Journal of Applied Information Science
12 (2) 2024, 33-43
http://www.publishingindia.com/jais

Assessing Cyber Intelligence, Learning, and Automation Capabilities

Cheryl Ann Alexander[1*] and Lidong Wang[2]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA.
Email: cheryl.alexander@techhealthsolutions.org
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA.
Email: lidong@iser.msstate.edu
[*]Corresponding Author

Abstract: Cybersecurity assessments are critical. Automation of a cyber risk assessment fosters real-time identification and assessment of risks, enabling rapid responses to potential threats. This paper deals with assessing cyber intelligence, learning, and automation capabilities. Specifically, several topics are introduced or discussed. They include human factors in cybersecurity and the relevance of cyber intelligent systems, machine learning (ML), and automation; the performance of ML and data preprocessing; the assessment of ML (bias, advantages, disadvantages, and metrics); and ML-based stealing attacks, intrusion detection systems, cyber threat intelligence, and cybersecurity automation. This paper presents cybersecurity assessment in healthcare (Internet of Medical Things, internal/external threats, and human factors) as a case study. Cyberthreat intelligence (CTI) represents actionable threat information that is useful for threat detection and remediation. Cybersecurity automation helps to enhance the management of vulnerabilities, security incidents, and risks. Cybersecurity assessment in healthcare helps mitigate internal and external threats. Creating a cybersecurity culture in the medical and healthcare environment is essential to robust cybersecurity.

Keywords: Artificial intelligence (AI), Automation, Cybersecurity, Cyber intelligence, Healthcare, Information, Internet of Medical Things (IoMT), Machine learning (ML).

I. Introduction

Machine learning (ML) has been used in detecting and classifying cyberattacks. Deep learning (DL) for intrusion-detection systems (IDSs) on the Internet of Things (IoT) was introduced [1]. Ensemble classifiers involve the integration of predictions by multiple individual classifiers. The ensemble classifiers can compensate for the weakness of individual classifiers and utilize their combined knowledge to improve performance. They have the potential to provide promising detection solutions [2].

Main trends that will affect and shape cyber development in the near future were identified, including 1) automation, 2) collaboration, 3) virtual and shared resources, 4) fighting the unknown, 5) the Internet of Things, and 6) the move toward an autonomous world [3]. The unavailability of benchmark and updated datasets for training ML models is a challenge. The detection speed of a cyberthreat and prompt action are also challenges for an ML model. It is necessary to have robust ML models to handle adversarial inputs. Training a model in adversarial settings should be emphasized to develop a robust model against adversarial inputs [4].

Cybersecurity assessments are significant in building assurance. Some assessment methods have been proposed, including 1) compliance checking, 2) checklist-based evaluation, 3) model-based testing, 4) simulation or emulation-based testing, 5) penetration testing, 6) formal analysis, 7) vulnerability

identification and analysis, and 8) reviews. Reviews involve passive (commonly manual) examinations of documentation related to the assessed object [5].

Performance measures and assessment in healthcare are accuracy, sensitivity, specificity, etc. Robustness (such as dealing with missing data or poor-quality data, particularly relevant in health data) is also important. There is not sufficient information regarding how an algorithm behaves on other data in real life. The problem is wide and eventually originates from improper experimental design and hypothesis testing procedures [6].

The purpose of research in this paper is to assess cyber intelligence, learning, and automation capabilities. The subsequent sections of the paper are organized as follows: the second section introduces system requirements and security requirements; the third section presents human factors in cybersecurity and the relevance of cyber intelligence systems, ML, and automation; the fourth section introduces the performance of ML and data preprocessing; the fifth section deals with the assessment of ML (bias, advantages, disadvantages, and metrics); the sixth section introduces ML-based stealing attacks, intrusion detection systems, cyber threat intelligence, and cybersecurity automation; the seventh section presents cybersecurity assessment in healthcare (including IoMT, internal/external threats, and human factors); and the eighth section is the conclusion.

II. System Requirements and Security Requirements

AI/ML requires a massive amount of storage and network access. A GPU is unnecessary if tasks are small and can adequately fit into a complex sequential processor making a CPU just enough. However, if intensive tasks are key and have manageable data, a better choice would be a powerful GPU; for Example, a laptop-dedicated high-end graphics card should be enough. Security requirements are often a major concern, for example, the most basic IoT architecture (three-layered architecture), attacks, and security requirements are shown in Table I [1].

Table I: The Architecture, Attacks, and Security Requirements of IOT

Layers	Attacks	Security Requirements
Perception	DoS, DDoS, side channel, denial of sleep, replay, node capture, fake node/sybil, mass node authentication	Authentication, data confidentiality, key management, lightweight encryption
Network	DoS, routing attacks, man-in-the-middle, eavesdropping/sniffing	Authentication, key management, communication security, intrusion detection, routing security
Application	Data privacy and identity, data accessibility and authentication, dealing with availability	Authentication, privacy protection, information security management

III. Human Factors in Cybersecurity and the Relevance of Cyber Intelligent Systems, ML, and Automation

One of the biggest barriers to adopting the digital transformation strategy is cybercrimes that exploit the vulnerabilities of systems as well as human-attributed weaknesses. A new kind of cyberattack (aiming to exploit human vulnerabilities) is classified as a social engineering attack. Social engineering attacks are a kind of psychological attack that exploit weaknesses in human's cognitive functions. Human actions also include the misuse of passwords and property loss (a laptop with confidential data), erroneous security settings, etc. The role of human behaviors in fighting cyberattacks and strengthening cyber defenses is classified into the topic of "human factors" in cybersecurity [7].

Job roles and responsibilities across various entities are significantly impacted by AI-powered automation. The need for manual labor is reduced by integrating AI automation as tasks become more effective. A sub-area of AI is ML. Automation of ML, a core method of ML, increases the speed of

ML processing and makes it more efficient. Entities are enabled to deploy ML models more rapidly by making the ML pipeline process more efficient and reducing errors.

IV. The Performance of ML and Data Preprocessing

The performance of ML substantially depends on data preprocessing. Data preprocessing decreases or eliminates undesirable features of input data. For ML, data preprocessing includes handling missing values, handling improper formats (such as symbolic values), removing redundant/irrelevant attributes, handling class imbalance, feature discretization, dimension reduction and sampling, normalization, etc. [8].

Data quality, types, distributions, dimensions (the number of input parameters), and cardinality (unique values within a categorical parameter) affect preprocessing, scaling, and feature engineering before the data is used for modeling and predictive analysis. There are approaches to handling class imbalance and improving the model performance, e.g., under-sampling of the majority class or oversampling of the minority class [9]. Data quality dimensions with six characteristics are listed in Table II [10]. Each of the dimensions has multiple interdependencies. The selection of the characteristics reflects the usability of such characteristics when applied to healthcare.

Table II: Data Quality Dependencies

Data Quality Dimension	Definition	Interdependencies
Completeness	Containing all the context needed for decision-making.	● Coverage, relevancy, density, & sufficiency
Relevancy	The information needed for a task at hand.	● Current, correct, timely, & sufficient
Usability	The information is delivered on/in a suitable device/format.	● Easy to organize & utilize ● Usefulness with completeness & relevance accuracy
Availability	Available where it is needed, existing in an accessible system.	● Accessible, locatable, interpretable, & compatible
Reliability	Adequately complete, error-free, and consistent in distributed settings.	● Consistency ● Unbiased ● Credibility inclusive of completeness & accuracy ● Data producer with previous experience & mistake correction ● Reputation traceability with data source and provenance
Security	Protected against extraction or tampering.	● Supporting all other dimensions

V. The Assessment of ML: Bias, Advantages, Disadvantages, and Metrics

Important components for assessing ML algorithms include but are not limited to, bias testing and metric selection. Elimination of bias, e.g., measurement bias, prejudicial bias, sample bias, and algorithmic bias, is crucial. Bias testing needs to be conducted on an ongoing basis rather than as a one-time task and needs monitoring over the entire lifecycle [9]. Table III [11] shows the advantages and disadvantages of ML methods.

Table III: A Comparison of ML Mechanisms

Techniques	Advantages	Disadvantages
Unsupervised learning	For clustering, e.g., *k*-mean, if *k* is decided, the left process is easy.	Most methods are for the clustering of continuous features only.
	Clustering methods are of quick response generation.	In a clustering-based anomaly detection system, an initial assumption is assigning a bigger cluster to normal instances and a smaller cluster to malicious instances. It is hard to assess the method without the assumption.
	For a large training dataset, it is better to split it into similar classes for detecting malicious instances efficiently (decreasing the computation complexity).	Utilizing improper proximity measures often decreases the detection rate.
	Providing a reliable performance compared with statistical or supervised methods.	Generally time-consuming in dynamically updating profiles.
	Easily identifying outliers in a small dataset.	Often using both clustering and outlier detection, producing higher complexity in comparison to other techniques.
	Able to detect bursty & isolated attacks.	Detection parameters are substantially relied on the methods.
Supervised learning	Flexible for training & testing.	Greatly relying on the presumptions.
	High detection accuracy for known attacks if choosing a suitable threshold.	Need more patterns compared to other techniques.
	Enable updating the implementation strategy with the concatenation of new data.	Unable to identify unknown attacks till similar training data is supplied.
Ensemble learning	Better performance due to the combination of multiple classifiers.	Difficult to perform subset selection among unbiased classifiers.
	Suitable for a large-scale dataset.	The greedy method of choosing subsets is usually time-consuming for a large-scale dataset.
	Using controlling parameters (comprehensive, easily adjusted).	Difficult to achieve real-time performance.
	Effective Adaboost and Stack generalization owing to the variety in prediction utilizing multiple base level classifiers.	High computation costs due to lack of appropriate hybridization.

For ML model performance assessment, usual metrics, or tools for the performance assessment of supervised classification models include: 1) accuracy, 2) true negative rate/specificity, 3) precision/positive predictive value, 4) recall/true positive rate/sensitivity, 5) F1 score, 6) confusion matrix, 7) precision recall curve (PRC), and receiver operator characteristic (ROC) curve. Both a PRC and ROC curve are helpful for understanding the model performance at various decision thresholds. The area under the curve (AUC) from the ROC curve is most often utilized when assessing the supervised binary classification. This metric delivers overall model performance and is helpful when identifying both classes is significant. For the assessment of a model to discriminate the positive class in an imbalanced dataset, the PRC (the average precision score) may be a better choice for a comparison of the model performance. For the metric selection, if it is crucial to minimize false negatives, then a focus on recall or true positive rate is warranted. If minimizing false positives is critical, then precision or positive predictive value is more significant. If both false positives and false negatives are important, the F1 score is useful. Although one metric is possibly recognized as the most informative to the model

performance assessment, it also needs to be explored in the context of other metrics [9].

VI. ML-Based Stealing Attacks, Intrusion Detection Systems, Cyberthreat Intelligence, and Cybersecurity Automation

The attack methodology against controlled information was explored and ML-based stealing attacks are studied according to three kinds of targeted controlled information, including controlled user activities, controlled ML model-related information, and controlled authentication information. Fig. 1 [12] shows the types of ML-based stealing attacks. The attack methodology for stealing controlled information using ML was proposed, which is shown in Fig. 2 [12]. Table IV [8] shows a taxonomy of intrusion detection systems. These categories are not mutually exclusive; therefore, an intrusion detection system can belong to several categories.

Cyberthreat intelligence (CTI) represents actionable threat information that is useful for proactive, preventive, and timely threat detection and remediation. A CTI capability model was proposed according to three dimensions: analytical component capability, contextual response capability, and experiential practice capability [13]. Fig. 3 [13] shows the model and anticipated effects.

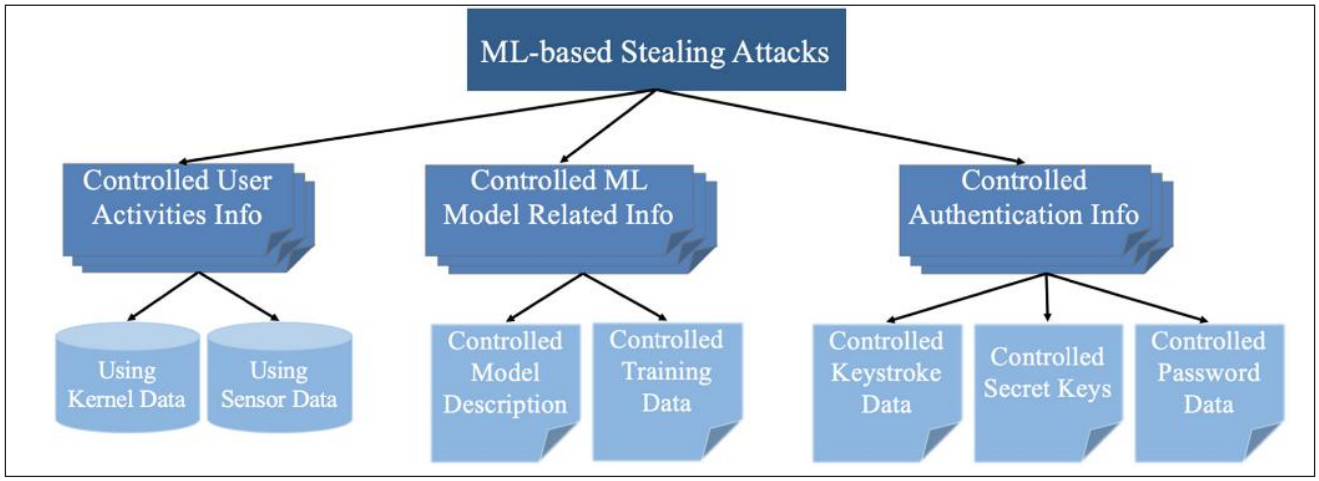

Fig. 1: Types of Stealing Controlled Information Attacks (Info: Information)

The key element in stopping a modern-day cyberattack is cyberthreat intelligence and monitoring. Informing decision-makers is the primary purpose of threat intelligence. It is evidence-based data and information, which includes indications, context, mechanisms, implications, and practical advice, concerning a current or potential threat or hazard that can be utilized to make informed decisions about that threat's responses to a risk or danger. Actionable data is the cornerstone of cyberthreat intelligence. It is useful data gathered by cybersecurity systems and security experts that can assist in better understanding vulnerabilities, taking appropriate action to stop an attack, and defending the network from current and future attacks. Planning, gathering, processing, analysis, and dissemination are the cornerstones of a cyberthreat intelligence lifecycle. Any cybersecurity solution that uses machine learning (ML) is the superior choice for extending the development of cyberthreat intelligence.

Through an understanding of cyberthreat intelligence, which completely incorporates the gathering of data, analysis, and explanation of data

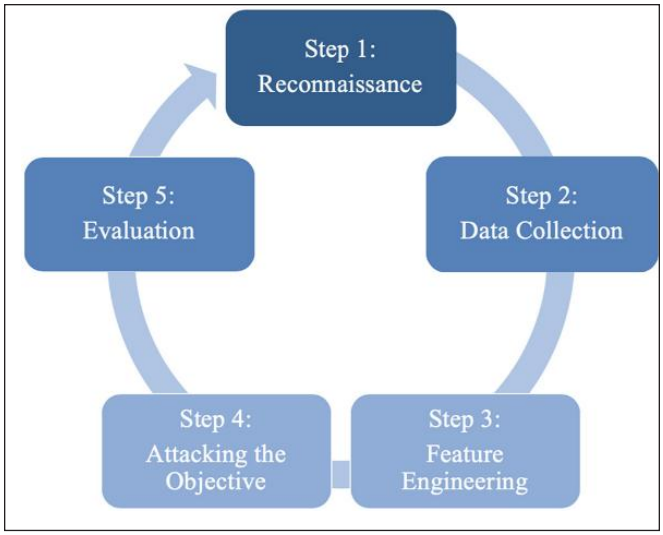

Fig. 2: ML-Based Stealing Attack Methodology

TABLE IV: A TAXONOMY OF INTRUSION DETECTION SYSTEMS

Factors	Details
Detection methods	Misuse-based (also called signature-based) ● Expression matching ● State-transition analysis
	Anomaly-based ● Knowledge ● Statistical ● Machine learning (ML) ➢ Unsupervised ➢ Supervised ➢ Single ➢ Hybrid ➢ Ensemble
Audit data sources	Host-based
	Network-based
Architectures	Centralized
	Distributed ● Agent-based ● Bio-inspired
Usage frequency	Continuous
	Periodic
Response to intrusion	Passive
	Active ● Proactive ● Reactive ➢ Target an attacking system ➢ Target an attacked system

Factors	Details
Attack characteristics	Single-source attacks
	Multi-source attacks (also called distributed attacks) ● Coordinated ● Direct ● Reflector

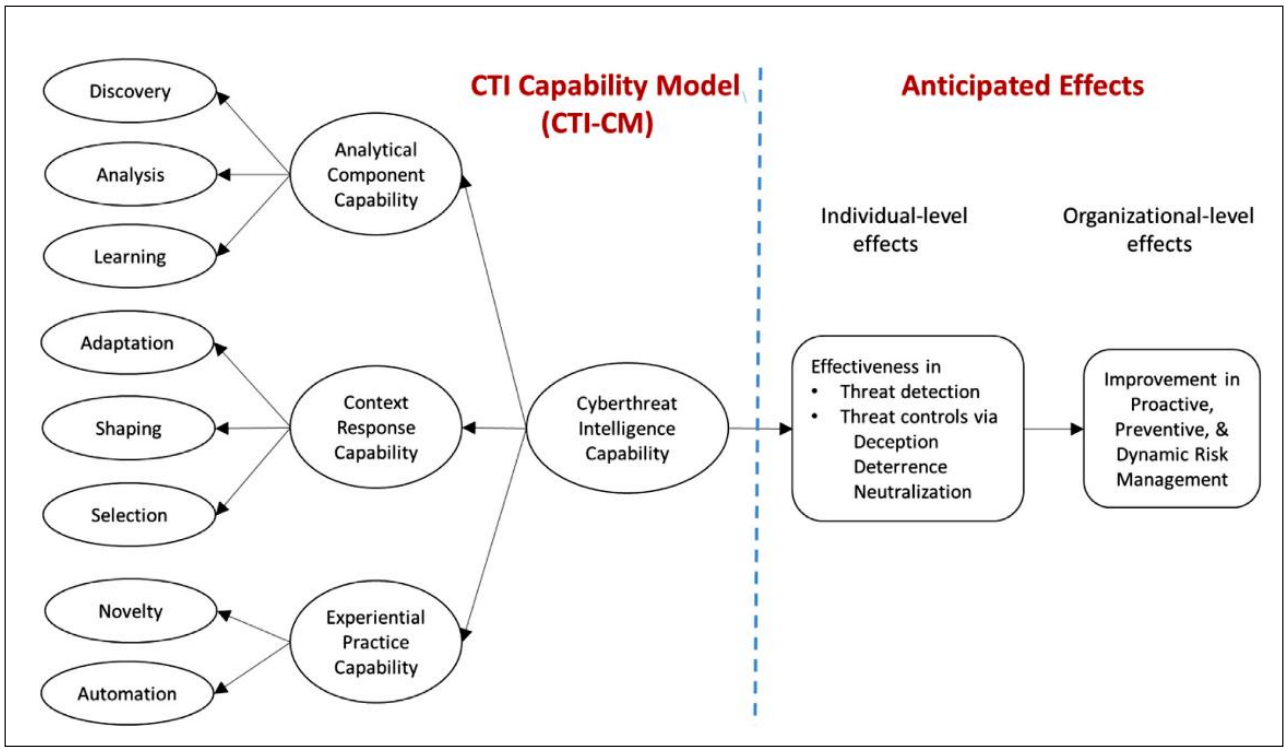

Fig. 3: A CTI Capability Model and Anticipated Effects

to identify any potential threats and their consequences an enterprise can use this key tool in many areas of cybersecurity. There are four critical elements: operational intelligence, technical intelligence, tactical intelligence, and strategic intelligence. Cybersecurity experts gather and analyze threat intelligence by monitoring various sources of information, such as open-source intelligence, technical data, and human intelligence that can be used to identify indicators of jeopardy and developing threats. Cyberthreat intelligence has a crucial role in incident response because this is how the security team can gather actionable data throughout a security incident. However, AI/ML have begun to revolutionize cyberthreat intelligence as the automation of data analysis, predictive insights, and identification of patterns help IT security teams increase their security practices.

Cybersecurity automation tools and platforms can be 1) Robotic Process Automation—involves capturing and compiling data, analysis, and detection methods for simple breaches and other limited-cognitive tasks; 2) Management and Security Orchestration Automation—improves the management of vulnerabilities, security incidents, and risks. The utilization of SOAR (security orchestration, automation, and response) internally or externally is more complicated and takes certain SIEM (security information and event management) warnings and automatedly responds to them when required for triage and remediation [14].

VII. Cybersecurity Assessment in Healthcare: IoMT, Internal/External Threats, and Human Factors

A security assessment of various medical devices in the design and post-market phases and data security assessment was proposed. An integrated fuzzy AHP TOPSIS approach was used to evaluate the security of devices and data. A security assessment framework of the Internet of Medical Things (IoMT) is shown in Fig. 4 [15]. Table V [15] shows IoMT security assessment and security factors. Types of attacks are as follows: 1) human attack surface (a kind of human factors, e.g., internal threats, forgery); 2) communication protocol attack surface (e.g., DoS, man-in-the-middle); 3) physical attack surface (e.g., equipment attacks, side-channel threats); and 4) aggregate attack surface (integrating networks, systems, and people) [15].

The FDA, HIPAA, and other regulatory agencies set strict guidelines and frameworks for healthcare entities demanding precision and high regulatory standards. To ensure compliance with these frameworks and standards and to deliver high-quality care, Data Security Test Automation can be applied. Efficient risk management depends on risk assessment as an elementary function to facilitate decision-making and is useful for identifying, estimating, and prioritizing risk to enterprise operations because of information systems. Risks can be measured as either quantitative or qualitative. Automation of a cyber risk assessment is necessary to facilitate the processes of gathering relevant data. Some systems and networks need continuous monitoring. Automation of risk assessment can be a measurement solution that can contribute to continuous monitoring and rapid response to potential or real threats. Relevant data can be collected by automating a cyber risk assessment. An automated risk assessment solution enables constant monitoring of systems and networks, which fosters real-time identification and assessment of risks enabling rapid responses to potential threats. Automated systems quickly detect anomalies, vulnerabilities, and suspicious activities through endless monitoring and analysis of security logs, network traffic, and event logs.

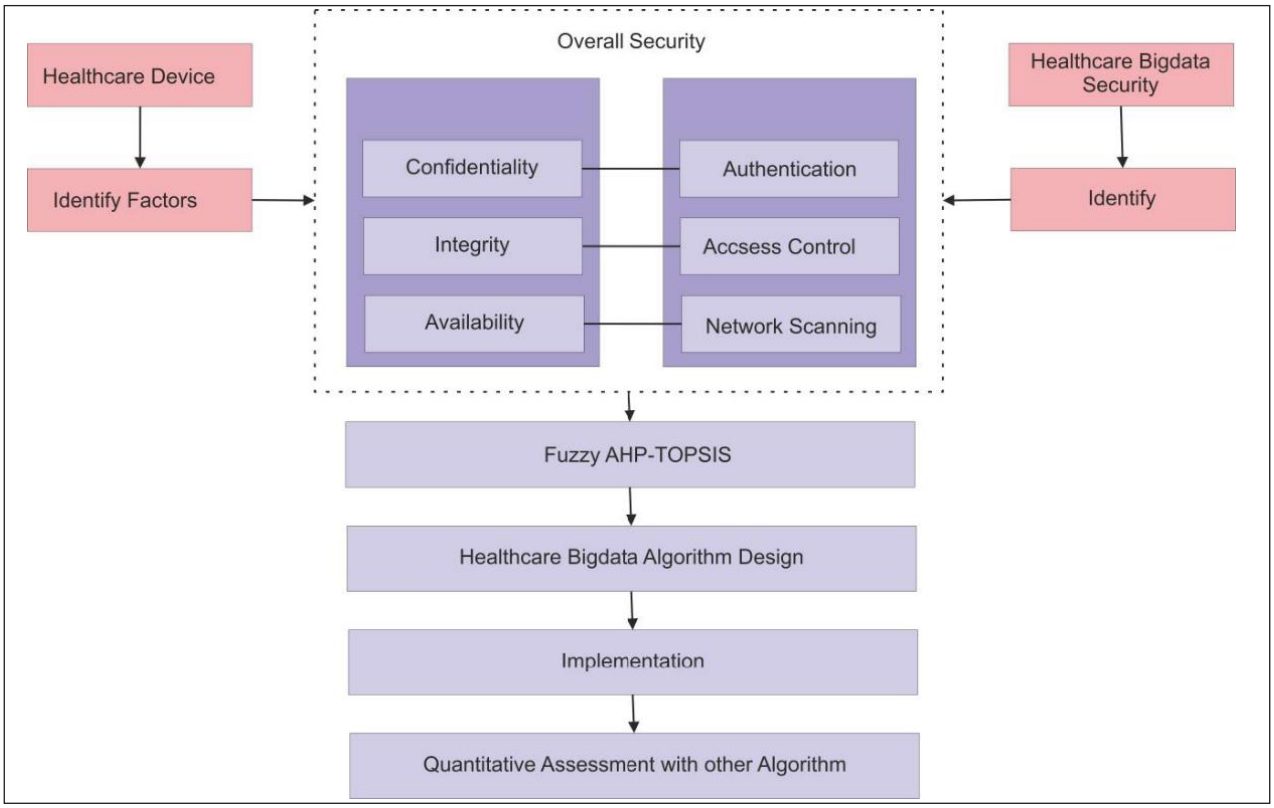

Fig. 4: A Security Assessment Framework of Medical Devices and Healthcare Big Data

Malicious actor internal/insider threats occur when an employee, staff member, or contractor has authorized access and intentionally misuses it or steals sensitive information such as patient data. Employees or contractors can steal information for several reasons including personal gain or to intentionally harm the organization. Unfortunately, it is rather difficult to determine internal/insider attacks or prevent malicious internal/insider threats because employees and contractors already have access to sensitive Personal Health Information (PHI). The key is to determine whether access has been authorized or unauthorized.

TABLE V: IOMT SECURITY ASSESSMENT AND SECURITY FACTORS

Categories	Sub-Categories
Compromise levels	Hardware
	Software
CIA compromise	Confidentiality
	Integrity
	Availability
Attack types	Individual
	Group
	State sponsored
Attack origins	Remote
	Local
Attack levels	Passive
	Active

Human errors (a human factor) are often overlooked as a major internal/insider threat. Lack of training, carelessness, or simple negligence can often occur when staff or third parties accidentally reveal patient data. For example, a third party such as a billing specialist may accidentally send an email revealing confidential information to the wrong person, thus permitting unauthorized persons to access confidential information. Creating a cybersecurity culture in the medical environment is essential to a robust cybersecurity program. Correct training and proper cybersecurity awareness, such as awarding staff who are proactive in protecting sensitive data or promptly reporting phishing attempts is also key to a robust cybersecurity program. Compliance officials and privacy officers must consistently walk through the work environment to check for other potential threats such as documents left on the copy machine, passwords on sticky notes stuck to the side of a computer, or unattended computers without screen savers.

There are external entities such as business associates (BA) who do have sensitive information access. Contractors, third-party vendors, consultants, etc. all work with healthcare providers. However, these associations can potentially constitute an internal/insider threat as one or more staff members may accidentally expose sensitive information, intentionally steal information, or fail to employ enough security measures. To prevent such occurrences, healthcare professionals and entities should do due diligence for all third parties and their relationship to the healthcare entity; ensuring that BAs have a sound understanding of cybersecurity principles and can comply with industry standards such as HIPAA, HiTech, etc. A Business Associate Agreement (BAA) should be executed when a third party has access to or discloses PHI on behalf of the healthcare entity. The healthcare entity should have a security team that monitors and audits BA compliance with the BAA requirements. BA should be vetted and trained in HIPAA, etc.

The most prevalent external threat to a healthcare entity is phishing or the practice of sending an infected email with a seemingly harmless email although it has malicious links. To ensure the email is opened for link clicking, phishing emails look very convincing and usually reference well-known information. Ransomware is another external threat and is malware injected into the network to infect and encrypt patient data until the medical center or hospital pays a ransom. Malicious actors typically use phishing emails to insert this malicious software. According to recent studies, ransomware attacks on hospital entities are a growing threat because malicious actors understand how critical patient data access is and how a disturbance in the access or transmission of patient data will maximize operational disturbances. Healthcare victims typically panic during a ransomware attack as regulatory consequences often follow the theft of patient data. Data breaches happen in healthcare

more often than in any other field. HIPAA has specific requirements for protecting PHI and other sensitive data from unauthorized access, but most healthcare facilities struggle with implementing security controls and a proper cybersecurity protocol. Instead, they leave gaps in cybersecurity that are openings for cyber criminals that continue to threaten patient data safety and other sensitive data, despite serious efforts to control exposure. A distributed denial-of-service attack (DDoS) targets the server, forcing it offline by flooding it with numerous connection requests. Multiple endpoints and IoT devices are controlled and forced into a botnet by a malware infection and participate in a coordinated attack.

VIII. Conclusion

The automation of AI/ML increases the speed of processing and makes it more efficient. The performance of ML substantially depends on data quality and data preprocessing. Actionable data is the cornerstone of cyber threat intelligence. Bias testing and metric selection are important components for assessing ML. Elimination of bias (such as measurement bias, prejudicial bias, sample bias, and algorithmic bias) is crucial. CTI represents actionable threat information that is helpful for proactive, preventive, and timely threat detection and remediation. Cybersecurity automation enhances the management of vulnerabilities, security incidents, and risks. Cybersecurity assessment in healthcare helps mitigate internal and external threats and reduce cyber risks. Creating a cybersecurity culture in the medical and healthcare environment is essential to robust cybersecurity.

Acknowledgements

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Conflict of Interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

[1] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT intrusion detection taxonomy, reference architecture, and analyses," *Sensors*, vol. 21, no. 19, p. 6432, 2021, doi: https://doi.org/10.3390/s21196432.

[2] G. Kumar, K. Thakur, and M. R. Ayyagari, "MLEsIDSs: Machine learning-based ensembles for intrusion detection systems - A review," *The Journal of Supercomputing*, vol. 76, no. 11, pp. 8938-8971, 2020, doi: https://doi.org/10.1007/s11227-020-03196-z.

[3] Y. Harel, I. B. Gal, and Y. Elovici, "Cyber security and the role of intelligent systems in addressing its challenges," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, pp. 1-12, 2017, doi: http://dx.doi.org/10.1145/3057729.

[4] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 13, no. 10, p. 2509, 2020, doi: http://dx.doi.org/10.3390/en13102509.

[5] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security*, vol. 108, p. 102376, 2021, doi: http://dx.doi.org/10.1016/j.cose.2021.102376.

[6] J. Tohka, and M. Van Gils, "Evaluation of machine learning algorithms for health and wellness applications: A tutorial," *Computers in Biology and Medicine*, vol. 132, p. 104324, 2021, doi: https://doi.org/10.1016/j.compbiomed.2021.104324.

[7] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, and

S. Bonacina, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, p. 5119, 2021, doi: https://doi.org/10.3390/s21155119.

[8] K. A. Al-Utaibi, and E.-S. M. El-Alfy, "Intrusion detection taxonomy and data preprocessing mechanisms," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 3, pp. 1369-1383, 2018, doi: http://dx.doi.org/10.3233/JIFS-169432.

[9] K. Nagarkar, and E. Russo, "Evaluating supervised machine learning classification models in healthcare analytics," White Paper, Milliman, Inc., Seattle, Washington, USA, Dec. 2022.

[10] P. A. Williams, B. Lovelock, T. Cabarrus, and M. Harvey, "Improving digital hospital transformation: Development of an outcomes-based infrastructure maturity assessment framework," *JMIR Medical Informatics*, vol. 7, no. 1, p. e12465, 2019.

[11] M. Rabbani, Y. Wang, R. Khoshkangini, H. Jelodar, R. Zhao, S. B. Baba Ahmadi, and S. Ayobi, "A review on machine learning approaches for network malicious behavior detection in emerging technologies," *Entropy*, vol. 23, no. 5, p. 529, 2021, doi: https://doi.org/10.3390/e23050529.

[12] Y. Miao, C. Chen, L. Pan, Q.-L. Han, J. Zhang, and Y. Xiang, "Machine learning–based cyber attacks targeting on controlled information: A survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, pp. 1-36, 2021, doi: https://doi.org/10.1145/3465171.

[13] B. Shin, and P. B. Lowry, "A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished," *Computers & Security*, vol. 92, p. 101761, 2020, doi: https://doi.org/10.1016/j.cose.2020.101761.

[14] S. M. Mohammad, and L. Surya, "Security automation in information technology," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 6, no. 2, pp. 901-905, 2018, doi: https://ssrn.com/abstract=3652597.

[15] F. A. Alzahrani, M. Ahmad, and M. T. J. Ansari, "Towards design and development of security assessment framework for internet of medical things," *Applied Sciences*, vol. 12, no. 16, p. 8148, 2022, doi: https://doi.org/10.3390/app12168148.