Grenze International Journal of Engineering and Technology, June Issue

Cyber Security in IOT based Electronics & Communication Systems using AI & ML techniques – A comprehensive Review of the Design Concepts for Implementation in Digital World with Applications

P. Sai Laasya[1], Dr. Pavithra G[2] and Dr.T.C.Manjunath[3]
[1]Third Year UG BE (ECE) Student, Dept. of Electronics & Communication Engg, Dayananda Sagar College of Engineering, Shavigemalleshwara Hills, Kumaraswamy Layout, Bangalore-111, Karnataka, India
Email: sailaasya29@gmail.com
[2]Associate Professor & Supervisor, Dept. of Electronics & Communication Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka
Email: dr.pavithrag.8984@gmail.com
[3]Professor & Head, Co-Supervisor, Dept. of Electronics & Communication Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka
Email: tcmanju@iitbombay.org

***Abstract*— Artificial Intelligence (AI) & Machine Learning (ML) stands as a robust technology empowering cybersecurity team with the automation of repetitive tasks, expediting threat detection and response, and enhancing the precision of actions to fortify security against a myriad of threats and cyberattacks. This article conducts a meticulous systematic literature review, analyzing the diverse use cases of AI in cybersecurity. Out of 2395 studies examined, 236 were identified as primary sources. Employing a thematic analysis approach and aligning with the NIST cybersecurity framework, this article categorizes the identified AI use cases. The resulting classification framework offers readers a comprehensive understanding of AI's potential to enhance cybersecurity across various contexts. The review also unveils future research prospects in burgeoning cybersecurity application domains, advanced AI methodologies, data representation techniques, and the establishment of novel infrastructures, pivotal for the successful integration of AI-based cybersecurity in the contemporary landscape marked by digital transformation and polycrisis. This research delves into the domain of cybersecurity within electronic communication systems, employing advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques. The study aims to present comprehensive design concepts for the implementation of robust cybersecurity measures. With the ever-growing complexity and sophistication of cyber threats, the integration of AI and ML becomes imperative to fortify electronic communication systems against potential risks. The research explores innovative approaches, strategies, and technologies, offering a holistic view of how AI and ML can be effectively harnessed to enhance cybersecurity in electronic communication systems. The outcomes of this study provide valuable insights for the development and implementation of advanced cybersecurity measures in the realm of electronic communications.**

***Index Terms*— Cybersecurity, Electronics, Communication Systems, Artificial Intelligence (AI), Machine Learning (ML), Design Concepts, Implementation, Digital World, Applications**

Grenze ID: 01.GIJET.10.2.544

I. INTRODUCTIONS

Cybersecurity establishes policies, procedures, and technical mechanisms to safeguard information and communication systems, aiming to protect, detect, correct, and defend against damage, unauthorized use, modification, or exploitation [2]. The ever-accelerating pace of technological change, coupled with the dynamic nature of cyber threats, adds complexity to the landscape. In response to this formidable challenge, AI-based cybersecurity tools have emerged, aiding security teams in efficiently mitigating risks and enhancing overall security measures. Given the diverse landscape of AI and cybersecurity, the need for a universally accepted and consolidated taxonomy becomes evident to systematically explore the literature on the application of AI in cybersecurity [3]. Such a structured taxonomy serves to foster a common understanding among researchers and practitioners regarding the technical procedures and services that AI can enhance for effective cybersecurity implementation [1].

To address this need, the study employs the cybersecurity framework proposed by the National Institute of Standards and Technology (NIST), which outlines solution categories for protecting, detecting, reacting, and defending against cyberattacks [3]. The NIST cybersecurity framework's core incorporates functions, categories, subcategories, and informative references. The first two levels, consisting of five cybersecurity functions and 23 solution categories, were utilized to categorize identified AI use cases. These functions provide a holistic view of the cybersecurity lifecycle, while the solution categories serve as a foundation for identifying AI use cases to bolster cybersecurity [4]. By selecting these two levels, the study aims to offer a clear and intuitive categorization, classifying existing AI for cybersecurity literature into the appropriate solution category. The proposed taxonomy introduces a third level consistent with the first two levels, specifying AI-based use cases corresponding to each level of the cybersecurity framework. This taxonomy enhances the understanding of how AI can be applied across different facets of cybersecurity, facilitating a structured exploration of literature and fostering a standardized approach to advancing AI in cybersecurity practices. The Fig. 1 gives the concepts of AI in cyber security [35].

Fig. 1 : AI in cyber security [35] & AI in cyber-Security with bolstering defense mechanisms [35]

II. AI IN CYBER-SECURITY: BOLSTERING DEFENSE MECHANISMS AGAINST CYBER THREATS

There are a number of applications for AI in cybersecurity, six of them are explained as follows in the communication scenarios [5].

Proactive Threat Detection: Utilizing AI for real-time data analysis enables the identification of anomalies and potential threats with heightened accuracy. AI's capability to discern patterns in data beyond human capacity enhances threat recognition, often overlooked by traditional security tools. For instance, AI can analyze network traffic, revealing suspicious patterns like an unusually high volume of connections from a single IP address [6].

Automated Incident Response: AI's rapid threat identification and response capabilities facilitate automated incident handling, minimizing damage and expediting recovery without human intervention. For example, AI can automate actions such as quarantining infected devices or rolling back changes made by malicious actors [7].

Behavioral Analysis & User Monitoring: AI excels in detecting suspicious user activities, providing protection against insider threats by learning and recognizing normal user behavior. It can identify deviations from this established behavior, such as detecting unauthorized attempts to access sensitive data from an unusual location [8].

Threat Intelligence and Prediction: AI processes threat intelligence data to predict and prevent potential threats, leveraging its ability to learn about known threats and identify emerging ones. For instance, AI can predict systems likely to be targeted by specific threat actors based on accumulated knowledge [9].Anomaly-Based Intrusion Detection: AI's proficiency in identifying deviations from normal behavior aids in detecting zero-day attacks by learning and recognizing typical system behavior. For example, AI can identify abnormal system behavior, serving as an indicator of a potential zero-day attack [10].

Enhanced Phishing Detection: AI enhances the identification of phishing attempts by analyzing emails and URLs, distinguishing them from legitimate communications. Through learning the characteristics of phishing emails and URLs, AI can effectively identify suspicious senders or malicious website links [11].

III. Role Of Artificial Intelligence & Machine Learning In Cyber Security

AI and ML hold the potential to automatically analyze data from diverse sources, including network traffic, endpoint data, and logs, enabling real-time identification and response to threats. This capability empowers organizations to swiftly contain and investigate incidents. Referencing Fig. 2, it illustrates the role of AI in cybersecurity, reinforcing defense mechanisms [35].
Goal is the overarching objective of artificial intelligence is to replicate human intelligence, showcasing substantial promise in the realm of cybersecurity. AI systems, when effectively implemented, can undergo training to detect threats, identify novel malware types, and safeguard sensitive data [12].
Security Threats and Issues in WSN are Wireless Sensor Networks (WSN) face vulnerabilities to security attacks due to the broadcast nature of the transmission medium. Attacks are broadly categorized into two types: active attacks and passive attacks [13].
Types of AI Used in Cybersecurity are Various types of AI are employed in cybersecurity, including machine learning, expert systems, neural networks, and deep learning. Machine learning, for instance, utilizes statistical techniques to enable computer systems to learn from data, progressively improving performance without explicit programming [14].
ML Usage in Cybersecurity can be used for Machine learning contributes to safeguarding productivity by analyzing suspicious cloud app login activity, detecting anomalies based on location, and conducting IP reputation analysis to identify threats and risks in cloud apps and platforms [15].
AI in Cybersecurity Improvement can be done by automating incident response, streamlining threat hunting, and analyzing extensive datasets, plays a pivotal role in enhancing cybersecurity. Advances in computational power and scalability offer promising glimpses into the future of AI, contributing to a safer online environment [16].

IV. Artificial Intelligence (Ai) In Changing Cybersecurity Models

AI is used in cybersecurity for real-time threat detection, behavior and prediction analysis, anomaly detection based on the established baseline, automation and orchestration of repetitive tasks, better end-point protection automation and more [17]. In an era of increasing digitalization, the escalation of Cyber Security threats is a daily concern. A pressing challenge for IT security professionals is finding effective measures to prevent fraudulent activities and save billions of dollars annually. Addressing cyber threats requires a comprehensive analysis of all data to identify potential risks. This is precisely where AI plays a crucial role, streamlining the laborious processes of data analysis, screening, and risk detection. This blog delves into the intricate use of AI in Cybersecurity. Refer to Fig. 3 for a broad illustration of an Internet of Things-based security system [33].

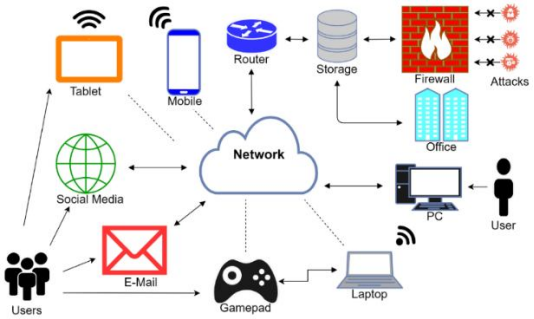

Fig 3 : General representation of an Internet of Things based security system [33]

V. Threats Facing In Cybersecurity Industry

Cybersecurity introduces distinctive threats, encompassing:

- A vast attack surface
- The need to safeguard numerous devices within each organization
- Numerous attack vectors exploitable by cybercriminals

- A considerable shortage of skilled security professionals to meet escalating demands
- Overwhelming volumes of data surpassing human-scale processing capacity, posing a formidable challenge in analysis and comprehension.

AI and machine learning are increasingly important for prevention against cybersecurity threats, they can analyse large amounts of data to detect risks like phishing and malware. The Fig. 4 gives the machine learning flow in intrusion detection [35].

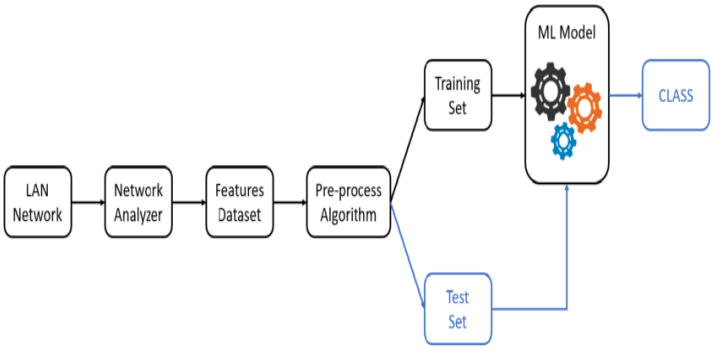

Fig. 4: A machine learning flow in intrusion detection

Nevertheless, cybercriminals possess the capability to modify malware code in order to elude detection. Machine Learning (ML) proves highly effective for anti-malware protection, leveraging insights from previously identified malware to recognize new variants. This capability remains robust even when malicious code is concealed within seemingly innocent code. The utilization of AI-powered network monitoring tools enables the tracking of user behavior, detection of anomalies, and responsive actions [18]. These technologies operate in real-time, halting threats without disrupting business processes, and can monitor data that may go unnoticed by human observers, including videos, chats, emails, and other communications. Refer to Fig. 5 for an illustration of the sources of cyber threats in communication systems, and Fig. 6 for the various types of cyber-attacks [34]..

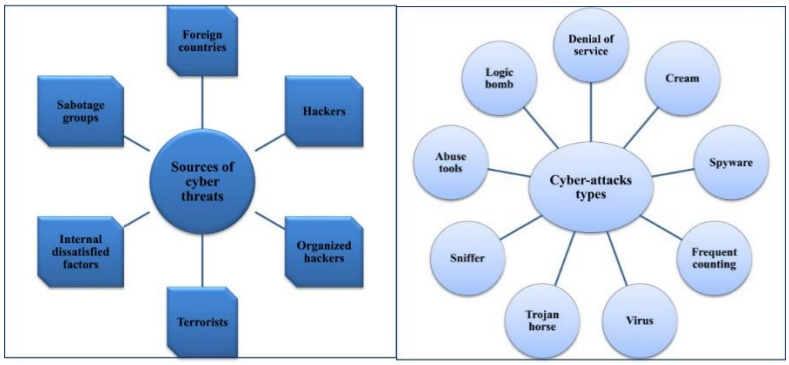

Fig. 5 : Sources of cyber threats in communication systems [34] & Cyber security & its types [34]

VI. Usage Of Ai & Ml In Cyber Security

Machine-learning-in-cybersecurity is used for a variety of applications, some of them are listed as follows - To classify data, To cluster the data, To recommend courses of action, Possibility synthesis, Predictive forecasting.

VII. Future Of Ai For Cybersecurity - Artificial Intelligence In Cybersecurity: Advantages, Challenges, And Integration

Artificial Intelligence (AI) plays a pivotal role in shaping the landscape of cybersecurity, bringing forth both advantages and challenges. On one hand, AI enhances the analysis, comprehension, and prevention of cybercrime, instilling trust and safety in companies and their clientele. However, the resource-intensive nature of AI and its potential exploitation by cybercriminals pose significant challenges. The realm of Virtual Private Networks (VPNs) stands out as an industry reaping the benefits of AI, employing machine learning to shield users from

online threats orchestrated by AI. The discussion surrounding the utilization of AI in cybersecurity gained prominence two years ago, emphasizing the rapid data analysis capabilities intrinsic to AI technology [31][32].

VIII. Conclusions

In conclusion, the primary AI use case in cybersecurity is indispensable for elevating IT security performance at the enterprise level. Through its capabilities in analysis and threat identification, AI aids security professionals in minimizing breach risks, prioritizing threats, orchestrating incident responses, and preemptively detecting malware attacks. While acknowledging potential drawbacks, it is evident that AI will propel the field of cybersecurity forward, contributing to the overall enhancement of organizations' security postures. In conclusion, this research on cybersecurity in electronic communication systems employing AI and ML techniques has revealed a comprehensive set of design concepts for implementation. The integration of AI and ML proves to be pivotal in addressing the intricate challenges posed by evolving cyber threats in the realm of electronic communication. The study underscores the significance of advanced technologies in fortifying security measures, offering an exhaustive exploration of innovative strategies and approaches.

References

[1] Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar Secure framework against cyber-attacks on cyber-physical robotic systems, J. Electron. Imaging, 31 (6) (2022), 061802-061802

[2] P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan, Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks, IEEE Internet Things J (2023), 10.1109/JIOT.2022.3231605

[3] M. Barrett, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA (2018)

[4] Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver, Artificial intelligence for cybersecurity: a systematic mapping of literature, IEEE Access, 8 (2020), pp. 146598-146612

[5] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artif. Intell. Rev., 55 (2022), pp. 1029-1053

[6] J. Martínez Torres, C. Iglesias Comesaña, P.J. García-Nieto, Machine learning techniques applied to cybersecurity, Int. J. Mach. Learn. Cybern., 10 (10) (2019), pp. 2823-2836

[7] T.C. Truong, I. Zelinka, J. Plucar, M. Čandík, V. Šulc, Artificial intelligence and cybersecurity: past, presence, and future, Artificial intelligence and evolutionary computations in engineering systems (2020), pp. 351-363

[8] S. Samoili, M.L. Cobo, E. Gomez, G. De Prato, F. Martinez-Plumed, B. Delipetrev, A.I. Watch, Technical report, Joint Research Center (Seville site) (2020)

[9] High-Level Expert Group on Artificial Intelligence. (HLEG AI), A definition of AI: main capabilities and disciplines, (2019).

[10] D. Zhao, A. Strotmann, Analysis and visualization of citation networks, Synthesis lectures on information concepts, retrieval, and services, 7 1 (2015) 1–207.

[11] V.G. Promyslov, K.V. Semenkov, A.S. Shumov, A clustering method of asset cybersecurity classification

[12] IFAC-PapersOnLine, 52 (13) (2019), pp. 928-933

[13] K. Millar, A. Cheng, H.G. Chew, C.C. Lim, Operating system classification: a minimalist approach 2020 International Conference on Machine Learning and Cybernetics (ICMLC) (2020), pp. 143-150

[14] Aksoy, M.H. Gunes, Automated iot device identification using network traffic, IEEE International Conference on Communications (ICC) (2019), pp. 1-7

[15] Sivanathan, H.H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman, Classifying IoT devices in smart environments using network traffic characteristics, IEEE Trans. Mobile Comput., 18 (8) (2018), pp. 1745-1759

[16] Cvitić, D. Peraković, M. Periša, B. Gupta, Ensemble machine learning approach for classification of IoT devices in smart home, Int. J. Machine Learn. Cybernetics, 12 (11) (2021), pp. 3179-3202

[17] H. Cam, Online detection and control of malware infected assets, IEEE Military Communications Conference (MILCOM) (2017), pp. 701-706

[18] H.I. Kure, S. Islam, M. Ghazanfar, A. Raza, M. Pasha, Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system, Neural Comput. App., 34 (1) (2022), pp. 493-514

[19] M. Vega-Barbas, V.A. Villagrá, F. Monje, R. Riesco, X. Larriva-Novo, J. Berrocal, Ontology-based system for dynamic risk management in administrative domains, Appl. Sci., 9 (21) (2019), p. 4547

[20] Tozer, T. Mazzuchi, S. Sarkani, optimizing attack surface and configuration diversity using multi-objective reinforcement learning, IEEE 14th international conference on machine learning and applications (2015), pp. 144-149

[21] L.E. García-Hernández, A. Tchernykh, V. Miranda-López, M. Babenko, A. Avetisyan, R. Rivera-Rodriguez, G. Radchenko, C.J. Barrios-Hernandez, H. Castro, A.Y. Drozdov, Multi-objective configuration of a secured distributed cloud data storage Latin American High Performance Computing Conference (2019), pp. 78-93 Sep.

[22] M. Sharifi, F. Eugene, J.G. Carbonell, Learning of personalized security settings, IEEE International Conference on Systems, Man and Cybernetics (2010), pp. 3428-3432

[23] Bringhenti, G. Marchetto, R. Sisto, F. Valenza, F.J. Yusupov, Towards a fully automated and optimized network security functions orchestration, 4th International Conference on Computing, Communications and Security (ICCCS) (2019), pp. 1-7
[24] Á.J. Varela-Vaca, R.M. Gasca, J.A. Carmona-Fombella, M.T. Gómez-López, AMADEUS: towards the AutoMAteD security testing, Proceedings of the 24th ACM Conference on Systems and Software Product Line (2020), pp. 1-12
[25] Á.J. Varela-Vaca, R.M. Gasca, R. Ceballos, M.T. Gómez-López, P.B. Torres, CyberSPL: a framework for the verification of cybersecurity policy compliance of system configurations using software product lines, Appl. Sci., 9 (24) (2019), p. 5364
[26] Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, M. Bailey, M. Liu, Cloudy with a chance of breach: forecasting cyber security incidents, 24th USENIX Security Symposium (USENIX Security 15) (2015), pp. 1009-1024
[27] Z. Zhan, M. Xu, S. Xu, A characterization of cybersecurity posture from network telescope data, International Conference on Trusted Systems (2014), pp. 105-126
[28] S.N.G. Gourisetti, M. Mylrea, E. Gervais, S. Bhadra, Multi-scenario use case-based demonstration of buildings cybersecurity framework webtool, 2017 IEEE Symposium Series on Computational Intelligence (SSCI) (2017), pp. 1-8
[29] L.V. Stepanov, A.S. Koltsov, A.V. Parinov, Evaluating the cybersecurity of an enterprise based on a genetic algorithm International Russian Automation Conference (2020), pp. 580-590
[30] V.L. Narasimhan, Using deep learning for assessing cybersecurity economic risks in virtual power plants
[31] 2021 7th International Conference on Electrical Energy Systems (ICEES) (2021), pp. 530-537
[32] H.H. Nguyen, D.M. Nicol, estimating loss due to cyber-attack in the presence of uncertainty, 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2020), pp. 361-369
[33] Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects. Electronics 2022, 11, 1502.
[34] Yuchong Li, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN 2352-4847.
[35] https://datasciencedojo.com/blog/ai-in-cybersecurity/#
[36] https://www.stanfieldit.com/the-role-of-ai-and-ml-in-business-cyber-security/
[37] Larriva-Novo, X., Villagrá, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors, 21(2), 656. 656.Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. Artificial Intelligence, 7(9)
[38] Machin, J., Batista, E., Martínez-Ballesté, A., & Solanas, A. (2021). Privacy and security in cognitive cities: A systematic review. Applied Sciences, 11(10), 4471.
[39] Maleh, Y., Baddi, Y., Alazab, M., Tawalbeh, L., & Romdhani, I. (Eds.). (2021). Artificial intelligence and blockchain for future cybersecurity applications (Vol. 90). Springer Nature.Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. Future Internet, 15(2), 83. https://doi.org/10.3390/fi15020083
[40] Mazhar, T., Muhammad Irfan, H., Haq, I., Ullah, I., Ashraf, M., Al Shloul, T., Yasin Ghadi, Y., & Elkamchouchi, D. H. (2023). Analysis of challenges and solutions of IoT in smart grids using AI and machine learning techniques: A review. Electronics, 12(1), 242.
[41] Shashank S., Kushal K., Abhay Surya Shankar, Madan Kumar G., Dr. Pavithra G., Dr. Sindhu Sree M., Padmavathy M., Dr. T.C. Manjunath, "RFID based attendance system with SMS Alert", Scopus Journal Q3, Schimago Ranking SJR 2022 0.32, H-Index 24, Tuijin Jishu/Journal of Propulsion Technology, ISSN: 1001-4055, Vol. 44, No. 3, pp. 774 – 782, Jul. - Sept. 2023.
[42] Abhishek, Sujith M.S., Jeevan D., P. Kamalesh, Dr. Sindhu Sree M., Dr. Pavithra G., Dr. T.C. Manjunath, "Design & Development of a Table Assisted Robotic Arm", Scopus Journal Q3, Schimago Ranking SJR 2022 0.32, H-Index 24, Tuijin Jishu/Journal of Propulsion Technology, ISSN: 1001-4055, Vol. 44, No. 3, pp. 818 – 822, Jul. - Sept. 2023.
[43] Apeksha U., Chithrashree G.S., Divya N.M., Shalmali S. Mankikar, Dr. Sindhu Sree M., Dr. Pavithra G., Dr. T.C. Manjunath, "Wireless LoRa Communication Between Two Arduino Uno for Military Application in Soldier Tracking", Scopus Journal Q3, Schimago Ranking SJR 2022 0.32, H-Index 24, Tuijin Jishu/Journal of Propulsion Technology, ISSN : 1001- 4055, Vol. 44, No. 3, pp. 768 – 773, Jul. - Sept. 2023.
[44] Akarsh Kesharwani, Ayush P. Chaudhary, Bhanu Pratap Singh, Ved Kumar, Padmavathi M., Dr. Pavithra G., Dr. Sindhu Sree M., Dr. T.C. Manjunath, "A Study on Hand Motion Controlled Robotic Arm", Scopus Journal Q3, Schimago Ranking SJR 2022 0.32, H-Index 24, Tuijin Jishu/Journal of Propulsion Technology, ISSN: 1001-4055, Vol. 44, No. 3, pp. 812 – 817, Jul. - Sept. 2023.
[45] Leena Jeyakumar, Prerana Aithal, Vismitha R., Pradhan Aithal, Dr. Pavithra G., Dr. Sindhu Sree M., Dr. T.C. Manjunath, "Development of Smart Bridge – Automatic Height Increase When Floodings Take Place", Scopus Journal Q3, Schimago Ranking SJR 2022 0.32, HIndex 24, Tuijin Jishu/Journal of Propulsion Technology, ISSN: 1001-4055, Vol. 44, No. 3, pp. 763 – 767, Jul. - Sept. 2023.