ISAA papers

| **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. 4. Introduction of the Encryption Enabled Metaheuristic Optimization-based Feed Forward Neural Network (EEMO-FFNN) for cloud-based big data environments. 5. Intent of the EEMO-FFNN model to enable secure communication and effective big data analytics in healthcare. 6. Description of the EEMO-FFNN model's process, including patient data augmentation using SMOTE and secure data transmission using Elliptic Curve Cryptography (ECC). 7. Mention of the MO-FFNN model for data classification on the Hadoop ecosystem to identify the presence of diseases. 8. Application of the Salp Swarm Optimization (SSA) algorithm to adjust weight and bias parameters in the FFNN model. 9. Performance evaluation through an extensive set of simulations to validate the effectiveness of the EEMO-FFNN model. 10. Examination of results under different aspects to ensure the model's efficacy. | 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. 4. Introduction of the Encryption Enabled Metaheuristic Optimization-based Feed Forward Neural Network (EEMO-FFNN) tailored for cloud-based big data environments. 5. Aim of the EEMO-FFNN model to facilitate secure communication and effective big data analytics in healthcare settings. 6. Explanation of the EEMO-FFNN model's workflow, covering patient data augmentation using SMOTE and secure data transmission using Elliptic Curve Cryptography (ECC). 7. Reference to the MO-FFNN model for data classification within the Hadoop ecosystem to detect the presence of diseases. 8. Adoption of the Salp Swarm Optimization (SSA) algorithm to adjust weight and bias parameters in the FFNN model. 9. Rigorous performance evaluation through extensive simulations to validate the EEMO-FFNN model's effectiveness. 10. Critical examination of results from diverse perspectives to ensure the model's robustness. |  |
| 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. 4. Outlook on potentials and research directions in the future. | 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, EMC, demonstrating the identification of malicious events and policy violations. | 1. Limited information on the specific techniques employed by Beehive. 2. More detailed insights into the implementation and scalability of Beehive could enhance the study. 3. Further discussion on the challenges faced during the evaluation would be beneficial. |  |
| Big Data: Big Promises for Information Security | R. Alguliyev, Y. Imamverdiyev | 2014 | 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT) | 1. Exploration of Big Data technologies for collecting, processing, and analyzing large volumes of data for information security. 2. Recognition of critical information security and privacy problems posed by Big Data. 3. Identification of opportunities for preventing and detecting advanced cyber-attacks through Big Data analytics. 4. Analysis of applications and definition of research directions for Big Data analytics in security intelligence. | 1. Limited discussion on specific applications or case studies of Big Data in information security. 2. The paper could delve deeper into the challenges associated with implementing Big Data solutions. 3. More insights into practical considerations and potential limitations would enhance the study. |  |
| Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection | Bo Dong, Xue Wang | 2016 | IEEE International Conference on Communication Software and Networks | 1. Exploration of deep learning techniques for network intrusion detection in comparison to traditional methods. 2. Application of different methods on an open dataset to experiment and determine the best approach for intrusion detection. 3. Recognition of the need for improvement in detection performance and accuracy in intrusion detection. | 1. Limited details on the specific deep learning methods and traditional techniques compared. 2. The paper could provide more in-depth analysis of experimental results and their implications. 3. Further discussion on challenges and potential limitations would enhance the study. |  |
| 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 (>90%) against various types of malware and DoS attacks. 4. Evaluation of the effectiveness of considering system-level and network-level data based on attack types. 5. Application of dedicated monitoring components per VM for flexible detection of new malware strains without prior knowledge. | 1. More insights into the practical implementation and deployment challenges of the proposed anomaly detection approach. 2. Discussion on the scalability and resource requirements of the system in real-world cloud scenarios. 3. Exploration of potential limitations or constraints when detecting new malware strains with no prior knowledge. |  |
| Malware Detection Kit for Malware Analysis of Big Data | T. Sree Lakshmi, M. Govindarajan, Asadi Sreenivasulu | 2021 | Learning and Analytics in Intelligent Systems | 1. Introduction of Malware Detection Kit (MDK) for addressing security issues in Big Data and IoT. 2. MDK includes static and dynamic analysis methods for identifying attacks and threats. 3. Static analysis utilizes the Random Forest classifier, showing high accuracy and low error rate on the Malgenome dataset. 4. Dynamic analysis involves automated sandboxes to determine whether a file is benign or malware. 5. Two iterations of MDK to analyze new data entries for enhanced threat detection. | 1. More detailed discussion on the implementation aspects and scalability of MDK in real-world Big Data and IoT environments. 2. Exploration of potential challenges or limitations in the static and dynamic analysis methods used by MDK. 3. Insights into the adaptability of MDK to evolving malware and security threats in the dynamic landscape of Big Data and IoT. |  |
| 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. |  |
| 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. Exploration of the term "Security analytics" and its diverse perspectives in contemporary literature. 2. Literature analysis to identify the lack of a unified definition for security analytics and its boundaries. 3. Use of keywords "Security analytics" to select papers and books from notable digital libraries, providing insights into the concept. 4. Proposal of a classification of security analytics viewpoints, organizing research and practical applications in the field. 5. Introduction of three views: (a) Analytics of the security, focusing on cyber threat analysis. (b) Analytics for the security, addressing security issues beyond cyberspace. (c) Security of the analytics, considering threats in traditional or machine learning environments. 6. Contribution to building a common understanding of the multifaceted area known as "Security analytics." | 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. Exploration of the impact of big data and IoT on various domains such as science, health, engineering, medicine, finance, business, and society. 2. Recognition of the need for new security techniques leveraging big data and big data analytics. 3. Emphasis on IoT security encompassing not only device security but also considerations for web interfaces, cloud services, and interconnected devices. 4. Identification and discussion of challenges in security, particularly addressing privacy concerns, inference, and aggregation issues. 5. Examination of the potential risks of insecure web interfaces resulting from certain security vulnerabilities. 6. Analysis of how big data can be utilized to address security challenges in the context of IoT. 7. In-depth exploration of various attacks and threat modeling relevant to the IoT and big data landscape. 8. Presentation of two case studies in different areas to illustrate practical implications and solutions. | 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. Recognition of the challenge posed by the significant increase in spam, constituting up to 30 percent of all inbox messages. 2. Acknowledgment that technical solutions alone are insufficient to address the spam problem effectively. 3. Highlighting the evolving nature of spam wars, with spammers continuously adapting to more intelligent filters. 4. Emphasis on the need for a new approach and proposing that spam is not just a personal problem but a social problem requiring a social response. 5. Observation that traditional social responses, such as law, courts, and the judiciary, are less effective in the cyberspace context. 6. Proposal to bridge the gap between society and technology by advocating the application of social concepts to technology design. | 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. Exploration of the integration of advanced computing and communication technologies in the context of smart grid development. 2. Identification of smart grid as the next-generation power system, emphasizing self-healing, resilience, sustainability, and efficiency. 3. Recognition of the challenges and initiatives arising from smart grid innovation in both industry and academia. 4. Critical examination of security concerns as a key focus in the smart grid ecosystem. 5. Application of a data-driven approach to survey recent security advances in smart grid, with a systematic breakdown into four sequential stages: a) Data generation. b) Data acquisition. c) Data storage. d) Data processing. 6. Comprehensive review of security vulnerabilities and solutions within the entire lifecycle of smart grid data. 7. In-depth analysis of security analytics in smart grid, highlighting the utilization of data analytics for ensuring smart grid security. 8. Forward-looking discussion on potential future research directions in the field of smart grid security. | 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. Investigation of security challenges associated with big data and the potential risks to enterprise information security. 2. Recognition of the need for robust security measures, especially in scenarios where data is outsourced to third parties. 3. Introduction of a mutual authentication scheme based on a virtual smart card using a hashing function for large information sets. 4. Resolution of issues related to unlawful user access to big data servers and illegal access to legal cloud servers through enhanced security measures. 5. Implementation of file swapping techniques to maintain user-sensitive information within big data, ensuring data privacy. 6. Description of the process wherein user information is swapped to different servers after data access, enhancing file security and preventing unauthorized access. 7. Aim to achieve strong countermeasures against cybercrime through the integration of security measures with big data 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. |  |
| Vanet FDIA Solutions using Blockchain Based IPFS-Trust Management System with ML SVR Model | Preeti Grover, Sanjeev Kumar Prasad | 2023 | (Missing Journal) | 1. Exploration of Internet of Vehicles (IoV) and its significance in the evolution of vehicular ad hoc networks (VANETs). 2. Recognition of multiple types of smart networks in the surrounding environment, including Wireless Sensor Networks (WSNs), Crowd Sensing Networks (CSNs), and Internet of Vehicles. 3. Definition of VANET as a collection of mobile nodes (vehicles) facilitating data sharing through ad hoc on-demand connections. 4. Identification of vehicle tracking as a key application of IoV and acknowledgment of vehicle security as a major concern for vehicle owners. 5. Highlighting the presence of on-board sensors on vehicles for sensing motion and the surrounding environment. 6. Emphasis on the warning capabilities of on-board sensors for drivers, including alerts about approaching vehicles, speeding, and slippery road conditions. 7. Main objective: Providing solutions for False Data Injection Attack (FDIA) by integrating a Blockchain-based IPFS-Trust Management System with an ML SVR Regression Model. 8. Addressing the critical safety concerns due to network assaults and threats in the VANET system. 9. Explanation of the vulnerability where a rogue node can send erroneous messages leading to unavoidable scenarios. 10. Methodology involves filtering received data from vehicles to detect false traffic jam warning messages using the ML SVR Regression Model. 11. Utilization of a Machine Learning supervised algorithm to determine the legitimacy of a vehicle and differentiate it from an attacker vehicle. 12. Validation of results using parameters such as Accuracy, Loss Rate, Precision, Recall, and F-Test Score. 13. Algorithm implementation results showing that the FDIA attack strategy with ML SVR Regression Model achieves better performance in predicting VANET security compared to a strategy without ML. 14. Study of various ways to mitigate the impact of false data injection into the network through a compromised node. 15. Accessibility of the system by users through a Distributed Application (DApp) on the Ethereum platform for managing vehicle data. | 1. Comprehensive exploration of IoV and its role in VANET evolution, including the presence of various smart networks. 2. Definition and recognition of VANET as a network of mobile nodes facilitating ad hoc data sharing. 3. Acknowledgment of the importance of vehicle tracking and the security concerns associated with IoV. 4. Highlighting the warning capabilities of on-board sensors for drivers in various scenarios. 5. Clear articulation of the main objective: providing solutions for False Data Injection Attack in VANET through a combination of blockchain, IPFS, and ML SVR Regression Model. 6. Addressing critical safety concerns arising from network assaults and threats in the VANET system. 7. Explanation of the vulnerability involving rogue nodes sending erroneous messages and its potential consequences. 8. Detailed methodology involving the use of ML SVR Regression Model to filter and detect false traffic jam warning messages. 9. Application of a Machine Learning supervised algorithm to distinguish between legitimate and attacker vehicles. 10. Validation of results using various performance metrics. 11. Demonstration of the superiority of the FDIA attack strategy with ML over a strategy without ML in predicting VANET security. 12. Exploration of mitigation strategies for false data injection impact through compromised nodes. 13. User accessibility to the system through a DApp on the Ethereum platform for efficient management of vehicle data. |  |
| Vision: Security-Usability Threat Modeling for Industrial Control Systems | Karen Li, A. Rashid, A. Roudaut | 2021 | European Symposium on Usable Security | 1. Focus on Industrial Control Systems (ICS) operating large-scale infrastructures such as water, power, and manufacturing. 2. Recognition of the increasing attention on ICS due to high-profile attacks against critical infrastructures. 3. Acknowledgment that ICS systems are connected to IT systems and the internet, presenting challenges for control systems engineers and operators. 4. Identification of the complexity of threats faced by ICS environments, including the intersection of users with security requirements. 5. Reference to the challenges of usable security in IT systems and existing work on security-usability threat modeling. 6. Highlighting the lack of examination of similar challenges within ICS settings, where additional requirements such as process safety, process integrity, and process reliability are critical. 7. Introduction of a case study involving a Programmable Logic Controller (PLC) to detail the user workflow for a security task. 8. Analysis of the workflow using STRIDE, an established threat modeling approach. 9. Mapping of threats against an existing security-usability threat model for IT systems, considering specific process-related requirements of ICS users. 10. Derivation of an initial security-usability threat model for ICS as a foundational step for further research in this area. | 1. Comprehensive focus on the challenges faced by Industrial Control Systems (ICS) in the context of large-scale infrastructures. 2. Recognition of the heightened attention on ICS due to notable attacks against critical infrastructures. 3. Acknowledgment of the interconnected nature of ICS with IT systems and the internet, posing challenges for control systems engineers and operators. 4. Identification of the intricate threats faced by ICS environments, emphasizing the intersection of users with security requirements. 5. Reference to the well-studied challenges of usable security in IT systems and existing work on security-usability threat modeling. 6. Clear articulation of the unexplored challenges within ICS settings, where unique requirements such as process safety, integrity, and reliability come into play. 7. Detailed case study involving a Programmable Logic Controller (PLC) to illustrate user workflows for security tasks. 8. Application of the STRIDE threat modeling approach to analyze the identified workflow. 9. Integration of threats with an existing security-usability threat model for IT systems, considering the specific requirements of ICS users. 10. Generation of an initial security-usability threat model for ICS, laying the groundwork for future research in this domain. |  |