IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

A Systematic Study of Machine Learning in Comprehensive Cybersecurity Approaches

Dandugudum Mahesh, Dr. T. Sampath Kumar

Research Scholar, School of CS&AI, SR University, Warangal, Telangana, India.

Assistant Professor, School of CS&AI, SR University, Warangal, Telangana, India.

ABSTRACT: Cybersecurity is pertinent in today's interconnected world, and it is protecting digital systems from different attacks. The integration of machine learning (ML) and cybersecurity involves combining machine learning techniques with cybersecurity practices to enhance the protection of digital systems and data. Machine learning enhances the effectiveness and efficiency of cybersecurity by offering advanced threat detection and rapid response capabilities, empowering organizations to better defend against a broad range of cyber threats. ML has become a crucial technology in various domains and is revolutionizing the way information systems work. ML algorithms can analyze large amount of data from different sources to identify patterns and anomalies that could indicate a potential security breach. ML models can be trained to detect unusual network activity, suspicious login attempts, and other types of activities that could indicate a cyber-attack. The main objective of this article to study on using machine learning in the field of cybersecurity is to enhance the efficiency, scalability, and contrivance of malware detection compared with traditional methods that rely on human intervention.

KEYWORDS: Cyber security, Random Forest, Support Vector Machine.

I. INTRODUCTION

Machine learning (ML) is a core subset of artificial intelligence (AI) and pertains to the procedure of training computers to acquire knowledge of patterns from existing information with the aim of formulating predictions on new data [1]. While AI and ML are often used interchangeably, it is crucial to acknowledge the fundamental distinctions between these two ideas. AI is a field of technology that involves the training of computers to replicate or mimic human cognitive processes in real-world settings [2]. ML on the other hand, pertains to the computer systems or models that are developed via AI, which have the ability to learn from data and make predictions. The Cybersecurity and Infrastructure Security Agency (CISA) is a federal agency within the United States government [3]. Its primary mission is to enhance the security and resilience of critical infrastructure across the nation. Critical infrastructure includes various essential systems and assets such as those related to energy, transportation, and water supply. CISA plays a pivotal role in safeguarding these critical systems and ensuring they are well-protected and capable of withstanding a range of threats and challenges, both in the physical and cyber realms. Maintaining security in the digital realm presents a perpetual and intricate problem, due to the progressive advancements in technology and cyber threats. A multitude of strategies and measures are implemented to ensure cyberspace security. The concise summary of security protocols in the field of cybersecurity has given below [4]. Common authentication protocols include Password Authentication Protocol (PAP) [5], Challenge-Handshake Authentication Protocol (CHAP) [6], and Remote Authentication Dial-In User Service (RADIUS)[7]. These are protocols that are used to verify the identity of users, devices, or services before granting access to resources. Common access control protocols include Role-Based Access Control (RBAC) [8], Attribute-Based Access Control (ABAC) [9], and Mandatory Access Control (MAC) [10]. These are protocols that determine what resources a user or device is authorized to access and how they can access them. Intrusion detection protocols include firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS) [11,12]. These are protocols that detect and prevent malicious activity or attacks on a network or system. Common key management protocols include Key Management Protocol (KMP), Key Exchange Protocol (KEP), and Simple Key-Management for Internet Protocol (SKIP) [13]. These are protocols that are used to manage cryptographic keys used for encryption and decryption to maintain the confidentiality and integrity of data. Blockchain-enabled security protocols provide secure communication and storage of data. They are designed to maintain the integrity, confidentiality, and availability of data. These protocols include blockchain-based secure digital identity systems, blockchain-based secure data sharing, and blockchain-based smart contract security [14-16].

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

This article is organized as follows. Section II describes Machine Learning in Cyber Security, Cybersecurity Policies Taxonomy. Implementing machine learning in the field of cybersecurity in Section III. Section IV presents the usage of Machine learning algorithms in Cyber Security. Finally, Section V presents conclusion.

II. MACHINE LEARNING IN CYBER SECURITY

Machine learning algorithms employ computational techniques to acquire knowledge directly from data, rather than depending on predefined equations as models. These algorithms enhance their performance as they gain more learning samples. Machine learning enables computers to acquire knowledge without the need for explicit programming. In simpler terms, it empowers computers to emulate the human capacity to learn from experience. Machine learning is a subset of the larger field of artificial intelligence [17].

In the context of security, machine learning consistently enhances its knowledge through data analysis, thereby improving its ability to identify malware within encrypted traffic, detect insider threats, forecast online areas of potential risk to ensure safe browsing, and safeguard cloud-stored data by uncovering any suspicious user behaviour.

Use case	Description
Detecting threats on a network	Machine learning identifies potential threats by consistently monitoring network behavior for irregularities. It involves processing large volumes of data in nearly real-time, using machine learning engines to uncover significant incidents. These methodologies are effective in detecting insider threats, unidentified malware, and breaches of security policies.
Keep people safe when browsing	Machine learning algorithms have the capability to forecast and identify "adversarial domains" on the internet, therefore aiding in the mitigation of individuals' exposure to potentially harmful websites. The process of machine learning involves the analysis of Internet traffic in order to autonomously detect attack infrastructures that are set up to carry out both existing and emerging threats.
Providing endpoint malware protection	Algorithms has the capability to identify previously unencountered malware that seeks to execute on endpoints. The system detects novel harmful files and activities by analyzing the characteristics and actions shown by previously identified malware.
Protection of data over cloud	Machine learning has the potential to enhance productivity by examining dubious login behavior in cloud applications, identifying abnormalities based on geography, and doing IP reputation research to uncover potential threats and vulnerabilities inside cloud applications and platforms.
Detect malware in encrypted traffic	The use of machine learning techniques enables the identification of malware inside encrypted communication via the examination of shared network telemetry data components associated with encrypted traffic. Instead of performing decryption, machine learning algorithms use pattern recognition techniques to detect concealed risks inside encrypted data.

Machine learning offers several significant advantages when applied to cybersecurity challenges. Security analysts often grapple with the daunting task of rapidly processing a flood of intelligence related to their attack surface. This data typically accumulates at a rate that surpasses the manual processing capabilities of their teams. Machine learning excels at quickly scrutinizing extensive datasets, both historical and real-time, allowing teams to harness data from diverse sources in nearly real-time. Continuous training cycles empower machine learning models to adapt to the evolving landscape of threats. This adaptation includes learning from analyst-verified detections and alerts. This ongoing learning process minimizes recurrent false positives and empowers models to incorporate expert-validated ground truth [18]. Machine learning can be harnessed to automate specific routine tasks, freeing security teams from repetitive and time-consuming responsibilities. This automation acts as a force multiplier, enabling teams to efficiently respond to incoming alerts while redirecting their valuable time and resources toward more complex, strategic initiatives [19]. Machine learning complements the capabilities of human analysts by providing them with real-time, current intelligence. This augmentation allows analysts involved in threat hunting and security operations to effectively prioritize resources in addressing critical vulnerabilities within their organization and promptly investigate detections flagged by machine learning algorithms.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

III. TAXNOMY OF CYBER SECURITY POLICIES

A cybersecurity policy sometimes referred to as an information security policy or IT security policy is a structured epitome of regulations, rules, and protocols established by an organization to protect its information technology systems, data, and assets from potential cyber attacks and security breaches. The principal objective of a cybersecurity policy is to develop a comprehensive structure for the management and mitigation of cybersecurity risks. Additionally, it aims to ensure that all individuals, including employees and stakeholders, possess a clear understanding of their respective roles and duties in maintaining an adequate computer systems environment. Mainly the organization is using information security concepts and technology in order to maintain the confidentiality, integrity, and availability (CIA) of its information assets and systems.

Our understanding of common cybersecurity policies for different businesses and the best practices is limited. The increase in cyberattacks has led to substantial business losses, emphasizing the need for better security solutions. This study examines security policies across various sectors to give a comprehensive view of electronic security. It has identified some important aspects of cybersecurity, including privacy, website security, Cloud security, email security, physical security, network security, information security, access control, data retention, and data protection.

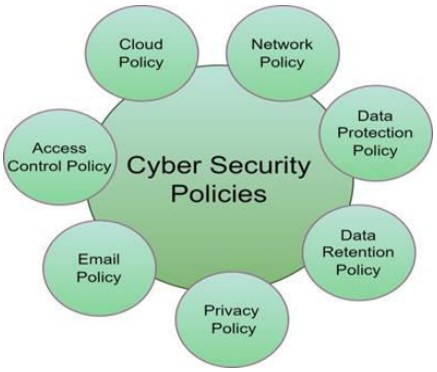

Fig. 1. Cybersecurity policies taxonomy

3.1 Privacy Policy:

The aim of this policy is to guide the proper use of sensitive personal data, like medical, biometric, and financial information, based on the agreed-upon reasons for using this data and to keep it safe from breaches. It prevents the unauthorized sharing, access, collection, transfer, or exchange of sensitive data by requiring user consent and the responsible handling of data by the organization in charge. This policy also safeguards both intellectual property and personal information, aligning with privacy rights and data protection. It imposes penalties on anyone who breaches consumer data privacy in a business context. In the U.S., federal privacy laws are grouped into four categories: protecting customer, children, patient, and credit card data.

3.2 Email Security Policy:

This policy has included in three main parts; the first part focuses on using emails as recommended by users [35]. It's all about explaining what's considered the right way to use email and educating employees about acceptable and unacceptable practices. This includes using email for work purposes only, safeguarding data and attachments sent by email, avoiding disruptive or offensive messages, and refraining from using the company's name for personal messages. The second part is about email security policies for administrators in businesses. The goal here is to monitor all email traffic and content, as well as storing and reviewing user emails. The third part promotes using encrypted communications and digital signatures to prevent spam messages when using email for communication.

3.3 Network Security Policy:

This policy is all about network security. It's aimed at making sure that the network components, connections, and what's being transmitted over the network are safe. This helps maintain a trustworthy network and ensures users know what's allowed and what's not. It involves protecting computer networks and communication equipment like routers, switches, and servers, as well as the data and services that travel through these networks. Special hardware like detection systems and firewalls are used to keep networks safe from unauthorized access or accidental changes. It also looks at defensive techniques, such as encryption, which keeps data safe when it's sent over the Internet. Plus, it focuses on secure network management.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

3.4 Access Control Policy

These rules aim to keep physical resources, information systems, and IT assets safe from unauthorized access by identifying, verifying, granting permission, and monitoring who can use them. They do this by using mechanisms like restrictions, access controls, permissions, and authorization to manage how individuals access an organization's resources or network services. Additionally, the access control policy ensures that only authorized people can take actions and regulates all entry to the organization's systems. Some organizations use authentication to manage access, while others use both authentication and authorization, depending on the organization's structure, the sensitivity of their data, and the level of access allowed for users.

3.5 Data-Retention Policy

This policy spells out what data to keep, how long to keep it, and in what format to store it. Its purpose is to safeguard important information by storing it in encrypted backups for a specific period. Additionally, it permits regular archiving, so organization members can easily access and delete unnecessary files, along with the encryption key for data security. For instance, the US Data Retention Act allows Internet service providers to retain data for two years. Some institutions can store this data under the Health Information Privacy and Accountability Act, while others cannot.

3.6 Data-Protection Policy

The aim of this policy is to safeguard the handling of personal data. It ensures that data from third parties is collected, used, shared, stored, transported, and sent securely for specific and necessary purposes. It also outlines the expected conduct of employees when dealing with this information. Additionally, the policy explains how companies should treat consumer data and promotes user awareness to prevent data loss. Since data security greatly influences a company's reputation, organizations should categorize and monitor data based on its type and sensitivity.

3.7 Cloud Computing Security Policy

This policy aims to ensure that Cloud services adhere to security standards and legal requirements. It's a document created by top management for the entire Cloud system to inform all employees and important external parties. The first part of the Cloud security policy covers various security aspects, including access control, data storage, and encryption. The second part deals with network security during data transmission. The third part focuses on computer security. To enable safe data exchange and interactions, the Cloud relies on a trusted third-party policy.

3.8 Website Security Policy:

This policy is about how to use online applications and services correctly. Its aim is to check how secure websites are and find vulnerabilities. It also protects important client information from harmful scripts on other pages, preventing attacks like scripting that can inject programs into web applications. The policy explains how to load content on websites and sets rules for accessing data from other pages with the same origin. A third-party web-tracking policy keeps an eye on a website's actions using consent-based cookies. Access control, through authorization rights, is used to secure personal data, like data on social media platforms.

IV. ML ALGORITHMS USED IN CYBER SECURITY

Machine learning stands as a pivotal technology in today's information systems and promises a significant role in shaping the future. Its applications span across diverse fields, showcasing its versatility. Despite its wide-reaching potential, there exists a notable disparity between the realms of research and practical implementation. Nowhere is this gap more conspicuous than in the nascent integration of machine learning into the domain of cybersecurity.

The prevailing state of affairs, where the true extent of machine learning's role in cybersecurity remains obscure, is the crux of this discrepancy. The full realization of machine learning's capabilities in bolstering cyber defenses hinges on a broader awareness of its merits and demerits. Until its advantages and limitations gain acknowledgment from a wider audience, the complete potential of machine learning in cybersecurity may remain untapped.

4.1 Decision Tree Algorithm:

Decision tree algorithms can be used effectively for detecting and classifying attacks in cybersecurity. They are a type of supervised machine learning algorithm that can analyze and classify data based on a set of rules and conditions. Using a Genetic Algorithm for the global feature search while using a Decision Tree Classifier for determining the minimum required features for each specific attack studied, reduce false positives, and reduce classification time. In [23] the normal and abnormal network traffic data were unevenly distributed, we employed both standard and additional performance scores (F2-score, Area Under ROC Curve) for a more precise assessment. The RF Classifier demonstrated superior performance with an F2-score of 97.68% and an AUC score of 98.47%. To expedite

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

computations, we utilized a smaller dataset. Features in the reference dataset were reduced by 82%, aligning with the NetFlow data stream structure. This paper compares diverse algorithms for anomaly detection in NetFlow data streams, ultimately selecting the best-performing one based on similar studies.

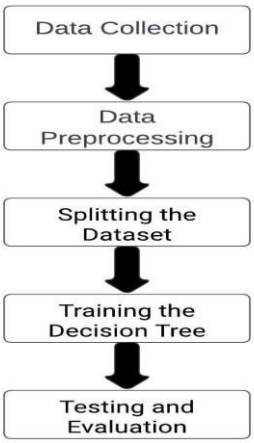

Fig 2. Decision Tree in Machine Learning

4.2 **Dimensionality Reduction Algorithms:**

These algorithms are utilized to simplify the dataset by reducing the number of variables or dimensions, which can be particularly beneficial in scenarios where the original dataset has a high number of features. The objective is to retain the critical characteristics and patterns of the data while minimizing redundancy and noise, ultimately improving computational efficiency and sometimes enhancing the performance of machine learning models. There are often too many factors to work with in machine learning tasks like classification or regression. Such characteristics can also be called features. As the number of features is high, it is more diligent to model them. This phenomenon is known as the "curse of dimensionality." The issues arise with high dimensional data are: (1) Running a risk of overfitting the machine learning model (2) Difficulty in clustering similar features (3) Increased space and computational time complexity. Decomposition algorithm and Principal Component Analysis (PCA), Singular value decomposition (SVD) has been applied to cyber security and cyber forensics since it can reduce data. However, SVD is hard to reduce high-order big data because it is designed for only matrix data initially [65]. Non-negative Matrix Factorization (NMF) [66], Manifold learning, t-Distributed Stochastic Neighbor Embedding (t-SNE), Locally Linear Embedding (LLE) algorithms are also used.

4.3 K-Means Clustering Algorithms:

K-means clustering is a popular unsupervised machine learning algorithm that can be used for detecting malware by grouping similar samples together. Here's a high-level overview of how K-means clustering can be applied in the context of malware detection

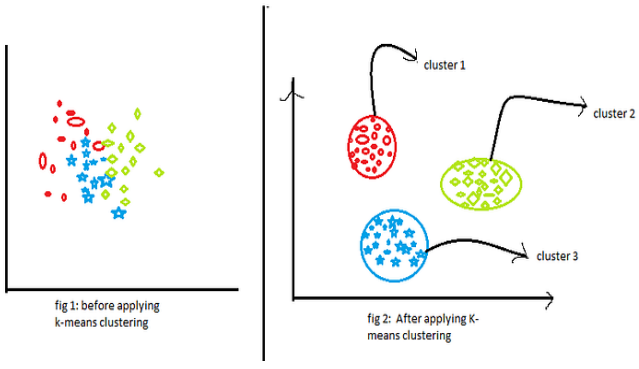

Fig 3. K-Means Clustering

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

Gather a dataset of malware samples, represented by features extracted from the samples. Features could include static analysis attributes like file size, byte frequencies, and entropy, as well as dynamic analysis attributes like API calls, system calls, or network activities. Extract the relevant features from the malware samples. This step involves transforming the raw data into a suitable format for clustering [24]. It is essential to choose features that capture the distinct characteristics of malware while minimizing noise and irrelevant information. Data Preprocessing is also an important and then selecting the number of clusters for analysis. It's important to note that K-means clustering alone may not provide a complete solution for detecting malware. It is often used as one component within a broader malware detection system, which could include other machine learning algorithms, feature selection techniques, and domain knowledge expertise.

4.4 K-Nearest Neighbors (kNN)Algorithms:

Facial recognition using kNN [26] offers a straightforward and effective approach to authentication, particularly in scenarios where a sufficient amount of labeled facial data is available for training. However, it's crucial to address potential challenges such as variations in lighting conditions, facial expressions, and occlusions to enhance the robustness of the system. In this experiment the accuracy rate is 92.5% without false positive error. In describes in depth how the identification of a real time face can be order to create a safety alert framework for the workplace, the machine learning algorithm Haarcascade classifier was used to build four distinct classes for identification of security equipment and eventually identify the faces in both images and video using python open CV.

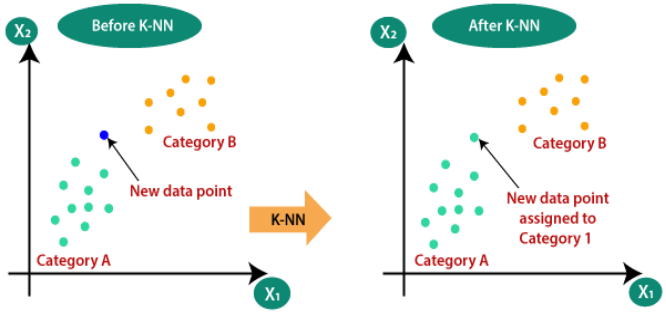

Fig 4. KNN Algorithm

4.5 Linear Regression:

Linear regression can be applied to predict network security outcomes by establishing a relationship between various factors (independent variables) and the security outcome of interest (dependent variable). It's important to note that while linear regression is a valuable tool, network security is a complex field, and other machine learning techniques, such as classification algorithms or anomaly detection methods, may be used in conjunction with linear regression for a more comprehensive security strategy. Additionally, the success of the model depends on the quality and relevance of the data used for training. This study estimates network security threats (Source: Devoteam report) [25].

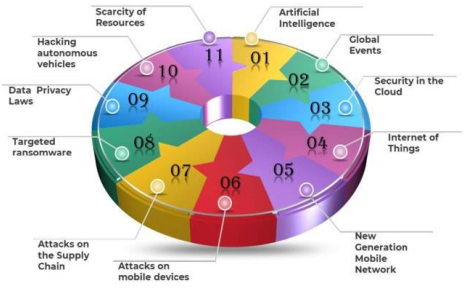

Fig 5. Cybersecurity Threats and Vulnerabilities

4.6 Logistic Regression:

Logistic regression is a commonly used algorithm for binary classification tasks, making it suitable for fraud detection where the goal is to classify transactions or activities as either fraudulent or non-fraudulent. In [20] the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

logistic regression algorithm accuracy will be nearer to 0.99% with this accuracy we can easily identify the frauds. We have used creditcard dataset (2019) for detecting the fraud.

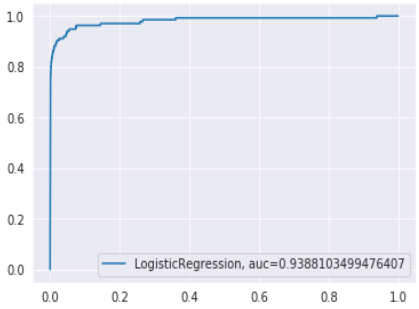

Fig 6. Logistic Regression

V. CONCLUSION

The integration of machine learning in cybersecurity holds immense potential to enhance the efficiency, scalability, and efficacy of cybersecurity practices. This article has explored the fundamental concepts of machine learning and its application in various cybersecurity domains, ranging from threat detection on networks to securing cloud-stored data. By leveraging ML algorithms, cybersecurity professionals can benefit from advanced threat detection capabilities, rapid response mechanisms, and improved protection against a diverse range of cyber threats. This article delves into the taxonomy of cybersecurity policies, highlighting the critical role these policies play in safeguarding information technology systems, data, and assets from cyber threats. As technology continues to advance, the continued exploration and integration of machine learning solutions will be pivotal in staying ahead of sophisticated cyber adversaries.

REFERENCES

[1] Sarker, Iqbal H., "Machine Learning: Algorithms, Real-World Applications and Research Directions", SN Computer Science, pp. 160-167, 2021.

[2] A] Sarker, Iqbal H. "Machine Learning: Algorithms, Real-World Applications and Research Directions." SN Computer Science, vol. 2, no. 3, May 2021, p. 160. DOI.org (Crossref), https://doi.org/10.1007/s42979-021-00592-x

[3] Xu, Yongjun, et al. "Artificial Intelligence: A Powerful Paradigm for Scientific Research." The Innovation, vol. 2, no. 4, Nov. 2021, p. 100179. DOI.org (Crossref), https://doi.org/10.1016/j.xinn.2021.100179.

[4] Singh, Dr. Brahampal, and Dr. Anukool Bajpai. "Status and Analysis of Cyber Security Infrastructure in Current Scenario." SSRN Electronic Journal, 2022. DOI.org (Crossref), https://doi.org/10.2139/ssrn.4040978.

[5] Lowe, G. "Some New Attacks upon Security Protocols." Proceedings 9th IEEE Computer Security Foundations Workshop, IEEE Comput. Soc. Press, 1996, pp. 162–69. DOI.org (Crossref), https://doi.org/10.1109/CSFW.1996.503701.

[6] Sun, Chia Ming, et al. "Protective Shields: The Drivers of Adopting Information Security Standards and Complementarity with Different Security Standards." International Journal of Services and Standards, vol. 13, no. 3/4, 2023, pp. 195–220. DOI.org (Crossref), https://doi.org/10.1504/IJSS.2023.132773.

[7] Youssef, M. W. "Securing Authentication of TCP/IP Layer Two By Modifying Challenge-Handshake Authentication Protocol." Advanced Computing: An International Journal, vol. 3, no. 2, Mar. 2012, pp. 93–16. DOI.org (Crossref), https://doi.org/10.5121/acij.2012.3202.

[8] Majid, Abdul. "Manajemen Jaringan Menggunakan Remote Authentication Dial in User Service (RADIUS)." Journal of System and Computer Engineering (JSCE), vol. 1, no. 2, Jan. 2021, pp. 20–32. DOI.org (Crossref), https://doi.org/10.47650/jsce.v1i2.140.

[9] Ferraiolo, David F., et al. "Proposed NIST Standard for Role-Based Access Control." ACM Transactions on Information and System Security, vol. 4, no. 3, Aug. 2001, pp. 224–74. DOI.org (Crossref), https://doi.org/10.1145/501978.501980.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303031 |

[10] Shendkar, Parth, et al. "Attribute-Based Access Control for Secure Firmware Over-The-Air Updates in Vehicles." 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, 2023, pp. 257–61. DOI.org (Crossref), https://doi.org/10.1109/I-SMAC58438.2023.10290472.

[11] Hu, Vincent C., et al. "Model Checking for Verification of Mandatory Access Control Models and Properties." International Journal of Software Engineering and Knowledge Engineering, vol. 21, no. 01, Feb. 2011, pp. 103–27. DOI.org (Crossref), https://doi.org/10.1142/S021819401100513X.

[12] Al-Jarrah, Omar Y., et al. "Intrusion Detection Systems for Intra-Vehicle Networks: A Review." IEEE Access, vol. 7, 2019, pp. 21266–89. DOI.org (Crossref), https://doi.org/10.1109/ACCESS.2019.2894183.

[13] Chebrolu, Srilatha, et al. "Feature Deduction and Ensemble Design of Intrusion Detection Systems." Computers & Security, vol. 24, no. 4, June 2005, pp. 295–307. DOI.org (Crossref), https://doi.org/10.1016/j.cose.2004.09.008

[14] Alawatugoda J. Authenticated Key Exchange Protocol in the Standard Model under Weaker Assumptions. *Cryptography*. 2023; 7(1):1. https://doi.org/10.3390/cryptography7010001

[15] Biswas M, Das D, Banerjee S, Mukherjee A, AL-Numay W, Biswas U, Zhang Y. Blockchain-Enabled ommunication Framework for Secure and Trustworthy Internet of Vehicles. *Sustainability*. 2023; 15(12):9399. https://doi.org/10.3390/su15129399

[16] Xiong Z, Zhang Y, Niyato D, Wang P, Han Z (2018) When Mobile Blockchain meets edge computing. IEEE Commun Mag 56(8):33–39. https://doi.org/10.1109/MCOM.2018.1701095

[17] Dai Y, Guan YL, Leung KK, Zhang Y (2021) "Reconfigurable Intelligent Surface for Low-Latency Edge Computing in 6G." IEEE Wirel Commun 28(6):72–79. https://doi.org/10.1109/MWC.001.2100229.

[18] haveri RH, Revathi A, Ramana K, Raut R, Dhanaraj RK. A review on machine learning strategies for real-world engineering applications. Hakak S, ed. Mobile Information Systems. 2022;2022:1-26. https://doi.org/10.1155/2022/1833507

[19] Das R, Morris TH. Machine learning and cyber security. In: 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE). Kolkata: IEEE; 2017:1-7. https://doi/10.1109/ICCECE.2017.8526232

[20] Calix RA, Singh SB, Chen T, Zhang D, Tu M. Cyber security tool kit (Cybersectk): a python library for machine learning and cyber security. Information. 2020;11(2):100. https://doi/10.3390/info11020100

[21] Devika M, Kishan SR, Manohar LS, Vijaya N. Credit card fraud detection using logistic regression. In: 2022 econd International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE). Bangalore, India: IEEE; 2022:1-6. https://doi/10.1109/ICATIECE56365.2022.10046976

[22] Brunt CM, Heyer MH. Principal component analysis of spectral line data: analytic formulation. Monthly Notices of the Royal Astronomical Society. 2013;433(1):117-126. https://doi/10.1093/mnras/stt707

[23] Cains MG, Flora L, Taber D, King Z, Henshel DS. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis. 2022;42(8):1643-1669. https://doi/10.1111/risa.13687

[24] Rana S. Anomaly detection in network traffic using machine learning and deep learning techniques. TURCOMAT. 2019;10(2):1063-1067. https://doi/10.17762/turcomat.v10i2.13626

[25] Alejandro Germ´an FRANK, Lucas Santos DALENOGARE, N´estor Fabi´an AYALA, Industry 4.0 technologies: implementation patterns in manufacturing companies, International Journal of Production Economics 210 (2019) 15–26.

[26] Yun, Su. "Research on Eigenvalue Decomposition Algorithm: —Based on Polarization Calibration." 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC), IEEE, 2022, pp. 459–63. https://doi.org/10.1109/ICNISC57059.2022.00097.

[27] Parizad, Ali, and Constantine J. Hatziadoniu. "Cyber-Attack Detection Using Principal Component Analysis and Noisy Clustering Algorithms: A Collaborative Machine Learning-Based Framework." IEEE Transactions on Smart Grid, vol. 13, no. 6, Nov. 2022, pp. 4848–61., https://doi.org/10.1109/TSG.2022.3176311.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details