discussed. |
| Analysis of Intruder Detection in Big Data Analytics | K. Sudar, P. Nagaraj, P. Deepalakshmi, P. Chinnasamy | 2021 | International Conference on Computational Collective Intelligence | 1. Focus on network intrusion detection in big data analytics. 2. Overview of models using data mining, machine learning, and deep learning techniques. 3. Addresses the need for efficient schemes in handling big data and modeling user behavior. | 1. Limited discussion on specific models or techniques. 2. The paper could delve deeper into the evaluation of intrusion detection models. 3. More detailed analysis of real-world application scenarios could enhance the study. |
| An Encryption Enabled Metaheuristic Optimization-based Feed Forward Neural Network for Cloud-based Big Data Environment | A. S. Kumar, Dr. S C Mohan | (Missing Year) | (Missing Journal) | 1. Recognition of the exponential utilization of information resources and advancements in data analytics leading to increased use of big data. 2. Identification of security and privacy as major concerns, particularly in the healthcare sector, within cloud-based big data platforms. 3. Acknowledgment of the need for efficient models to handle big data, prompting attention from researchers. | 1. Focus on the growing utilization of information resources and data analytics advancements, leading to increased reliance on big data. 2. Recognition of security and privacy as critical concerns, especially in healthcare, within the context of cloud-based big data platforms. 3. Acknowledgment of the research community's attention to developing efficient models for handling big data challenges. |
| Applying Big Data Analytics Into Network Security: Challenges, Techniques and Outlooks | Caiyou Zhang, Xiaojun Shen, Xubin Pei, Yiyang Yao | 2016 | (Missing Journal) | 1. Comprehensive sketch of techniques about the applications of big data in network security analytics. 2. Classification of research works into supervised, unsupervised, and hybrid approaches. 3. Elaboration on technical issues and a comparison of their advantages and disadvantages. | 1. Lack of information about the specific journal. 2. Limited discussion on real-world application scenarios. 3. More detailed analysis of challenges could enhance the study. |
| A Review on Cyberattacks: Security Threats and Solution Techniques for Different Applications | Gaganjot Kaur Saini, Malka N. Halgamuge, Pallavi Sharma, James Stephen Purkis | 2019 | Advances in computer and electrical engineering book series | 1. Analysis of cybersecurity issues and solutions based on 31 peer-reviewed scientific research studies (2009-2017). 2. Identification of the majority of applications in government and the public sector. 3. Determination that the government sector is more susceptible to cyber-attacks. | 1. Lack of information about the specific journal. 2. Limited discussion on real-world application scenarios. 3. More detailed analysis of challenges could enhance the study. |
| A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection | A. Buczak, E. Guven | 2016 | IEEE Communications Surveys & Tutorials | 1. Focused literature survey of machine learning and data mining methods for cyber analytics in support of intrusion detection. 2. Short tutorial descriptions of each ML/DM method provided. 3. Summary of papers representing each method based on citations or relevance. 4. Description of well-known cyber datasets used in ML/DM. 5. Addressing the complexity of ML/DM algorithms and discussion of challenges in cyber security. | 1. The paper could provide more in-depth analysis of emerging ML/DM methods. 2. Additional discussion on practical implementation challenges could enhance the study. 3. More insights into real-world applications and case studies could be beneficial. |
| Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks | T. Yen, Alina Oprea, Kaan Onarlioglu, Todd Leetham, William K. Robertson, A. Juels, E. Kirda | 2013 | ACSAC | 1. Novel system (Beehive) for mining and extracting knowledge from dirty log data produced by various security products in large enterprises. 2. Improvement on signature-based approaches by identifying suspicious host behaviors. 3. Potential security incidents reported by Beehive for further analysis by incident response teams. 4. Evaluation on log data from a large enterprise |  |
| Big Data: Big Promises for Information Security | R. Alguliyev, Y. Imamverdiyev | 2014 | IEEE AICT | Exploration of Big Data technologies for information security, recognizing privacy issues, and proposing preventive strategies. | Limited discussion on specific applications, lacks depth on implementation challenges, and needs more insights into practical considerations. |
| Comparison Deep Learning Method to Traditional Methods for Network Intrusion Detection | Bo Dong, Xue Wang | 2016 | IEEE CSCN | Explores deep learning for intrusion detection, compares methods, and addresses the need for performance improvement. | Limited details on techniques, could provide deeper analysis of experimental results, and needs more discussion on challenges. |
| Context-Awareness for Adversarial and Defensive Machine Learning Methods in Cybersecurity | Kyle Quintal | 2020 | (Missing Journal) | 1. Exploration of combining machine learning with contextual information in cybersecurity. 2. Focus on context-aware attacker modeling and defensive methods. 3. Introduction of an attacker injection model (SINAM) and intelligent machine learning technique for mitigating anomalous behaviors. 4. Investigation of adopting similar defensive methodology in the cyber-physical domain. 5. Contributions in Mobile CrowdSensing, authentication methods improvement, and risk analysis using context. | 1. Lack of information about the specific journal. 2. Limited details on the implementation and evaluation of the introduced models and techniques. 3. The paper could provide more insights into real-world applications and case studies. |
| Data-Driven Security: Analysis, Visualization and Dashboards | Jay Jacobs, Bob Rudis | 2014 | (Missing Journal) | 1. Exploration of using data analysis and visualization for increased visibility in security. 2. Practical application for information security professionals. 3. Real-world examples and hands-on exercises demonstrating the analysis of security data and intelligence. | 1. Lack of information about the specific journal. 2. Limited details on the hands-on exercises and real-world examples provided. 3. The paper could delve deeper into the practical implementation and application of the discussed techniques. |
| Deep Learning Enabled Class Imbalance with Sand Piper Optimization Based Intrusion Detection for Secure Cyber-Physical Systems | Anwer Mustafa Hilal, Shaha Al-Otaibi, Hany Mahgoub, Fahd N. Al-Wesabi, Ghadah Aldehim, Abdelwahed Motwakel, Mohammed Rizwanullah, Ishfaq Yaseen | 2022 | (Missing Journal) | 1. Introduction of IGAN-OKELM technique for intrusion detection in Cyber-Physical Systems (CPS). 2. Addressing class imbalance using an imbalanced generative adversarial network (IGAN) with optimal kernel extreme learning machine (OKELM). 3. Integration of sand piper optimization (SPO) algorithm for optimal parameter tuning and improved intrusion detection performance. 4. Wide-ranging simulation analysis with benchmark datasets showcasing superior performance. | 1. Lack of information about the specific journal. 2. The paper could provide more details on the implementation and specific aspects of the simulation analysis. 3. More insights into the practical considerations and potential limitations would enhance the study. |
| Empirical Study on Multiclass Classification-Based Network Intrusion Detection | Wisam Elmasry, A. Akbulut, A. Zaim | 2019 | Computational Intelligence | 1. Comprehensive empirical study on network intrusion detection as a multiclass classification task. 2. Utilization of four deep learning models (deep neural networks, LSTM, GRU, and deep belief networks) with hyperparameter optimization. 3. Comparison with well-known shallow learning methods (decision forest and decision jungle). 4. Evaluation on four datasets (KDD CUP 99, NSL-KDD, CIDDS, and CICIDS2017) using 22 metrics. 5. Statistical analysis (Friedman test, ranking methods) showcasing significant improvement in detection performance. | 1. The paper could provide more details on the specific findings and insights gained from the extensive quantitative analysis. 2. Further discussion on the practical implications and potential challenges of implementing the recommended approach would enhance the study. 3. More information about the computational requirements and scalability of the proposed models would be beneficial. |
| Evolving Deep Learning Architectures for Network Intrusion Detection using a Double PSO Metaheuristic | Wisam Elmasry, Akhan Akbulut, Abdul Halim Zaim | 2020 | Computer Networks | 1. Introduction of a double Particle Swarm Optimization (PSO)-based algorithm for feature subset and hyperparameter selection. 2. Utilization of three deep learning models (DNN, LSTM-RNN, DBN) with automatic optimization in the pre-training phase. 3. Application and validation on two common IDS datasets with extensive evaluation metrics for both binary and multiclass classifications. 4. Significant improvement in network intrusion detection demonstrated through quantitative, Friedman test, and ranking methods analyses. | 1. The abstract provides a clear overview, but more details on the specific findings and insights would be beneficial. 2. Further discussion on the practical implications and potential challenges of implementing the proposed algorithm. 3. Additional insights into the computational requirements and scalability of the developed models would enhance the study. |
| Malware Detection in Cloud Computing Infrastructures | Michael R. Watson, Noor-ul-Hassan Shirazi, Angelos K. Marnerides, A. Mauthe, D. Hutchison | 2016 | IEEE Transactions on Dependable and Secure Computing | 1. Introduction of an online cloud anomaly detection approach for resilient cloud infrastructures. 2. Utilization of one-class Support Vector Machine (SVM) for novelty detection at the hypervisor level. 3. Demonstration of high detection accuracy (> |  |
| Method of Intrusion Detection using Deep Neural Network | Jin Kim, Nara Shin, S. Y. Jo, Sang Hyun Kim | 2017 | IEEE International Conference on Big Data and Smart Computing (BigComp) | 1. Investigation of an AI-based intrusion detection system using a deep neural network (DNN). 2. Testing conducted with the KDD Cup 99 dataset to address evolving network attacks. 3. Preprocessing steps, including data transformation and normalization, applied to prepare data for the DNN model. 4. DNN algorithm utilized to create a learning model, validated on the entire KDD Cup 99 dataset. 5. Evaluation metrics include accuracy, detection rate, and false alarm rate, demonstrating the effectiveness of the DNN model for intrusion detection. | 1. Further discussion on the specific architectural details of the deep neural network used in the intrusion detection system. 2. Insights into the adaptability of the proposed approach to different datasets or real-world network environments. 3. Consideration of potential challenges or limitations in deploying the DNN-based intrusion detection system in practical cybersecurity scenarios. |
| Malware Detection Kit for Malware Analysis of Big Data | T. Sree Lakshmi, M. Govindarajan, Asadi Sreenivasulu | 2021 | Learning and Analytics in Intelligent Systems | Introduces MDK for Big Data and IoT security, with effective static and dynamic analysis. Static analysis achieves high accuracy on Malgenome dataset. Utilizes automated sandboxes for dynamic analysis. Conducts two iterations of MDK for enhanced threat detection on new data. | Requires more detailed discussion on implementation and scalability in real-world environments. Exploration of potential challenges and limitations in static and dynamic analysis methods is needed. More insights into MDK's adaptability to evolving threats in the dynamic landscape are essential. |
| Performance Evaluation of Big Data Technology on Designing Big Network Traffic Data Analysis System | Nattawat Khamphakdee, N. Benjamas, Saiyan Saiyod | 2016 | Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS) | 1. Addressing the challenge of big network traffic data analysis faced by network and computer systems administrators. 2. Introduction of a Hadoop-based traffic querying and analyzing system designed for handling TCP, ICMP, and UDP analysis of large network traffic data. 3. System architecture composed of six modules: Data Collection, Transferring and Storing Information, Convertor, Data Mining Process, DM2SC, and Report. 4. Utilization of Hive, a data warehouse tool built on Hadoop, for storing, processing, querying, and analyzing large volumes of data. 5. Comparison of complex search queries and query response times between MySQL and Hive in the Hadoop environment. | 1. Further exploration of the specific challenges and intricacies involved in analyzing different types of network traffic protocols (TCP, ICMP, UDP). 2. In-depth analysis of the scalability and performance characteristics of the proposed system as the size of the Hadoop cluster increases. 3. Consideration of practical implications and recommendations for deploying big data technology in real-world network traffic analysis scenarios. |
| Phase II: CSDS Practitionersâ€”Diagnostic Opinion Research and Gap Analysis | Scott Mongeau, Andrzej Hajdasinski | 2021 | (missing journal) | 1. Exploration of cybersecurity data science (CSDS) as an emerging field in its early stages of professionalization. 2. Results of diagnostic background analysis asserting the need for the advancement of the CSDS body of theory. 3. Derivation of sensitizing concepts from literature analysis to provide a foundation for interview and gap analysis. 4. Summarization of key themes in CSDS literature. | 1. Development of CSDS theory to facilitate the professional emergence of the new domain. 2. Detailed exploration of sensitizing concepts derived from literature analysis. 3. Consideration of practical implications for the professionalization and advancement of CSDS. |
| Phase III: CSDS Gap-Prescriptionsâ€”Design Science Problem-Solving | Scott Mongeau, Andrzej Hajdasinski | 2021 | (missing journal) | 1. Presentation of the capstone phase in the research inquiry focused on Cybersecurity Data Science (CSDS). 2. Framing and advocating design-derived gap-prescriptions for CSDS. 3. Systematic exploration of CSDS through triangulated diagnostic methods. 4. Previous phases include practice-oriented diagnostic research: background analysis (Phase I), opinion research (Phase II), and gap analysis (Phase II). 5. Application of a design approach as a natural conclusion to diagnostic analysis in problem-solving research. | 1. In-depth exploration and understanding of the design-derived gap-prescriptions proposed for CSDS. 2. Evaluation of the effectiveness and practical applicability of the design-derived prescriptions in addressing identified gaps in CSDS. 3. Consideration of the broader implications and potential contributions of the proposed design-derived prescriptions to the field of Cybersecurity Data Science. |
| Real-time Big Data Processing for Anomaly Detection: A Survey | Riyaz Ahamed Ariyaluran Habeeb, Fariza Nasaruddin, Abdullah Gani, Ibrahim Abaker Targio Hashem, Ejaz Ahmed, Muhammad Imran | 2019 | International Journal of Information Management | 1. Investigation of challenges in network security analytics, focusing on real-time anomaly detection. 2. Recognition of limitations in existing approaches for real-time anomaly detection. 3. Proposal of a framework for effective real-time big data processing in anomaly detection. 4. Survey of state-of-the-art technologies for real-time big data processing and machine learning algorithms. 5. Exploration of essential contexts, taxonomy, and characteristics of real-time big data processing, anomalous detection, and machine learning algorithms. 6. Review of big data processing technologies relevant to real-time anomaly detection. 7. Discussion of research challenges in real-time big data processing for anomaly detection. | 1. In-depth understanding of challenges in real-time anomaly detection for network security analytics. 2. Evaluation of the proposed framework's effectiveness in handling real-time big data processing for anomaly detection. 3. Critical analysis of surveyed state-of-the-art technologies and machine learning algorithms for real-time anomaly detection. 4. Consideration of identified research challenges and potential solutions for improving real-time big data processing in anomaly detection. |
| Security Analytics: Dispelling the Fog | I. Birzniece | 2018 | BIR Workshops | 1. Examination of the implications of differing perspectives on security analytics in up-to-date literature. 2. Evaluation of the proposed classification model and its effectiveness in organizing research directions in security analytics. 3. Critical analysis of the three identified views to provide a nuanced understanding of security analytics. 4. Consideration of potential challenges and future directions in the field of security analytics. |  |
| Security Vulnerabilities, Threats, and Attacks in IoT and Big Data | Prabha Selvaraj, Sumathi Doraikannan, Vijay Kumar Burugari | 2020 | (Missing Journal) | 1. Evaluation of the effectiveness of big data in addressing security challenges in the IoT domain. 2. Critical examination of the proposed security techniques and their applicability in diverse areas. 3. Discussion on the practical implications and lessons learned from the presented case studies. 4. Consideration of future directions and emerging trends in addressing security concerns in the intersection of IoT and big data. |  |
| Spam and the Social-Technical Gap | B. Whitworth, E. Whitworth | 2004 | Computer | 1. Exploration of the evolving strategies employed by spammers in response to advancements in spam filters. 2. In-depth analysis of the limitations of traditional legal and judicial approaches in addressing spam-related challenges. 3. Discussion on specific social concepts and strategies that can be integrated into technology design to mitigate the spam problem. 4. Examination of the implications and potential effectiveness of a social response to spam in the context of technological design. |  |
| Survey of Security Advances in Smart Grid: A Data-Driven Approach | Song Tan, Debraj De, Wenzhan Song, Junjie Yang, Sajal K. Das | 2017 | IEEE Communications Surveys & Tutorials | 1. Detailed exploration of each stage in the lifecycle of smart grid data, providing insights into the security challenges and solutions at each step. 2. Systematic breakdown of security considerations in smart grid, facilitating a structured understanding of vulnerabilities and corresponding solutions. 3. Recognition of the significance of data analytics in addressing security concerns within the smart grid ecosystem. 4. Evaluation of the effectiveness of a data-driven approach in comprehensively surveying recent security advances in smart grid technology. 5. Identification of gaps and opportunities for future research endeavors aimed at enhancing smart grid security. |  |
| Survey Paper on Big Data based Isolation Security by Smartcard Authentication System | S. Panimalar | 2019 | International Journal for Research in Applied Science and Engineering Technology | 1. Comprehensive exploration of security challenges specific to big data and the potential implications for enterprise information security. 2. Proposal of a mutual authentication scheme based on a virtual smart card, leveraging hashing functions for enhanced security. 3. Addressing the issues of unlawful user access to big data servers and illegal access to legal cloud servers through innovative security approaches. 4. Introduction of file swapping techniques as a means to maintain user-sensitive information within big data, ensuring data privacy and protection. 5. Application of security measures to achieve strong countermeasures against cybercrime in the context of big data technology. |  |