Leveraging Machine Learning for Advanced Cybersecurity in Next-Generation Networks

Diginomics.
2025; 4:181
DOI: 10.56294/digi2025181
ISSN: 3072-8428

Aprovechamiento del aprendizaje automático para una ciberseguridad avanzada en redes de próxima generación

Md. Alimul Haque[1], **Kushboo Mishra**[2], **B. K. Mishra**[2]

[1]Department of Computer Science, Veer Kunwar Singh University, Ara. India.
[2]P.G. Department of Physics, Veer Kunwar Singh University, Ara. India.

Cite as: Alimul Haque M, Mishra K, Mishra BK. Leveraging Machine Learning for Advanced Cybersecurity in Next-Generation Networks. Diginomics. 2025; 4:181. https://doi.org/10.56294/digi2025181

Corresponding author: Md. Alimul Haque

ABSTRACT

Introduction: as technology advances rapidly, cybersecurity has become a pressing global issue. The growing complexity of cyber threats presents significant challenges to individuals, organizations, and governments alike.
Objective: cybersecurity tools are essential for detecting, monitoring, and mitigating these risks, ensuring data security, preventing unauthorized access, and protecting sensitive information. However, conventional methods often fall short in addressing the sophistication of modern cyber-attacks.
Method: machine learning (ML) has emerged as a transformative approach to strengthening cybersecurity. By analyzing vast datasets, ML algorithms can identify anomalies and predict threats with higher precision. When integrated into cybersecurity frameworks, ML enhances defenses against issues like data breaches, identity theft, and system intrusions.
Result: this research focuses on utilizing ML to develop and optimize cybersecurity models tailored for enterprise ICT systems. Additionally, it highlights the increasing demand for experts capable of designing and implementing ML-driven security solutions.
Conclusion: by exploring emerging trends, this study underscores the pivotal role of ML in fortifying digital security globally.

Keywords: Cyber Security; Data Analysis; Cybercrime; ML Algorithms; Threats; Network Security.

RESUMEN

Introducción: con el rápido avance de la tecnología, la ciberseguridad se ha convertido en un problema global urgente. La creciente complejidad de las amenazas cibernéticas plantea importantes retos tanto para las personas como para las organizaciones y los gobiernos.
Objetivo: las herramientas de ciberseguridad son esenciales para detectar, supervisar y mitigar estos riesgos, garantizar la seguridad de los datos, impedir el acceso no autorizado y proteger la información confidencial. Sin embargo, los métodos convencionales suelen ser insuficientes para hacer frente a la sofisticación de los ciberataques modernos.
Método: el aprendizaje automático (ML) se ha convertido en un enfoque transformador para reforzar la ciberseguridad. Mediante el análisis de grandes conjuntos de datos, los algoritmos de ML pueden identificar anomalías y predecir amenazas con mayor precisión. Cuando se integra en los marcos de ciberseguridad, el ML mejora las defensas contra problemas como las violaciones de datos, el robo de identidad y las intrusiones en el sistema.
Resultado: esta investigación se centra en la utilización del ML para desarrollar y optimizar modelos de ciberseguridad adaptados a los sistemas TIC de las empresas. Además, destaca la creciente demanda de expertos capaces de diseñar e implementar soluciones de seguridad basadas en el ML.
Conclusión: al explorar las tendencias emergentes, este estudio subraya el papel fundamental del ML en el fortalecimiento de la seguridad digital a nivel mundial.

Palabras clave: Ciberseguridad; Análisis de Datos; Ciberdelincuencia; Algoritmos de ML; Amenazas; Seguridad de Redes.

Submitted: 05-07-2024 **Revised:** 05-12-2024 **Accepted:** 22-05-2025 **Published:** 23-05-2025

INTRODUCTION

The rapid advancement of digital technology has brought about unprecedented convenience and connectivity but has also given rise to a pressing global issue: cybercrime. Defined as illegal activities conducted through computer networks or the internet, cybercrime poses significant risks to individuals, organizations, and governments. The repercussions include financial losses, reputational harm, and emotional distress. Cybercrime encompasses a wide array of malicious activities, such as hacking, phishing, malware attacks, identity theft, cyberbullying, and cyberstalking, each with its unique impact and challenges.[1] Hacking involves unauthorized access to computer systems or networks, often with the intent to steal sensitive information, cause disruption, or inflict damage.[2] This type of intrusion undermines trust in digital systems and compromises critical data.[3] Similarly, phishing is a prevalent cybercrime tactic where attackers masquerade as legitimate entities to trick victims into disclosing personal or financial information.[4] This often involves fake emails or websites that appear authentic, resulting in data breaches, identity theft, or financial losses for victims. Malware attacks represent another common threat, where malicious software such as viruses, ransomware, or spyware is used to infiltrate systems. These attacks can disrupt operations, compromise data integrity, or even hold information hostage for ransom. On a personal level, cyberbullying and cyberstalking exploit the internet to harass, threaten, or intimidate individuals, leading to severe emotional and psychological harm.[5] The financial toll of cybercrime is staggering, with costs steadily increasing year after year. These expenses include direct costs, such as repairing damaged systems and recovering stolen data, and indirect costs, such as the loss of business due to reputational damage.[6] Additionally, the theft of sensitive information can lead to identity fraud and further financial repercussions. The evolution of network-based technologies has also introduced new vulnerabilities and threats.[7] To counter these challenges, innovative security mechanisms are essential. The digital landscape generates vast amounts of cybersecurity data from online transactions, communications, and interactions. This data, when properly analyzed, provides critical insights into cyber threats, enabling organizations to identify vulnerabilities, detect attacks, and enhance their security frameworks.[8,9]

However, the sheer volume of cybersecurity data in today's digital era can be overwhelming for organizations. The complexity and scale of this data make it challenging to monitor, analyze, and respond to potential threats effectively.[10] To address this issue, many organizations are turning to machine learning (ML) algorithms.[11,12] These advanced tools automate the analysis of cybersecurity data, detecting patterns and anomalies that might otherwise go unnoticed. Machine learning offers real-time insights, allowing organizations to identify potential threats early and respond swiftly. By leveraging ML, organizations can not only minimize the damage caused by cyber-attacks but also bolster their overall security posture.[13] For example, ML algorithms can analyze large datasets to detect unusual activity, flagging potential phishing attempts, or identifying malware behavior. This proactive approach ensures that security teams can act before an attack causes significant harm.

The main objective of this paper is to represent a growing threat in the modern digital landscape, impacting individuals, businesses, and governments. Its diverse forms, including hacking, phishing, malware attacks, and cyber harassment, highlight the critical need for robust cybersecurity strategies.[14] While the volume of cybersecurity data presents challenges, innovative solutions such as machine learning provide hope. By automating data analysis and offering real-time threat detection, ML empowers organizations to stay ahead of cybercriminals, enhancing digital safety and ensuring a more secure future for all.

METHOD

Data

The dataset provides a comprehensive overview of global cybersecurity incidents from 2015 to 2024, encompassing approximately 3 000 recorded cases. It includes critical columns such as the country of occurrence, year, attack type, target industry, financial loss, affected users, attack source, exploited vulnerabilities, defense mechanisms, and incident resolution times. Key insights reveal Distributed Denial of Service (DDoS) attacks as the most frequent, targeting predominantly the IT sector, underscoring the industry's need for enhanced cybersecurity. Financial impacts average $50,5 million per incident, with losses ranging from $0,5 million to $100 million, reflecting the severity of these threats. A median of 500 000 users affected per incident highlights the extensive reach of some attacks. Nation-state actors are identified as the most common sources of threats, often exploiting zero-day vulnerabilities, which calls for heightened vigilance in system patching. Antivirus software is the primary defense mechanism used, though organizations may require more advanced strategies for robust security. Incident resolution times vary from 1 to 72 hours, with a median of 37 hours, demonstrating the variability in response efficiency. Visualization of the data reveals trends, spikes in incidents, and correlations with cybersecurity events over time, aiding in understanding patterns and potential risks. This dataset is invaluable for organizations aiming to assess vulnerabilities, improve defense strategies, and respond more effectively to emerging threats in the evolving cybersecurity landscape.[15]

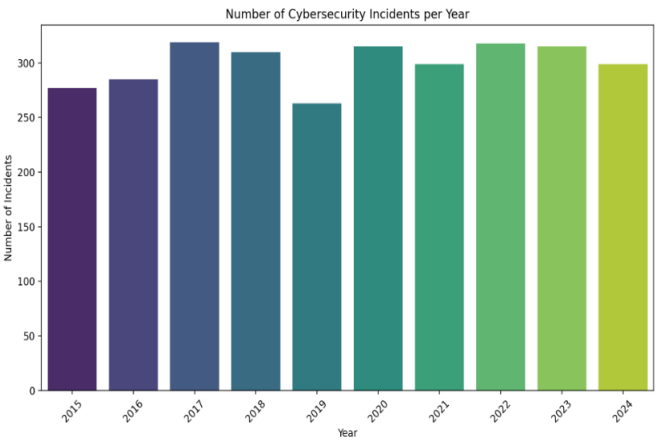

Figure 1. Number of cyber security incidents per year[15]

Data Analysis

Analyse attack types over years

This analysis provides valuable insights into evolving cybersecurity threats by identifying key trends across multiple dimensions. By examining the frequency of attack types such

as phishing, ransomware, and DDoS, organizations can track which methods are becoming more prevalent or fading over time. Financial impact assessments reveal the economic toll of different attacks, highlighting those causing the most significant damage. Industry-specific patterns, such as the susceptibility of educational institutions to phishing in certain years, enable targeted defense strategies. Emerging trends, such as the year-over-year increase in ransomware incidents, underscore the need for proactive measures against growing threats. Comparative analysis allows side-by-side evaluation of attack types, shedding light on shifts in the threat landscape and prioritizing response efforts. Visualizing these findings through charts or graphs makes patterns more apparent, facilitating informed decision-making. This comprehensive approach equips organizations with the knowledge to adapt and fortify their cybersecurity strategies effectively.

The figure above shows the number of incidents for each attack type from 2015 to 2019. For example, DDoS and Malware attacks were consistently high, while Man-in-the-Middle and SQL Injection attacks fluctuated. Below is a line chart visualizing these trends (figure 2)

Identify industries most targeted

The IT sector remains the top target for cybercriminals, followed closely by Banking, Healthcare, Retail, and Education. This trend underscores that industries managing sensitive data, financial transactions, or critical operations are particularly vulnerable to cyber threats. The dominance of IT highlights its critical role in global infrastructure, while the significant targeting of Banking and Healthcare emphasizes the high value of their data. These findings stress the urgent need for advanced cybersecurity strategies, especially in sectors dealing with valuable information, to mitigate risks and safeguard essential systems against evolving cyberattacks. (figures 2,3,4,5)

	DDoS	Malware	Man-in-the-Middle	Phishing	Ransomware	SQL Injection
2015	50	51	41	46	47	42
2016	53	41	47	55	42	47
2017	58	46	58	64	44	49
2018	60	56	36	52	49	57
2019	48	43	44	45	38	45

Figure 2. Number of incidents for each attack type

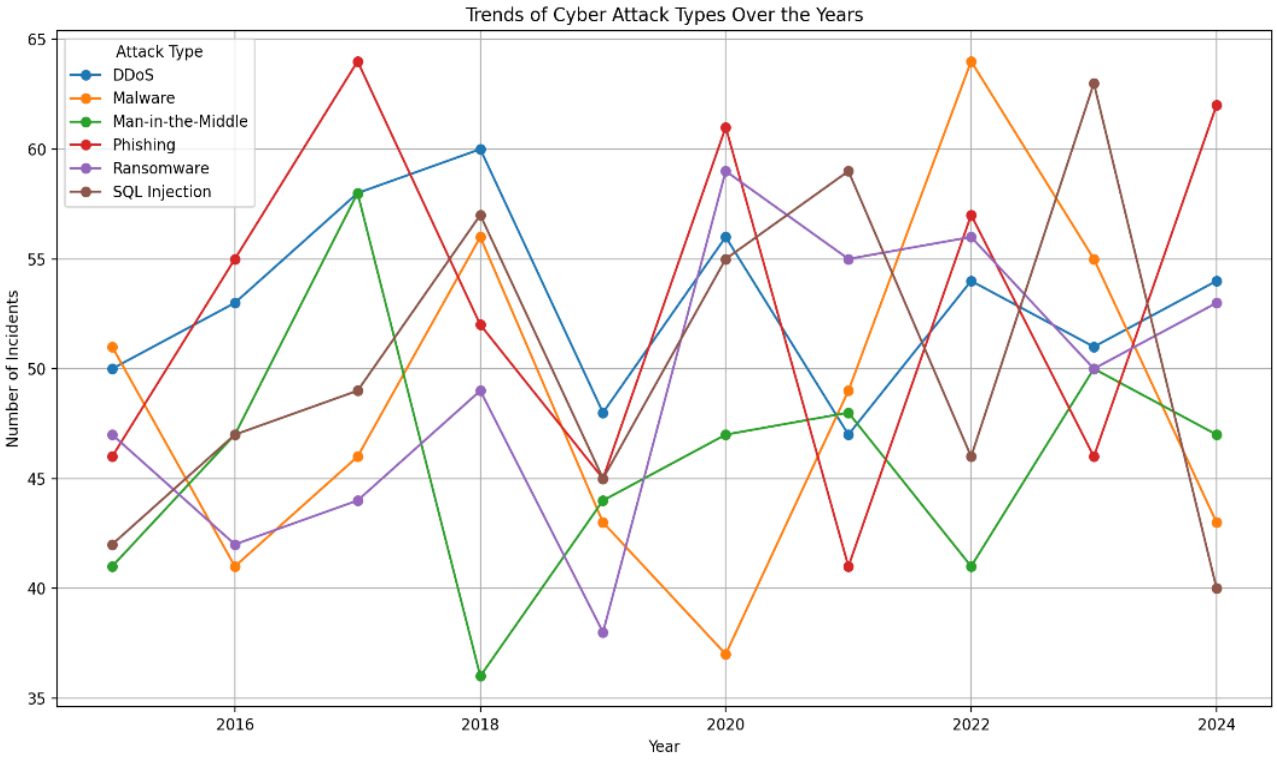

Figure 3. Trends of cyber-attack type over the year[15]

IT	478
Banking	445
Healthcare	429
Retail	423
Education	419

Figure 4. Top target industries for cybercriminals

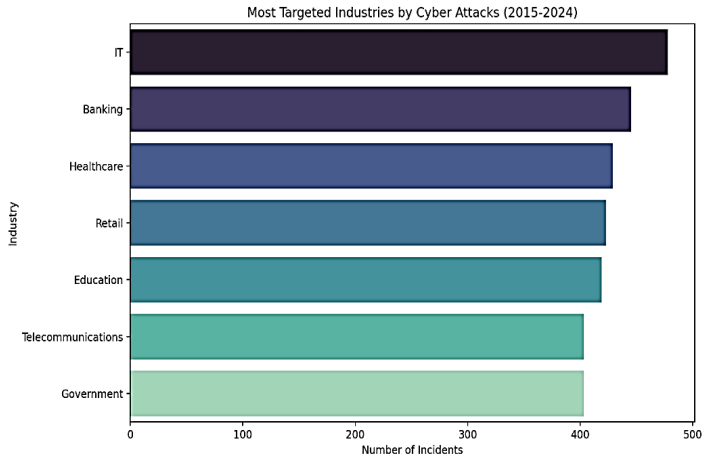

Figure 5. Most targeted industries by cyber attacks (2015-2024) [15]

Exploration of financial losses by industry

The figure highlights financial losses across the top five industries, revealing that the IT sector faced the highest total losses, followed closely by Banking and Government. Despite varying total losses, the average loss per incident remains consistent across these industries, approximately $50 million. Visualizations further emphasize these findings: the first chart illustrates the cumulative financial impact, showcasing IT, Banking, and Government as the hardest hit, while the second chart delves into average losses per incident, reflecting the severity of individual cyberattacks. These insights underscore the immense financial risks associated with cyberattacks, particularly in industries managing high-value assets and sensitive data. (figures 6,7 and 8).

	mean	sum	count
IT	51.9034100418	24809.83	478
Banking	51.1739101124	22772.39	445
Government	52.6186848635	21205.33	403
Retail	49.9280141844	21119.55	423
Healthcare	49.0472960373	21041.29	429

Figure 6. The average and total financial losses (in millions of dollars) for the top five industries

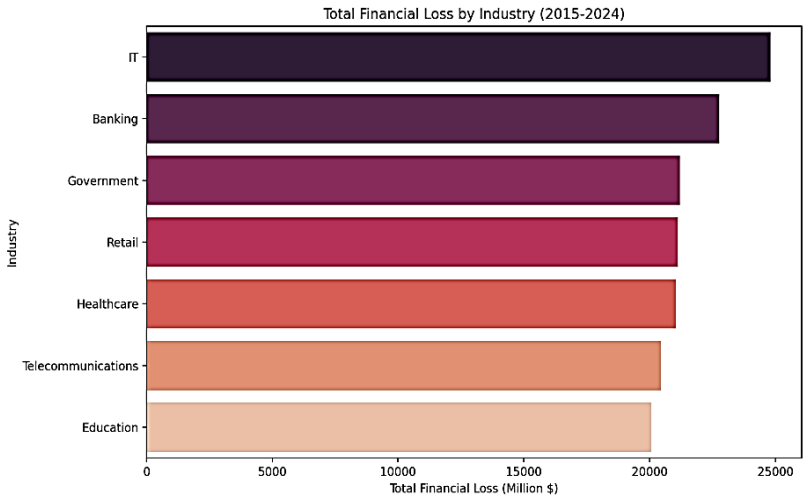

Figure 7. Total financial loss by industry[15]

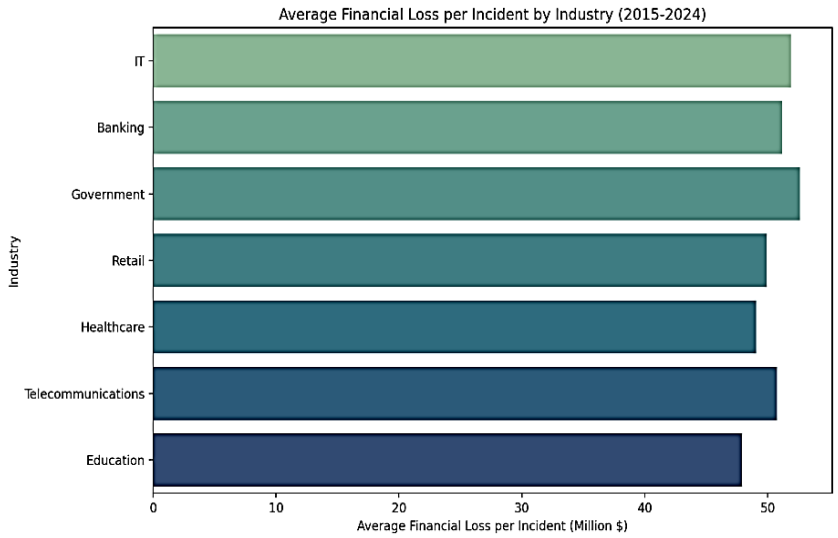

Figure 8. Average financial loss per incident[15]

Impact of attacks on business continuity

Cyber attacks pose significant challenges to business continuity, impacting operations, finances, reputation, and long-term strategy. Operationally, attacks such as ransomware or DDoS can paralyze critical systems, disrupting workflows and delaying service delivery. Financial losses are immediate and substantial, including recovery costs, potential ransom payments, revenue losses during downtime, and expenses for implementing stronger security measures. Reputational damage often follows, eroding customer trust and leading to lost business and market share. Legal and regulatory repercussions can also arise, with companies facing fines, lawsuits, and increased scrutiny for failing to safeguard sensitive data. Strategically, significant breaches may force businesses to redirect resources toward cybersecurity investments, potentially detracting from other priorities. Employee morale and productivity may decline, as concerns over data security and personal risk grow. Furthermore, supply chain disruptions caused by attacks on third-party vendors can cascade across operations, amplifying the overall impact. These multifaceted risks emphasize the need for robust cybersecurity strategies to safeguard organizational resilience and long-term viability (figure 9).

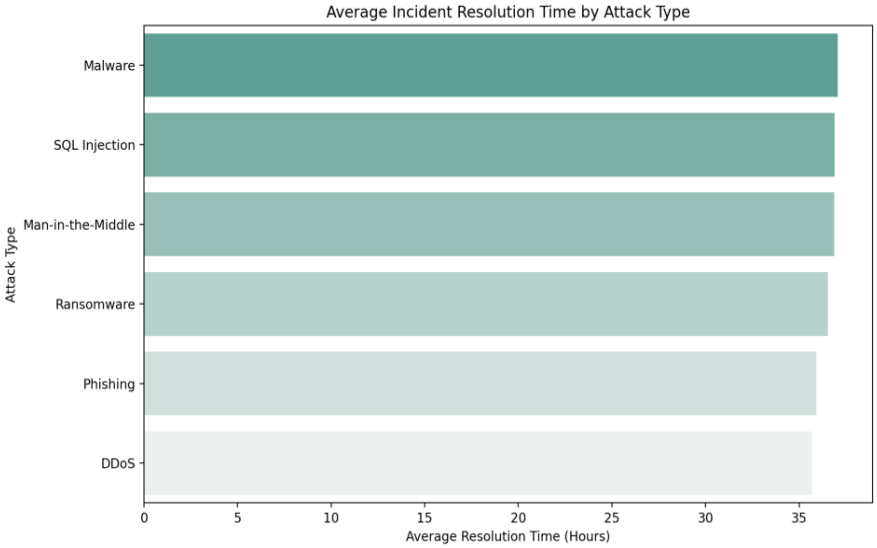

Figure 9. Average incident resolution time by attack type[15]

RESULTS AND DISCUSSION

The analysis reveals crucial trends and patterns in cybersecurity threats, providing actionable insights for organizations. The frequency of cyberattacks, such as phishing, ransomware, and DDoS, demonstrates evolving tactics, with ransomware incidents showing a year-over-year increase. Financial impact analysis highlights significant economic losses across industries, with the IT sector experiencing the highest total losses, followed by Banking and Government. Despite variations in total losses, the average financial loss per incident across industries remains consistently high, around $50 million. Industry-specific trends reveal that sectors handling sensitive data, such as IT, Banking, and Healthcare, are prime targets for cybercriminals, emphasizing the need for tailored defenses. Moreover, visualizations of attack types and financial losses enable organizations to prioritize response efforts and resource allocation effectively. The impact on business continuity is multifaceted, with operational disruptions, reputational damage,

and financial setbacks underscoring the urgency of robust cybersecurity measures. The findings stress the critical role of proactive strategies in minimizing risks and maintaining resilience against evolving threats.

CONCLUSION

The rapid evolution of technology and the increasing sophistication of cyber threats necessitate innovative approaches to cybersecurity. This study highlights the transformative potential of machine learning in addressing these challenges by enabling precise threat detection, anomaly identification, and predictive capabilities. By integrating ML into cybersecurity frameworks, organizations can fortify their defenses against complex threats like data breaches and system intrusions. Moreover, the research emphasizes the importance of equipping industries managing high-value assets with advanced security solutions to ensure operational continuity, financial stability, and resilience in the face of an ever-evolving digital threat landscape.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Md. Alimul Haque, Kushboo Mishra, B. K. Mishra.

Methodology: Md. Alimul Haque, Kushboo Mishra, B. K. Mishra.

Research: Md. Alimul Haque, Kushboo Mishra, B. K. Mishra.

Drafting - original draft: Md. Alimul Haque, Kushboo Mishra, B. K. Mishra.

Writing - proofreading and editing: Md. Alimul Haque, Kushboo Mishra, B. K. Mishra.

REFERENCES

1. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, et al.Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020;20:1-10.
2. McLaughlin S, Konstantinou C, Wang X, Davi L, Sadeghi AR, Maniatakos M, et al. The cybersecurity landscape in industrial control systems. Proc IEEE. 2016;104(5):1039-57.
3. Tao F, Akhtar MS, Jiayuan Z. The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Trans Creat Technol. 2021;8(28):e3.
4. Zeadally S, Adi E, Baig Z, Khan IA. Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access. 2020;8:23817-37.
5. Hobbs A. The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity. In: SAGE Business Cases. SAGE Publications: SAGE Business Cases Originals; 2021.
6. Atoum I, Otoom A. A Classification Scheme for Cybersecurity Models. Int J Secur Its Appl. 2017;11(1):109-20.
7. Martínez Torres J, Iglesias Comesaña C, García-Nieto PJ. Machine learning techniques applied to cybersecurity. Int J Mach Learn Cybern. 2019;10:2823-36.
8. Azam A, Haque A, Rai SR. Predicting Housing Sale Prices Using Machine Learning with Various Data Split Ratios. Data Metadata. 2024 Dec 15;3. doi: https://doi.org/10.56294/dm2024231.
9. Haque MA, Faizanuddin M, Singh NK. A Study of Cognitive Wireless Sensor Networks: Taxonomy of Attacks and Countermeasures. 2012;
10. Haque MA, Bokhari MU, Sinha AK, Singh NK. Comparative study on Wireless threats and their Classification. In: INDIACom-2017; IEEE Conference ID: 40353 2017 4th International Conference on “Computing for Sustainable Global Development”, 01st - 03rd March, 2017 BVICAM. 2017. p. 5057-9.
11. Haque MA, Haque S, Alhazmi S. Artificial Intelligence and Covid-19: A Practical Approach. Bentham Science Publisher; 2022. p. 92-109.
12. Haque MA, Haque S, Kumar K, Singh NK. A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. In: Digital Transformation and Challenges to Data Security and Privacy. IGI Global; 2021. p. 63-90.
13. Zeba S, Haque MA, Alhazmi S, Haque S. Advanced Topics in Machine Learning. Mach Learn Methods Eng Appl Dev. 2022;197.
14. Almrezeq N, Haque MA, Haque S, El-Aziz AAA. Device Access Control and Key Exchange (DACK) Protocol for Internet of Things. Int J Cloud Appl Comput. 2022 Jan;12(1):1-14. doi: https://doi.org/10.4018/IJCAC.297103.
15. Cybersecurity Threats (2015-2024)ML. Available from: https://www.kaggle.com/code/sonawanelalitsunil/cybersecurity-threats-2015-2024-ml/output