International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7185
***Article Received**: 24 April 2023 **Revised:** 12 June 2023 **Accepted:** 27 June 2023*

Analysis of Social Network Data Mining for Security Intelligence Privacy Machine Learning

S. Elango[1], V Revathi[2], S. Aruna Deepthi[3], Ananya Bhargavi Kodali[4], M. Gopila[5], Bibin K Jose[6]
[1]Assistant Professor, Dept of CSE,
Madanapalle Institute of Technology & Science, Madanapalle,Andhra Pradesh
etechday@gmail.com
[2]Professor, Department of Physics, Applied Sciences,
New Horizon College of Engineering, Bangalore, Karnataka, India
[3]Assistant Professor, ECE, Vasavi college of Engineering, Hyderabad
[4]UG Student -Computer Science, Arizona State University, Arizona, USA
[5]AP(Sr.G), Electrical and Electronics Engineering,
Sona college of Technology, Sona Nagar, Salem
[6]Associate Professor, PG & Research Department of Mathematics,
Sanatana Dharma College Alappuzha, Kerala, India

Abstract—The Modern communication on the Internet platform is most responsive through social media. Social media has changed and is still reshaping how we share our thoughts and emotions in communication. It has introduced a constant real-time communication pattern that was before unheard of. Young and old, organizations, governmental agencies, professional associations, etc., all have social media accounts that they use exclusively for communication with other users. Social media also acts as a powerful network engine that connects users regardless of where they are in the world. The development of global communication will greatly benefit from the availability of this new communication platform in the future. Consequently, there is a pressing need to research usage trends. Therefore, it is vital to investigate social media platform usage trends in order to develop automated systems that intelligence services can use to help avert national security incidents. Through the use of social media data mining, this research study suggests an automated machine learning model that can improve speedy response to crises involving national and International security.

Keywords—Data mining, Privacy, Machine Learning, Internet platform, Security, social media.

I. INTRODUCTION

Social network platforms for social network platforms, there are data mining models aimed at many industries, including healthcare for illness control, business for price and consumer behavior forecasting, etc. Others are at the proposal stage while some are still being developed. For the sake of national security, this research project will make use of the current machine learning approaches on social media data. Therefore, it is vital to investigate social media platform usage trends in order to develop automated systems that intelligence services can use to help avert national security incidents. Through the use of social media data mining, this research study suggests an automated machine learning model that can improve speedy response to crises involving national security. When the project is finished, an application with manageable features and the ability to generate automated incident notifications will be created, which law enforcement authorities may find useful in the event of a national security incident.

II. PRIVACY MACHINE LEARNING AND DATA MINING SELECTION

When creating a predictive model using machine learning algorithms, features selection is a method of reducing the amount of inputs. Because there is valuable information hidden in these vast amounts of data, metadata is a benefit. For data analytics to produce exact forecasts that enable better decision-making, more in-depth understanding and the detection of fine-grain patterns are required. The confidentiality of the data must be maintained in order to identify the data. It will guarantee that no information is disclosed to unauthorized parties. In order to protect data privacy, we analyze feature selection for data mining and machine learning algorithms in this work. Method for Distributed Systems Data Mining with Privacy Preserved It might have an impact on information security violations. Source data may be made public when being sent over open networks or when being captured and stored.

The goal of this work is to address the issue of distributed data mining systems' information security. Over vertically partitioned data, we describe a privacy-preserving DBSCAN clustering algorithm, examine this algorithm's security in light of several adversaries, and show its effectiveness. The recommended method could be applied widely to protect data privacy in industrial systems.

The widespread use of computers makes it easier to comprehend the significance of issues with data analysis and knowledge discovery. To collect this helpful information, it is crucial to design strategies and construct data storages [1]. Data mining (DM) is a technology for finding knowledge in unstructured data collections that was not previously recognized. Generating decisions, generating predictions, spotting abnormalities, and other tasks may benefit from this information. There are various DM algorithms available [2] for association rules mining, data clustering, and classification. Finding meaningful associations and correlation patterns between big sets of data items is the aim of association rules mining [3]. The class of each object under consideration is determined by classification analysis techniques.

Today, however, we can observe a tendency toward the usage of scattered data sources, which each contain a different portion of the whole data set. They can distribute the data in any way, including horizontally [4], vertically [5], Using Database Security as a gateway data mining is the process of correctly examining or testing relevant data that is largely held in a database or many databases in command to include valuable in sequence with the purpose of might be statistically or strategically important. Such analyzed database might include a number of exquisite characteristics or information that could be used in an attack to reveal someone is sensitive information. Once more, a trade-off between privacy and utility of data must be made. PPDM may be viewed as a research that illustrates how to prevent such disclosure.

We also go through the characteristics of potential solutions that can safeguard these components, ensuring privacy in outsourcing situations. Introducing myself Business computing is becoming a crucial component of some business processes and a factor in the success of organizations due to the expansion of information systems and technology. Every transaction is documented someplace, and data collecting is becoming a common practice in corporate computers [6]. businesses is data mining, which is acknowledged as a critical method for turning "data rich" into "knowledge rich" by extracting knowledge from vast amounts of collected or accumulated raw data. Organizations frequently use data mining techniques to aid in making strategic decisions, and the advantages have been shown in a variety of business Market basket analysis [7], another name for Association rule mining, is a process of exploring and analyzing raw data to find novel and significant patterns in routine company processes [8]. It has been used extensively in market strategy and decision support for organizations [9].Public safety and intelligence data are also plagued by validity and reliability issues. Victims are frequently too stressed, witnesses typically forget, and criminals often lie when reporting an occurrence. Together, these problems substantially impair the majority of the material that criminal analysts and intelligence specialists come across. Output difficulties However, someone needs to be able to comprehend and use the analytical result[10].As a result, while constructing models, analysts frequently have to strike a balance between accuracy and the capacity to produce operationally useful output. The two frequently compromise with one another; this is more common than not[11]. Making wise decisions in this area necessitates a high level .The goal of privacy preserving data mining method is to glean insightful information from data while safeguarding individual privacy and sensitive data. These methods use a variety of ways to guarantee the security, privacy, and confidentiality of the data. We will analyze and categorize a few popular privacy-preserving data mining strategies in this analysis based on their methodologies.

III. PRIVACY-PRESERVING DATA MINING

Randomization methods: Randomized Response: To conceal sensitive information during data collecting or surveys, this technique employs controlled noise or randomization. It ensures believable denial, making it difficult to discern people's real reactions[12]. Random disturbance: This technique includes introducing arbitrary noise or disturbance to the dataset in order to protect privacy while enabling statistical analysis. Common techniques include the addition of Gaussian or Laplacian noise. Methods of Anonymization :K-Anonymity: This method makes sure that every record in a dataset can be compared to at least k-1 other records without being recognized. In order to maintain the usefulness of the data while achieving anonymity, qualities must be generalized or suppressed. L-Diversity: Using k-anonymity as a foundation, l-diversity makes sure that each set of k-anonymous records' sensitive characteristics have at least l different values, prohibiting attribute disclosure-Closeness: By taking the distribution of sensitive traits into account, it improves on l-diversity. Cryptographic Methods o Homomorphic Encryption: This method enables calculations to be made on encrypted material without having to first decrypt it. It permits computations on encrypted data that protect privacy, guaranteeing confidentiality. Differential Privacy: To prevent the identification of specific individuals in the dataset, differential privacy adds noise to query results or database records. It offers a paradigm for quantifying and ensuring privacy through mathematics.PrivBayes: A differentially private technique for disseminating fake data, PrivBayes. It creates synthetic data with privacy assurances by learning a Bayesian network structure from the original data[13]. Secure Summarization Techniques: These methods generate aggregates or summary statistics from sensitive material while protecting privacy. They use cryptographic techniques to compute aggregates without disclosing individual data, such as secure multi-party computation. It is important to note that these strategies are not exclusive of one another, and that numerous techniques are sometimes used to

***Article Received**: 24 April 2023 **Revised:** 12 June 2023 **Accepted:** 27 June 2023*

achieve stronger privacy assurances. The technique chosen will rely on the details of the data mining task and the desired level of privacy protection.

IV. TECHNIQUES FOR DATA MINING THAT RESPECT PRIVACY SYNTHETIC INTELLIGENCE

Artificial intelligence separateness preserving data mining technique refer to tactics and procedures that seek to safeguard private information and the privacy of persons while utilizing AI algorithms for data analysis. These methods guarantee that AI models can be developed and used without jeopardizing privacy[14]. Here are a few typical data mining methods that protect privacy that are used in the context of AI:Federated Learning: Without transferring raw data, federated learning enables cooperative model training across numerous decentralized servers or devices. AI models are instead locally trained on user devices, and only model updates or gradients are transmitted and combined to create a global model. This strategy makes use of group intelligence while protecting data privacy on individual devices. Secure Multiparty Computation (SMC): SMC techniques let several parties run AI algorithms on their individual private data without disclosing sensitive information[15-16]. During collaborative AI tasks like model training, prediction, or data analysis, SMC maintains privacy and secrecy. Differential protect, guard, safeguard Privacy for AI: When building or using models, AI can use Differential Privacy approaches to safeguard users' privacy. Differential privacy ensures that the presence or absence of any specific data point does not materially affect the conclusion by adding noise to the training process or query responses. This protects sensitive data.Homomorphic Encryption: With homomorphic encryption, calculations can be made on encrypted material without having to first decrypt it. A direct application of AI algorithms to encrypted data can guarantee privacy during inference and training. This method makes it possible to train and predict models securely without disclosing the underlying data. Privacy-Preserving Deep Learning: Privacy-preserving methods can be added to or modified in deep learning models. Deep learning processes can use methods like secure aggregation, secure enclaves, or encrypted computing to safeguard sensitive data. Synthetic Data Generation: This process involves producing fake data that closely resembles the statistical traits and attributes of the real dataset. Privacy can be protected while still enabling the development and use of AI systems by producing fake data. Through the use of methods like PrivBayes, which offer differential privacy, privacy guarantees can be attained[17-18]. The selection of a privacy-preserving AI method must take into account a variety of elements, including the sensitivity of the data, the particular AI task at hand, and the desired level of privacy assurances. In real-world situations, a mix of these methods might be used to strengthen privacy protection in AI applications.

V. SECURITY USING DATA MINING AND ARTIFICIAL INTELLIGENCE

Fig1Artificial intelligence (AI) that is based on data mining is extremely important for improving security measures and tackling numerous security issues[20]. AI can examine massive amounts of data to find patterns, abnormalities, and potential security issues by utilizing data mining techniques. The following are some crucial elements of applying AI data mining for security:

1. Detecting and preventing intrusions Network traffic logs, system logs, and other security-related data can be examined by data mining algorithms to identify and stop attack attempts. AI models can recognize suspicious behaviors, anomalies, or patterns that may point to possible cyber attacks or security breaches by learning from prior data. Malware detection: To create efficient detection models, data mining technique can be used to examine the patterns and traits of known malware samples[21-23]. By finding comparable patterns or behaviors from large-scale datasets, AI systems can uncover new and unidentified malware, enabling proactive security measures. Fraud Detection: Data mining technologies, such as anomaly detection and pattern recognition, can aid in the discovery of fraudulent activities in a variety of industries, including finance, e-commerce, and insurance. AI models can detect questionable transactions by examining transactional data, user behavior, or historical patterns, thereby preventing financial loss or unlawful access. Threat Intelligence: Data mining is essential for gathering and evaluating massive amounts of security-related information from a variety of sources, including as threat feeds, vulnerability databases, and social media. AI models may extract pertinent data and offer insightful threat intelligence, assisting in proactive security actions and risk assessment. User activity Analysis: Data mining algorithms can examine patterns of user activity to find anomalies or departures from routine behavior. This can be used for user authentication, insider threat detection, and access control systems. AI systems are able to recognize the patterns of regular activity and inform users when something out of the ordinary happen. Data Leakage Prevention: To monitor and analyze data flows inside an organization and spot potential data leaks or unauthorized data access, data mining techniques can be used. Artificial intelligence (AI) models are able to spot suspicious data flows and enforce data protection protocols by examining network traffic, data transfers, or user access logs. Security Event Prediction: Data mining algorithms can forecast potential security events or vulnerabilities by using historical security data[19]. AI systems are able to learn from prior events and spot trends or causes of security breaches. By using this information, security precautions may be proactively strengthened and possible threats can be reduced. It is crucial to remember that

while data mining-based AI provides major security advantages, there are also privacy issues that must be resolved. To balance security and privacy needs, privacy-preserving data mining approaches can be used, such as differential privacy or federated learning.

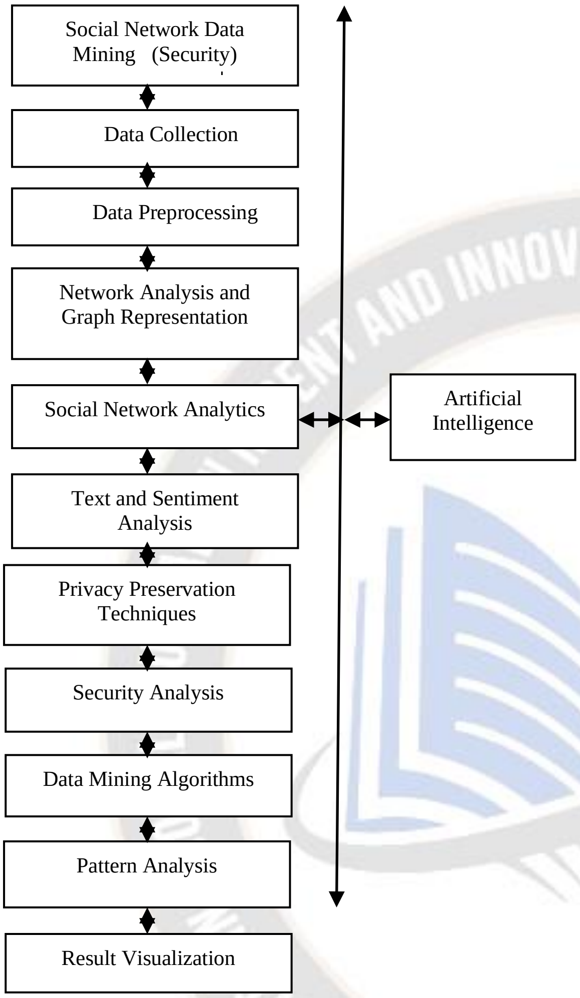

Fig. 1. Block diagram

VI. ELECTRONICS AND SENSOR SYSTEMS

In the context of electronics and sensor systems, advanced data mining methods in conjunction with artificial intelligence (AI) can greatly improve security. AI can evaluate sensor data, spot anomalies, and spot potential security vulnerabilities by using data mining techniques. Here are a few ways that sophisticated data mining AI approaches can be used to improve sensor and electronics security: Anomaly Detection: Anomalies in sensor data can be found using data mining algorithms like clustering or classification. AI algorithms can recognize anomalous behavior or departures from expected norms by examining prior sensor data or patterns. This could assist in identifying sensor manipulation, unlawful entry, or unusual operating circumstances.Intrusion Detection in Sensor Networks: In sensor networks, network traffic, communication patterns, and sensor data may all be examined using data mining-based AI. AI models can recognize suspicious behaviors, abnormalities, or patterns that might point to illegal access, data tampering, or network attacks by learning from historical data. Sensor Data Fusion: To extract insightful information and improve security, data mining techniques can be used to combine data from various sensors. AI models can examine the merged sensor data to find intricate patterns, correlations, or occurrences that might not be obvious when only looking at the individual sensor readings. This makes danger detection and situational awareness more precise. Predictive Maintenance: Data mining algorithms can examine sensor data to foretell electronic system breakdowns or equipment failures. AI models can improve security and dependability by providing early warnings or alerts for maintenance and preventing future system breakdowns by seeing trends or anomalies in sensor readings. Privacy-Preserving Data Analysis: Privacy issues must be taken into account when data mining sensor data. Differential privacy and safe multi-party computation are two privacy-preserving data mining approaches that can be used to protect sensitive data while still gaining insightful knowledge from the data. This guarantees that safety precautions are fulfilled while preserving privacy. Threat Intelligence and Risk Assessment: Security-related data, such as sensor data, threat feeds, vulnerability databases, or security incident records, can be analyzed using advanced data mining techniques. AI models can offer insightful information for threat intelligence and risk assessment by extracting pertinent data. This aids in discovering potential security risks, holes in the electronics, or weak points in the sensor network. Real-time Security Monitoring: AI powered by data mining can monitor and analyze sensor data streams in real-time. AI models can swiftly identify and respond to security threats or unusual events by continually evaluating incoming sensor readings, sending out timely notifications and reducing potential hazards. Overall, by offering effective anomaly detection, predictive maintenance, privacy-preserving analysis, and real-time monitoring capabilities, sophisticated data mining approaches combined with AI can improve security in electronics and sensor systems. These strategies make it possible to take preventative security actions, identify threats earlier, and increase system dependability.

VII. DATA MINING METHODS ELECTRONICS AND SENSORS

Fig 2Insightful information can be gleaned from data gathered by electronics and sensors using data mining techniques. Data mining methods can be used to analyze sensor data to find patterns, connections, and trends that can be useful for a variety of applications. Here are some examples of how data mining is applied to electronics and sensor data: Anomaly

Detection: Sensor data can be analyzed by data mining techniques to find anomalies or outliers. Anomalies indicating flaws, malfunctions, or unexpected behavior can be found by comparing sensor values to typical patterns, statistical models, or thresholds. This promotes the performance and dependability of electronic systems. Predictive Maintenance: Based on sensor data, data mining can be used to forecast the health and maintenance requirements of electronic systems. AI models can find signs of prospective breakdowns by examining historical sensor readings and equipment failure trends. This lowers downtime and allows for preventive maintenance. Fault Diagnosis: Sensor data can be used to apply data mining methods to fault-finding or problem-solving in electronic systems.

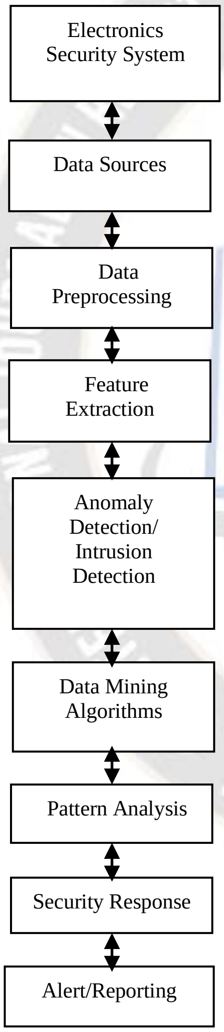

Fig. 2. Security for electronics Diagram of Data Mining Techniques

AI models can determine the underlying causes of failures or abnormalities by comparing sensor readings with recognized problem patterns or by employing machine learning techniques. This enables effective troubleshooting and repair. Quality Control: To assure product quality, sensor data gathered during the production process can be examined using data mining techniques. AI models can highlight potential quality issues early on and enable corrective measures by finding relationships between sensor readings and product flaws.

Fig 3 and 4 Optimization and Performance Enhancement: Data mining can reveal patterns and connections in sensor data that can be used to enhance the performance of electronic systems. AI models can pinpoint areas for enhancement by examining sensor data, such as energy efficiency, throughput, or resource allocation, resulting in improved system performance. Sensor Calibration: Processes for sensor calibration can benefit from data mining approaches.

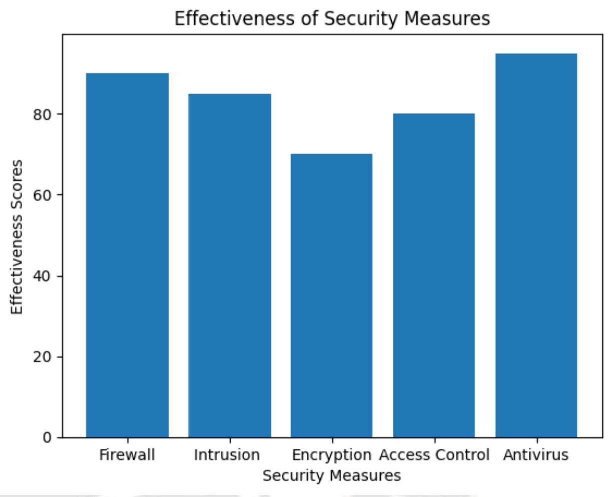

Fig. 3. Security using data mining and artificial intelligence

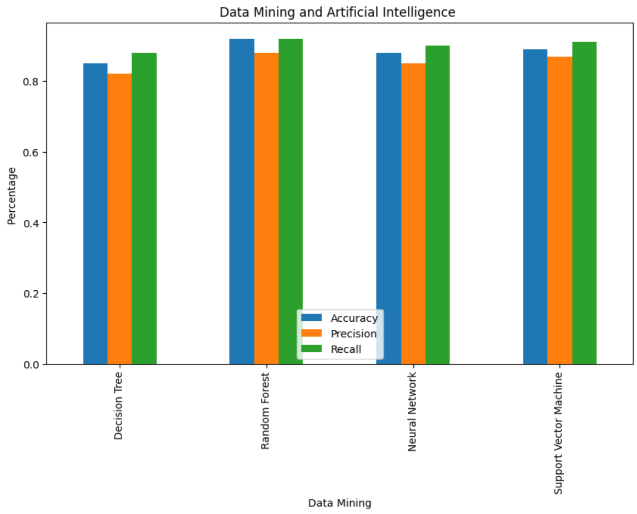

Fig. 4. Data mining and artificial intelligence

Fig 5 and 6 AI algorithms can learn calibration models or spot departures from predicted behavior by examining sensor data gathered under controlled conditions. This makes it possible to calibrate sensors correctly, guaranteeing the precision and dependability of measurements. Environmental Monitoring:

Sensor data gathered for environmental monitoring purposes can be mined for information

AI models can find patterns, trends, or anomalies in the data collected by numerous sensors that monitor variables like temperature, humidity, air quality, or radiation levels. These insights into environmental conditions are extremely useful.

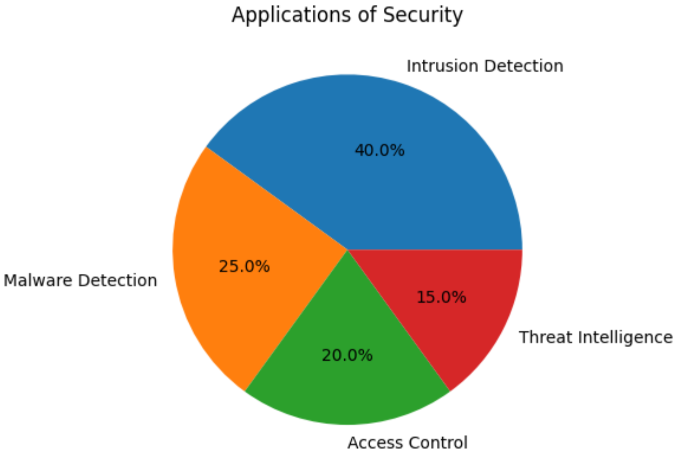

Fig. 5. Application of Data mining output comparsion

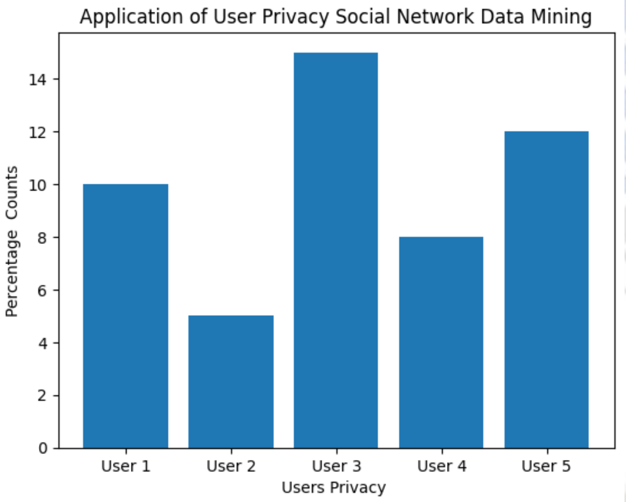

Fig. 6. Application of User Privacy Social Network Data Mining

VIII. CONCLUSION

Through enhanced system performance, problem detection, predictive maintenance, and optimization, these applications show how data mining techniques may be used to maximize the potential of electronics and sensor data. Data mining enables the extraction of useful information from sensor data, improving decision-making and maximizing resource efficiency.

Acknowledgement

G.Ramachandran, Support, Centre of Research and development ,Tamilnadu, India

REFERENCES

[1] de Leeuw, AW., Heijboer, M., Verdonck, T. et al. Exploiting sensor data in professional road cycling: personalized data-driven approach for frequent fitness monitoring. Data Min Knowl Disc **37**, 1125–1153 (2023). https://doi.org/10.1007/s10618-022-00905-5

[2] Ziyu, Z., Kuang, K., Li, B. et al. Differentiated matching for individual and average treatment effect estimation. Data Min Knowl Disc **37**, 205–227 (2023). https://doi.org/10.1007/s10618-022-00886-5

[3] R. Josphineleela, S. Kaliappan, L. Natrayan and A. Garg, "Big Data Security through Privacy – Preserving Data Mining (PPDM): A Decentralization Approach," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 718-721, doi: 10.1109/ICEARS56392.2023.10085646.

[4] T. C. S. Lakshmi, R. A. A. Rosaline, R. T. Selvi, D. Karunkuzhali and S. Lavanya, "Privacy-Preserving Data Mining Process in Industry," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 834-839, doi: 10.1109/IITCEE57236.2023.10091069.

[5] K. N. Prasanthi, C. Sekhara Rao Mvp and S. B. Pallapothu, "Boosted Hybrid Privacy Preserving Data Mining (BHPPDM) Technique to Increase Privacy and Accuracy," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 378-384, doi: 10.1109/ICAIS56108.2023.10073804.

[6] Ana Oliveira, Yosef Ben-David, Susan Smit , Elena Popova, Milica Milić. Machine Learning for Decision Optimization in Complex Systems. Kuwait Journal of Machine Learning, 2(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/201

[7] M. Rafiei and W. M. P. Van Der Aalst, "An Abstraction-Based Approach for Privacy-Aware Federated Process Mining," in IEEE Access, vol. 11, pp. 33697-33714, 2023, doi: 10.1109/ACCESS.2023.3263673.

[8] Suryawanshi, R. ., & Vanjale, S. . (2023). Brain Activity Monitoring for Stress Analysis through EEG Dataset using Machine Learning. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 236–240. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2498

[9] P. A., G. V. Reddy and G. Ramachandran, "Artificial Intelligence Techniques for the wireless wearable Smart Healthcare Prediction System Applications," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 879-884, doi: 10.1109/ICEARS56392.2023.10085051.

[10] Bandara, E., Liang, X., Shetty, S. et al. Octopus: privacy preserving peer-to-peer transactions system with InterPlanetary file system (IPFS). Int. J. Inf. Secur. **22**, 591–609 (2023). https://doi.org/10.1007/s10207-022-00650-2

[11] A. V. Kumar, K. Monica and K. Mandadi, "Data Privacy Over Cloud Computing using Multi Party Computation," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru,

India, 2023, pp. 262-267, doi: 10.1109/IDCIoT56793.2023.10053427.

[12] Lovrenčić, R., Škvorc, D. Multi-cloud applications: data and code fragmentation for improved security. Int. J. Inf. Secur. **22**, 713–721 (2023). https://doi.org/10.1007/s10207-022-00658-8

[13] P. A. Padmaavathy, A. Celina, R. P. Devi, B. N. Arathi, G. Sureshkumar and G. Ramachandran, "Analysis Techniques for Pharmaceutical Drugs Biomedicine Big Data Analytics and Machine Learning," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 83-86, doi: 10.1109/ICICCS56967.2023.10142645.

[14] Mishra, K.C., Dutta, S. A simple and secure user authentication scheme using Map Street View with usability analysis based on ISO/IEC 25022. Int. J. Inf. Secur. **22**, 403–415 (2023). https://doi.org/10.1007/s10207-022-00636-0

[15] A. Padma, S. Gadde, B. S. P. Rao and G. Ramachandran, "Effective Cleaning System management using JSP and Servlet Technology," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1472-1478, doi: 10.1109/ICCES51350.2021.9488925.

[16] P. Kumar Goswami, S. Baruah and L. Thakuria, "Cyber Security and Data Mining Techniques," 2022 International Conference on Edge Computing and Applications (ICECAA), Tamilnadu, India, 2022, pp. 1427-1431, doi: 10.1109/ICECAA55415.2022.9936489.

[17] P. A., B. Seth and G. Ramachandran, "Analysis of Current Smart Wearable Trends using Internet of Medical Things," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 19-22, doi: 10.1109/ICAIS56108.2023.10073832.

[18] R. N. Yasa, I. K. S. Buana, Girinoto, H. Setiawan and R. B. Hadiprakoso, "Modified RNP Privacy Protection Data Mining Method as Big Data Security," 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS, Jakarta, Indonesia, 2021, pp. 30-34, doi: 10.1109/ICIMCIS53775.2021.9699180.

[19] H. Chen, "Construction of Network Information Security Risk Framework Based on Data Mining and Analysis," 2022 International Conference on Artificial Intelligence of Things and Crowdsensing (AIoTCs), Nicosia, Cyprus, 2022, pp. 185-189, doi: 10.1109/AIoTCs58181.2022.00035.

[20] T. Soewu, Hemant, M. Rakhra and D. Singh, "Analysis of Data Mining-Based Approach for Intrusion Detection System," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 908-912, doi: 10.1109/IC3I56241.2022.10072828.

[21] W. Deng, Z. Huang, J. Zhang and J. Xu, "A Data Mining Based System For Transaction Fraud Detection," 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 2021, pp. 542-545, doi: 10.1109/ICCECE51280.2021.9342376.

[22] S. M et al., "Analysis of Hydroponic System Crop Yield Prediction and Crop IoT-based monitoring system for precision agriculture," 2022 International Conference on Edge Computing and Applications (ICECAA), Tamilnadu, India, 2022, pp. 575-578, doi: 10.1109/ICECAA55415.2022.9936473.

[23] S. M. Arıkan and S. Acar, "A Data Mining Based System for Automating Creation of Cyber Threat Intelligence," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-7, doi: 10.1109/ISDFS52919.2021.9486335.

[24] Y. Huang and W. Zhang, "Research on the Methods of Data Mining based on the Edge Computing for the IoT," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099991.

[25] A. Vaghela and A. Suthar, "Comprehensive Analysis of Privacy and Data Mining Techniques," 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA, Pune, India, 2022, pp. 1-6, doi: 10.1109/ICCUBEA54992.2022.10010944.