Computers & Security 137 (2024) 103627

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Data mining for cyber biosecurity risk management – A comprehensive review

Deepa D. Shankar [a,*], Adresya Suresh Azhakath [b], Nesma Khalil [c], Sajeev J . [a], Mahalakshmi T . [a], Sheeba K . [a]

[a] Abu Dhabi University, United Arab Emirates
[b] Danmarks Tekniske Universitet, Denmark
[c] Khalifa University of Science and Technology, United Arab Emirates

ARTICLE INFO

Keywords:
Cyberbiosecurity
Data mining

ABSTRACT

The world is currently facing the era of Cyberbiosecurity, also known as Biocybersecurity, or Digital Biosecurity, which poses a few unique security vulnerabilities. A significant percentage of the scientific, agricultural, and health communities are still unaware of the unique security complexities that have resulted from fusion of the supply chain, infrastructure, cyber, and life and medical sciences. Measurement, analysis, and mitigation of cyberattacks on biological systems are the goals of Cyberbiosecurity. Data mining is a promising avenue for further investigation as a means of mitigating cyber-attacks for research purposes. Data mining is the process of extracting useful patterns, information, and expertise from massive datasets. In the domain of Cyberbiosecurity, data mining techniques have received little attention. The purpose of this survey on data mining in cybersecurity is to determine the state of the art in cybersecurity issues, including different types of assaults and data mining methods that could be used to address these issues. This review's findings shed insight on the characteristics of security issues as well as gaps in Cyberbiosecurity. Furthermore, the review's conclusions show that most responses to Cyberbiosecurity attacks advocate for national or international government/private organizations to raise public awareness of these attacks and equip their clients/dealers with secure methods to transmit data online. These attempts to raise awareness can be divided into four distinct levels, each with its own set of techniques and objectives, resulting in a holistic strategy to addressing the difficulties of Cyberbiosecurity. A notable gap found in this review is the absence of appropriate countermeasures against cyberattacks employing data mining in the biological systems domain such as healthcare, agriculture, biomedical research, and other domains. The goal of this review is to increase knowledge among Cyberbiosecurity experts and to develop innovative solutions by utilizing cutting-edge data mining techniques in this sector.

1. Introduction

Cyberbiosecurity, also known as Biocybersecurity, is an interdisciplinary science that emerged in 2018, which converging three fields: Cyber Security, Cyber Physical and Biosecurity (Mueller, 2021). In this paper, the term Cyberbiosecurity is used extensively, as experts in this domain have been using it more than the term Biocybersecurity.

Cyberbiosecurity combines the crucial components of all three disciplines to protect the ever-expanding biotech landscape within cyberspace. One of the foundations of Cyberbiosecurity is cybersecurity, which is a well-researched field that primarily concerns the protection of computer systems against theft, damage, disruption, and illegal access to sensitive information. (Richardson et al., 2019). While cybersecurity has received much attention, its application to the unique issues of life sciences necessitates an interdisciplinary approach. It is crucial to emphasize that due to the unique characteristics and vulnerabilities of biological systems, the application of cybersecurity techniques to Cyberbiosecurity is not always straightforward.

Another component of Cyberbiosecurity is Cyber-Physical Systems (CPS). CPS is a collection of physical and computer components that are integrated with each other to ensure a safe and efficient operation of a process. These systems integrate sensing, data processing, control, and networking into physical objects and infrastructures, connecting them to cyberspace. CPS encompasses interconnected systems that serve as communication hub between physical, networking and computation processes (Yaacoub et al., 2020). The third component of

* Corresponding author.

https://doi.org/10.1016/j.cose.2023.103627
Received 29 April 2023; Received in revised form 25 October 2023; Accepted 24 November 2023
Available online 3 December 2023

Cyberbiosecurity is Biosecurity, which involves a set of procedures or measures designed to protect the population against harmful biological or biochemical substances deployed by threat actors. Threat actors impacting biosecurity risk may target valuable biological materials and related sensitive information leading to unauthorized acquisition, theft, diversion, misuse, or intentional release (Kurdan, n.d.).To address these risks effectively, organizations should adopt strong biosecurity measures encompassing physical security, access controls, data encryption, staff training, and well-defined incident response protocols (Latino and Menegoli, 2022).The goal is to mitigate the chance of a disease-causing element leaving an environment of foodstuff production and processing through people, animals, equipment, or vehicles (Latino and Menegoli, 2020).

The advent of Cyberbiosecurity has led to a significant rise in data exposure on the internet. Consequently, there is a growing concern regarding the protection and integrity of the enormous amount of data generated daily (Richardson et al., 2019; Malik et al., 2018).The process of digitization has paved the way for generating an immense volume of data, with humans creating, copying, and consuming around approximately 74 zettabytes (trillions of gigabytes) of data in 2021 alone (Yatsenko, 2022). Nowadays, data creation is not limited to scientists; even the common person plays a role in generating data, which makes it increasingly challenging to both find relevant information and protect data as time advances.

Considering aforementioned factors, the field of Cyberbiosecurity has three main concerns specific to life sciences, which are:

- Identifying potential risks that involve vulnerabilities and potential malicious activities that could target or exploit the life sciences infrastructure (Berger and Schneck, 2019) and technologies.
- Developing, validating, and implementing safeguards.
- Understanding risks that are specific to the life sciences.

In this study, we investigate data mining as a potential solution to these challenges in the context of Cyberbiosecurity. Data mining, the process of extracting valuable patterns, information, and knowledge from massive datasets, plays an important role in identifying and minimizing risks in the life sciences, and we will address its significance and potential in this expanding sector further. The study focuses mostly on the second pointer mentioned above.

The remainder of this paper is organized as follows: Section 2 presents the research methodology, Section 3 provides the background of the field, Section 4 summarizes the contributions, Section 5 discusses research issues within this domain, Section 6 explores future directions, Section 7 concludes the research.

Contributions

- Proposed modifications to the components of Cyberbiosecurity.
- Suggested a new architecture comprising a perception layer, transmission layer, and application layer.
- Defined the security goals of CBS.
- Identified the potential for CBS mitigation using data mining.
- Identified the characteristics of cyber-attacks in the domain of Cyberbiosecurity.

2. Research methodology

The research focuses on publications between 2018 and the present. Various keywords were chosen with an emphasis on security aspects like intrusion detection, malware detection, within the realm of Cyberbiosecurity, particularly concerning data mining techniques (Wu et al., 2021; Jothi and Rashid, 2015) as in Table 1. The search yielded several hits below 3 for exact keyword phrases. Nonetheless, the keyword phrase "Machine learning and Cyberbiosecurity" yielded 195 hits, highlighting the significance of research in this field.

A different analysis was conducted to verify the security trend in the discipline of Cyberbiosecurity within the context of data mining techniques. For this purpose, the year-by-year distribution (from 2018 to 2022) of the keywords used in Table 1 was used to create Table 2. Observations indicate an increase in research focused on “Machine learning and Cyberbiosecurity”. The topic “Need for Cyberbiosecurity” also experienced a substantial rise in hits relative to 2018.

3. Background

This section provides an overview of the related technologies of Cyberbiosecurity data science, including distinct types of Cyberbiosecurity incidents and defence strategies.

3.1. Cyberbiosecurity

The literature review conducted revealed a variety of definitions for

Table 1
Keyword search results of the distributed domains in Google scholar.

Keywords	Total Number of results	Exact Phrase	Excluding Citation	Excluding Patents	Excluding Citations and Patents
Need for cyberbiosecurity	340	1	335	335	330
Security in biological data mining	7,44,000	0	6,91,000	4,38,000	4,10,000
Security analysis of artificial intelligence in biological data mining	11,900	0	11,700	9550	9540
Biological data mining and security	10,600	0	7,08,000	4,48,000	4,10,000
Biological data mining and privacy	16,300	0	16,300	16,100	16,100
Biological data mining and cyberbiosecurity	6	0	6	6	6
Deep learning and cybersecurity	7860	0	7800	7800	7860
Cyber security data mining	13,200	2	13,200	12,700	12,700
Information security and data mining	28,70,000	0	27,80,000	26,60,000	25,60,000
Deep neural networks and biological data mining	1,17,000	0	1,16,000	1,04,000	1,02,000
Pattern matching and cyber security	19,000	0	19,000	15,300	15,200
Feature extraction and cyber security	23,700	0	21,900	21,500	19,700
Attacks in biological data mining	2,15,000	0	2,11,000	1,87,000	1,86,000
Attacks in data mining	7,27,000	0	6,76,000	6,39,000	5,90,000
Biological data mining	29,40,000	1	28,00,000	27,80,000	26,40,000
Machine learning and cyber biosecurity	195	0	194	192	191
Cyber security attacks in biological data mining	33,800	0	33,800	31,800	31,600
Adverserial ml in biological data mining	28,100	0	25,600	25,400	23,200
Biological data mining and privacy	14,900	0	1,470,000	1,340,000	1,380,000
Vulnerability analysis and biological data mining	202,000	0	204,000	189,000	189,000
Computer security and biological data mining	535,000	0	533,000	270,000	264,000
CNN and cyber security	19,500	1	19,400	19,000	19,000

Table 2
Keyword search results of the distributed domains in google scholar year wise.

Keywords	2018	2019	2020	2021	2022
Need for cyberbiosecurity	13	46	79	82	36
Security in biological data mining	23,300	25,400	27,400	29,300	16,600
Security analysis of artificial intelligence in biological data mining	12,500	14,500	16,400	17,700	9960
Biological data mining and security	23,300	25,400	27,400	29,400	16,700
Biological data mining and privacy	58,500	61,900	62,000	49,400	28,600
Biological data mining and cyberbiosecurity	1	9	19	18	6
Deep learning and cybersecurity	4410	7290	11,100	15,700	7740
Cyber security data mining	16,500	20,300	24,100	25,800	13,400
Information security and data mining	87,200	86,400	73,800	55,400	32,000
Deep neural networks and biological data mining	14,500	18,000	21,800	25,500	17,300
Pattern matching and cybersecurity	1530	2160	2770	3570	1580
Feature extraction and cybersecurity	1802	3080	4360	6280	3190
Attacks in biological data mining	17,400	18,100	19,100	19,100	12,300
Attacks in data mining	28,500	31,100	32,100	29,500	17,100
Biological data mining	78,800	72,300	64,100	50,300	29,800
MAchine learning andcyberbiosecurity	6	28	51	59	26
Cyber security attacks in biological data mining	16,000	16,100	16,200	16,400	10,300
Adverseral ml in biological data mining	582	1030	1680	2770	1550
Biological data mining and privacy	58,500	61,900	62,000	49,400	28,600
Vulnerability analysis and biological data mining	18,900	20,000	21,500	22,900	16,100
Computer security and biological data mining	22,200	23,500	24,100	25,800	20,000
CNN and cybersecurity	1580	2210	3360	5000	2680

the term Cyberbiosecurity, which are summarized below:

a) "Cyberbiosecurity illustrates the security vulnerabilities that occur at the juncture of cybersecurity, cyber-physical security, and biosecurity" (Murch et al., 2018).
b) "Cyberbiosecurity" has been defined as "understanding the vulnerabilities to intrusions, and malicious activities which can arise within or at the interfaces of life sciences, cyber and cyber-physical systems, and establishing measures to mitigate, investigate and attribute such threats as it pertains to security" (Murch and Di Euliis, 2019).
c) Cyberbiosecurity is a newly emerging interdisciplinary field at the convergence of life sciences and information technology (Richardson et al., 2019).
d) Cyberbiosecurity has been created to bring together disparate communities to identify and address a complex ecosystem of security vulnerabilities at the interface of life sciences, information systems, biosecurity, and cybersecurity (Richardson et al., 2019; Murch et al., 2018).
e) Attacks against DNA-information systems may follow well-known paradigms from computer security, and hence this field can also be defined as bio-cyber security (Ney, 2019).

The literature survey indicates that there is a collection of articles on the topic of Cyberbiosecurity (Murch and Di Euliis, 2019). Certain articles address the methods of accessing disseminating biological data or the absent of data sharing (Caswell et al., 2019). Conversely, some articles delve into the malicious use of valuable digitally stored information, such as employing DNA signatures to construct counterfeit genetically tailored organisms (Mueller, 2019). Other articles explain the defenses against cyber-attacks that target the food industry, the agriculture industry and those involved in DNA synthesis (Mueller, 2021).

A summary of the results of these articles can be found in Table 3, which reflects the current understanding of Cyberbiosecurity and the digitization of biology. The findings from Table 3 illustrate how computer networks, biological facilities, information systems, and data are vulnerable to various types of cyber-attacks. Some authors have highlighted the actual infiltration of networks in healthcare, corporate, and academia. Nevertheless, a systematic mapping of the cyber threat and risk landscape across the biological domain is notably absent.

The survey revealed that Cyberbiosecurity has applications in numerous disciplines. Some of these are given below (Richardson et al., 2019), and are discussed in detail in section 4.3.

i. Biomedical domain.
ii. Automation.
iii. Engineering of biology – biomaterials, biofuels – in agriculture and food systems.
iv. Biotechnology.
v. Synthetic biology domain.

The breadth of Cyberbiosecurity extends across nearly every aspect of human life, and data within these domains can potentially disrupt cyberspace. Therefore, protection of information from these areas is crucial. A comprehensive understanding of cybersecurity attacks, knowledge of cyber security threats and their solutions is essential. Moreover, these remedies can be employed to mitigate Cyberbiosecurity threats. In the subsequent section, the literature review of cyber security attacks is discussed.

3.2. *Review of cyber security attacks*

Various categories encompass cyber-attacks (Kaur and Ramkumar, 2021), such as phishing, malware, or the use of cryptography during the development process. A taxonomy of security breaches has been proposed by an author (Kaur and Ramkumar, 2021) in the context of cyber security. This classification comprises nine primary categories: cryptographic attacks, reconnaissance attacks, access attacks, active attacks, passive attacks, phishing attacks, malware attacks, quantum attacks, and web attacks. Both cryptographic and quantum attacks have seven subtypes, passive and phishing attacks have two subtypes, access, and reconnaissance attacks each have three subtypes, and the remaining three attack categories have four subtypes.

These attacks target the three fundamental security objectives, referred to as the CIA triad, which are confidentiality, integrity, and availability. Linking these attack types to the CIA helps to understand which aspect of security, or their combination thereof, is affected by the attack categories. This association is presented in Table 4.

All nine attack categories can result in a data breach, meaning confidentiality is broken by any of these attacks. Out of these, five of the attack categories can cause integrity and availability issues. This categorization can guide the security experts to formulate suitable measures based on the fundamental principles of information security.

Besides the three basic triads of security, data protection and availability are of equal significance within the Cybersecurity domain, as evidenced by the literature (Liu et al., 2021; Lou et al., 2019). Therefore, each of these aspects has been thoroughly reviewed based on various attacks that target them. A comprehensive overview of these aspects and their targeted attacks is provided, which is essential for understanding cyber security vulnerabilities and their solutions and will contribute to further Cyberbiosecurity research. This information is presented in Table 5. Social Engineering and malware attacks are also included in the table because they are prevalent in cyber security domain (Schaumont, 2018; Yuce, 2018; Balaban, 2019; Zahra and Chishti, 2019).

Table 3
Cyberbiosecurity review.

Work	Findings
(Wunsch and Hier, 2021)	The security of medical dataset is of paramount importance when these datasets are subjected to dimensionality reduction by data mining tools.
(Millett et al., 2019)	The security of critical infrastructure and data produced by the biotechnology industry depends on effective cybersecurity measures.
(Fujibayashi et al., 2021)	Demonstrate how a conventional nonlinear transformation from native space to template space made safe using security techniques.
(Berger and Schneck, 2019)	Current cyber risk management solutions focus on remediation through regulation, enterprise support, and data owner activities.
(Lv et al., 2021)	Identifying the optimal training duration that led to good online performance while using a variety of security measures
(George, 2019)	The need to limit cyber biological risk has become both necessary and vital because of new types of combination weapons.
(Vivaldi et al., 2021)	EEG ML system might be able to distinguish between different neurological diseases using cyber security measures
(Schabacker et al., 2019)	Roadmap for Cyberbiosecurity framework.
(Yeh and Chen, 2021)	A drug development system with safeguards to locate find appropriate drugs for GC and identify important biomarkers.
(Duncan et al., 2019)	A multidisciplinary approach involving expertise in food, agriculture, engineering, informatics, and cyber security is needed to develop new policies and strategies to protect data in these sectors.
(Madaan and Goyal, 2020)	Model based on ensemble learning techniques and Table appropriate safeguards, significantly outperforms traditional approaches.
(Caswell et al., 2019)	Problems with biological databases and strategies for ensuring database integrity
(Zhou et al., 2018)	The accuracy of LSTM and cyber security effects for the predicting DNA-binding residues is confirmed by additional feature analysis.
(Vinatzer et al., 2019)	Cited several potential cyber security vulnerabilities in today's pathogen gene databases and pointed the need for the community of those creating genomic databases to work together to establish a baseline security standard for new genomic database projects.
(Rashed-Al-Mahfuz et al., 2021)	The results show that when using the suggested machine learning models to diagnose CKD, optimized datasets with significant security features give good results.
(Mantle et al., 2019)	Cyberbiosecurity is becoming increasingly important to the biopharmaceutical manufacturing community due to technological and manufacturing advances in the manufacturing process and transportation.
(Guttieres et al., 2019)	Cyber-physical systems and vulnerabilities of cyber security systems (sabotage, industrial espionage, and crime) in current and future paradigms of bio-manufacturing addressed here.
(Diggans and Leproust, 2019)	Certain measures are promoted that can ensure synthesis screening systems keep well ahead of new difficulties and support ethical research advancements. These actions are partly inspired by accomplishments in the cyber security sector.
(Mueller, 2019)	"DNA signatures," are used to identify an organism and establish its presence using cyber security systems.
(Schmale et al., 2019)	Water security from the perspective of CPS and cyber security systems to identify, assess, and mitigate security risks to water infrastructure.
(L.C. Richardson et al., 2019)	Summarizes the current Cyberbiosecurity landscape and identifies existing vulnerabilities.
(Reed and Dunaway, 2019)	Artificial Intelligent personal assistants networked across multiple enterprises can be subjected to cyber bio security vulnerabilities
(Leung et al., 2015)	Here, more focus on how machine learning can use cybersecurity measures to simulate the link between DNA and the levels of important chemicals in cells.

Table 4
Categorization of cyber attacks.

Sl. No	Attack category	Sub type	Category of triads
1.	Cryptographic attack	Attention-based LSTM encoder-decoder (Ahmadzadeh et al., 2021), side channel attack (Lerman et al., 2011), replay attack (Pries et al., 2008), differential crypt analysis (Heys, 2002), linear crypt attack (Lee et al., 2002)	Confidentiality, Integrity
2.	Access attack	Trust exploitation attack (Wong et al., 2014), port redirection attack (Sulaiman, 2012), password attack (Tasevski, 2011)	Confidentiality
3.	Reconnaissance attack	Packet sniffer attack (Anu and Vimala, 2017), port scanning attack (El-Hajj et al., 2008), ping sweeps attack (Teo, 2000)	Confidentiality
4.	Active attack	impersonation attack (Aminanto and Kim, 2016), message modification attack (Yang et al., 2013), Masquerade attack (Salem and Stolfo, 2009), replay attack (Pries et al., 2008),	Confidentiality, Integrity, Availability
5.	Passive attack	Traffic analysis attack (Kausar et al., 2019), message content release (Bruce et al., 2017)	Confidentiality, Availability
6.	Phishing attack	Spear phishing attack (Halevi et al., 2015), whale phishing attack (Yadav and Bohra, 2015)	Confidentiality, Integrity
7.	Malware attack	Ransomware attack (Tandon and Nayyar, 2019), drive by attack (Sood and Zeadally, 2016), Trojan horse (Gisin et al., 2006), worm (Xie et al., 2005; Ney et al., 2017) Bio malware (Elgabry, 2023)	Confidentiality, Integrity, Availability
8.	Quantum attack	coherent attack (Kronberg, 2014), intercept resend attack (Lin et al., 2013), detector blinding attack (Yuan et al., 2010), collective attack (Pirandola et al., 2008), time-shift attack (Qi et al., 2005), Individual attack (Tamaki et al., 2003), photon number splitting attack (Lütkenhaus and Jahma, 2002),	Confidentiality, Availability
9.	Web attack	denial-of-service attack (Jamal et al., 2018), session hijacking (Jain et al., 2015), Cross site scripting (Vogt et al., 2007), SQL injection (Boyd and Keromytis, 2004),	Confidentiality, Integrity, Availability

In the domain of Cyberbiosecurity, cyber-attacks primarily affect the biological data transferred through the network. Among these data, DNA sequences are commonly used, particularly in the domain of synthetic biology. One tool used to protect this data is steganography.

Steganography involves hiding messages inside another medium, known as cover media. This cover media can be an image, a text message, or even a DNA sequence. Concealing messages within a DNA sequence is referred to as DNA Steganography, which offers the advantage of hiding large volumes of data using different encoding techniques.

In DNA Steganography, the process of encoding differs significantly from other Steganography techniques. The message that needs to be hidden in a DNA sequence must first be encoded into a short DNA sequence, i.e., a sequence made of letters A, G, C and T.

Table 5
Attack categorization in security aspects and possible solutions.

Security Aspects/ Category	Attack Type	Solutions	Possible Reason(s)	Reference
Privacy	Machine learning Attack	Adversarial Training	Lack of security to Training data (input), ML Model, ML Model output	(Liu et al., 2021)
	Traffic Analysis	VPNs & Proxies Non-Likability Pseudonyms	Source and destination information is not encrypted. Lack of secure channels Weak encryption algorithm	(Joshi and Hadi, 2015)
	Identity / Location Tracking	Anonymity Non-Likability Pseudonyms	Secure channel absence No encryption is used for location or identifying parameters.	(Son et al., 2015; Wex et al., 2008)
Data Confidentiality	Eavesdropping	Encryption	Broadcast messages that travel across wireless channels Unencrypted Communication channel	(Coleman and Westcott, 2012)
	Data Interception	Encryption	Non-Secure Channels Open Wireless Communications	(He et al., 2017)
	Packet Capturing	Encryption	Open Wireless Communications Non-Secure Channels Lack of Encryption	(Braun et al., 2010)
	Dumpster Diving	Improved Employee Training Paperless Process	Lack of Employee Training Lack of Awareness	(Koyun and Al Janabi, 2017)
Data Integrity and Message Authentication	Message Tampering-Alternation Malicious data injection Malicious Script Injection Cloning & Spoofing	Keyed Hash Function (HMAC). Message Authentication Algorithms	No source authentication or data integrity protections are in place.	(Jain et al., 2004; Liu et al., 2011; Rahman and Mohsenian-Rad, 2012; Shah et al., 2016; Spiekermann, 2015; Yang et al., 2013; Wang et al., 2010)
Availability	Jamming	Frequency Hopping, direct sequence, spread spectrum, beam-forming	Target Access Points or wireless IoMT devices	(Grover et al., 2014; Proano and Lazos, 2010; Vadlamani et al., 2016)
	Denial Of Service	Backup Devices	Absence of Backup Devices	(Carl et al., 2006)
	Distributed Denial of Service (DDOS)	DDOS detection solutions. To prevent transforming to bots, security levels of your gadgets should he upgraded	Use tools to transform them into bots	(Bhuyan et al., 2014)
	De-authentication	Firewalls, Instruction Detection Systems, Encryption	uses a handshake to launch a denial-of-service attack or password-cracking attempt.	(Noman et al., 2015)
	Flood	Timestamps, Certificate Authority, IDS	False information injection overwhelms and exhausts IoMT's resources.	(Baig and Amoudi, 2013)
	Delay	Firewalls, Timestamps, IDS	overwhelms and severely hinders or delays the transmission of critical data.	(Lou et al., 2019)
Authentication	Man-in-the-Middle	Multi-Factor authentication scheme	Weak authentication scheme (one factor)	(Liang et al., 2016)
	Masquerading	Multi-Factor authentication scheme	Weak authentication scheme (one factor)	(Kumar et al., 2012)
	Cracking	Multi-Factor authentication scheme	Weak authentication scheme (one factor)	(Liang et al., 2016)
	Reply	For each session connection, a fresh random number or a timestamp is used. Multi-Factor authentication scheme	The authentication process is insecure	(Baig and Amoudi, 2013; Grunwald, 2006; Spiekermann, 2015)
	Dictionary	Strong password Sufficient size of the secret key	single authentication factor and a weak password	(Cho et al., 2011; Nam et al., 2009)
	Brute force	Strong and long password Sufficient size of the secret key Multi-Factor authentication scheme	Weak password and single authentication factor	(McMahon et al., 2017; Ten et al., 2010)
	Rainbow Table	Long Salt Passwords	Weak Username / Password Short Salt Passwords	(Narayanan and Shmatikov, 2005; Tahir et al., 2013)
	Birthday	Secure Hash Algorithm	Weak Hashing	(Bellare and Kohno, 2004)
	Session Hijacking	Encryption Sniffing Filters	Lack of / Poor Encryption Non-Secure Channels	(Baitha and Vinod, 2018)
Social Engineering	Social Engineering	Educating employees about pre-texting and baiting	A lack of personnel training	(Heartfield and Loukas, 2015)
	Reverse Social Engineering	Staff education regarding questions from strangers	No methods for identification and verification	(Irani et al., 2011)
	Error Debug	Object information that takes shape	Additional information is provided via various error questions.	(Schaumont, 2018; Yuce, 2018)
Malware	Botnet	Solution for detecting botnets (anti-malware), penetration testing, and intrusion detection	a logical grouping of IoMT devices—Internet of Things devices—that have been exploited	(Bellare and Kohno, 2004; Kambourakis et al., 2017; Kolias et al., 2017; Stone-Gross et al., 2009; Zhang et al., 2011)

(*continued on next page*)

Table 5 (*continued*)

Security Aspects/ Category	Attack Type	Solutions	Possible Reason(s)	Reference
	Worm & Viruses	Anti-virus, anti-malware, pen-testing, intrusion detection	relying on breaches in computer network security	(Cooke et al., 2005; Edwards and Profetis, 2016; Falliere et al., 2011)
	Spyware	Employ antivirus and anti-spyware software, keep the operating system up to date, ensure enhanced security and privacy measures, and implement intrusion detection.	Downloads from file-sharing websites or included in other software	(Lee and Kozar, 2005)
	Remote Access Trojan	Ensure antivirus software is regularly updated, block unused ports, and implement intrusion detection	Invisibility that was downloaded using an application or fresh software	(Alperovitch, 2011)
	Rootkit	Suitable system setup, robust authentication, updates and configuration control, and intrusion detection	Root privileges are obtained by exploits that either target the kernel or the user application space.	(Lobo et al., 2010)
	Ransomware	Using the latest Anti-Virus / Anti-Malware tools, refraining from using personal information, strengthening system security, and promoting greater awareness.	Weak Passwords, Weak Multi-Factor, Paying Ransoms.	(Balaban, 2019; Dickson, 2016; Yaqoob et al., 2017; Zahra and Chishti, 2019)

Another crucial consideration when concealing the encoded message within a DNA sequence is that the original function of the cover media (DNA sequence) must be retained. Data can be hidden in different ways, such as inserting the enclosed message in one stretch or in parts. To preserve the functionality of the cover media, the hidden message within it should align with the original cover media. This alignment will ensure the similarity between both sequences.

3.3. Review of data mining techniques

The previous section discussed various types of cyber-attacks and their solutions, particularly in the field of biotechnology and biological data. These solutions can be broadly divided into statistical methods and data mining techniques. Statistical methods are intended for making inferences about the relationships between variables, while machine learning models are designed to make the most accurate predictions possible (Yatsenko, 2022). Therefore, this section provides a review of data mining techniques as solutions for cyber security problems.

In general, data mining techniques can be categorized into two types: predictive and descriptive techniques. Predictive techniques can be subdivided into three types: classification, regression, and time series analysis, while descriptive techniques can be divided into three types: clustering, summarization, and associative rule analysis (Yatsenko, 2022). The algorithms within these techniques can be employed as solutions to cyber security problems, and some of these solutions are listed in Table 6. To illustrate the wide range of applications of these algorithms, Table 6 also lists works from cyber security and other application domains that make use of data mining techniques.

Table 6 provides an overview of different types of solutions for cyber security attacks through the utilization of data mining algorithms. It's possible to adapt and customize these solutions to address Cyberbiosecurity attacks within diverse cybersecurity applications. This will be discussed in the following section.

Table 6
Application of data mining algorithms as solutions in cyber security problems and others.

Sl. No	Data Mining Algorithm	Cyber security problems that use the algorithm.	Works	Works from other area that uses the algorithm
1	Deep neural networks	Trojan attacks detection	(Islam et al., 2022),	(Xue et al., 2020; Guo et al., 2017; Lee et al., 2019; Mahmud et al., 2021; Juuti et al., 2019)
2	Artificial neural networks	DNA injection attacks detection	(Farbiash and Puzis, 2020; Islam et al., 2019),	(Yang et al., 2020; Alloghani et al., 2020)
3	Random Forest	Ransomware detection	(Khan et al., 2020)	(Y. Chen et al., 2021)
4	SVM	Intrusion detection system	(Abdullah and Abdulazeez, 2021),	(Handa et al., 2019; Xue et al., 2020; Kantarcioglu and Xi, 2016; Tong et al., 2019)
5	KNN	Intrusion detection system	(Liu et al., 1407)	(Xiong and Yao, 2021)
6	Naïve Bayes	Intrusion detection system	(Gu and Lu, 2021),	(Kantarcioglu and Xi, 2016)
7	C4.5	Ransomware detection	(Kuswanto and Anjad, 2021)	(Tempola et al., 2022)
8	C5.0	Intrusion detection system	(Hao et al., 2022)	(Murugan Bhagavathi et al., 2021)
9	LDA	Malware detection	(Smmarwar Smmarwar et al., 2022)	(Ignaczak et al., 2021, Adams et al., 2018)

3.4. Review of data mining solutions for cyberbiosecurity applications

The literature review has revealed that Cyberbiosecurity plays a key role in various areas such as Bio-manufacturing, Synthetic Biology, Automation, Agriculture, and Biomedicine, as discussed earlier in this section. Therefore, a survey was conducted to identify the type of mitigation/solutions using data mining techniques for the attacks/threats identified in these domains.

One of the applications of Cyberbiosecurity is bio-manufacturing. The literature review reveals a significant rise in the number of organizations relying on science and technology for security aspects in this field (Walsh, 2022). Bio-manufacturing organizations use biological systems to produce important biomolecules and materials for medical purposes such as pharmaceutical production, tissue engineering, and regenerative medicine etc. (Dixon et al., 2021). The procedure entails harnessing living cells, microorganisms, or biological elements to generate substances of therapeutic or medical importance (Szychlinska et al., 2019). Since these organizations are targets of security attacks, special care should be taken to mitigate such issues. The literature review also reveals that Machine Learning techniques have been proposed as solutions to these attacks in this field, as shown in Table 7. Ranging from support vector machine techniques to the latest deep learning techniques, security attacks in this area can be effectively mitigated. In (Albattah et al., 2022), SVM techniques were combined with deep learning models to improve the robustness of plant disease classification systems against adversarial attacks. The integration of SVM techniques can aid the system in addressing specific adversarial perturbations better

Table 7
Data mining algorithms as solutions for Cyberbiosecurity applications.

Application Domain	Author	Technology
Bio-manufacturing	(Naser et al., 2021)	Deep neural network
"	(Sanicola et al., 2020)	Deep learning
"	(Kavakiotis et al., 2017)	Support vector machine
Synthetic biology	(Chen et al., 2021)	XGBoost regression algorithm
"	(Moorman et al., 2019)	Biomolecular neural network
"	(Wang et al., 2017)	Squared linear mixed model
"	(Giaretta et al., 2015)	Bayes' rule
Automation	(AL MOGBIL et al., 2020)	Machine learning
"	(Jose et al., 2016)	Device fingerprinting algorithm
"	(Varga et al., 2017)	Machine learning
Agriculture	(Tawalbeh et al., 2021)	Deep neural network
"	(Vangala et al., 2020)	Deep learning
"	(Ferrag et al., 2020)	Deep learning
Biomedical	(LeMoyne and Mastroianni, 2020)	Machine learning
"	(Fatima et al., 2020)	Supervised learning
"	(Snigdha et al., 2020)	Support vector machine and K Nearest Algorithm
"	(Yang et al., 2017)	Deep learning

suited for traditional machine learning. Concurrently, the incorporation of deep learning enables the system to effectively capture intricate image patterns and features, thereby enhancing its accuracy and resilience against diverse forms of attacks.

Another application of Cyberbiosecurity is in the field of synthetic biology. Synthetic biology is closely associated with disciplines such as chemistry, bioengineering, and molecular biology. Advances in synthetic biology are a major concern of Cyberbiosecurity because laboratory automation techniques are now widely available, which can attract the attention of cybercriminals. This new possibility of exploitation can only be addressed through advanced research. The utilization of machine learning techniques as a solution to these attacks in this field, as described in the literature, is shown in Table 7. A variety of methods, ranging from Bayes' rule to the most recent XGBoost regression techniques, are employed in this field. The Biomolecular neural network technique is also considered a solution for cyber-attacks in this domain.

The next application in Cyberbiosecurity is within the field of automation. Automated approaches in biology, manufacturing, education, and various other fields are enabled using robotics, AI, machine learning, and similar cutting-edge technologies. It has also been found that merging biological engineering techniques with robotics yields better results (Malik et al., 2018). Since all these assets are networked, they are vulnerable to cyber security attacks. The use of machine learning techniques as a solution to these attacks in this field, as described in the literature, is shown in Table 7. It can be observed that the device fingerprinting algorithm and various machine learning algorithms are used to provide a solution to cyber-attacks in this domain.

Another application of Cyberbiosecurity involves agriculture. In many countries, agriculture and related consumer products are being cyber-enabled to maximize efficiency in terms of food safety, contamination detection, outbreak analysis, and other novel analytics (Pauwels, 2019). This domain also attracts the attention of cyber criminals. The presence of advanced machine learning techniques as a solution to these attacks in this area, as seen from literature, is depicted in Table 7. It is seen that deep learning techniques are used to find solutions for cyber-attacks in this sector.

Another promising application of Cyberbiosecurity is Biomedical Science. Some key areas include medical and billing information, patient records, personalized medicine information, and medical expert systems (Richardson et al., 2019). The workings in this area are based on cyberspace infrastructure and are hence prone to cyberspace vulnerabilities. The use of machine learning techniques as a solution to these attacks in this area, as described in the literature, is demonstrated in Table 7. Support Vector Machines, K Nearest Algorithm, Supervised learning algorithms, and Deep learning techniques are employed to find solutions for cyber-attacks in this domain.

This study establishes data mining as an effective solution for a range of applications within the Cyberbiosecurity field. Further review has shown that there are opportunities to improve these solutions which are discussed in the next section.

A more detailed study of this topic is also available on (Greenbaum, 2023). The author also discusses case studies involving cyber-attacks across diverse domains, strategies for mitigation threats through AI techniques, the development of Biocybersecurity policies, and the utilization of CVSS for assessing vulnerability scores in Cyber-Biological systems etc.

CVSS captures the principal technical characteristics of vulnerabilities, including their impact on confidentiality, integrity, and availability. These components are quantified through various metrics, including Base Metrics, Temporal Metrics and Environmental Metric (Greenbaum, 2023).

In the context of Cyberbiosecurity, performing security scoring and vulnerability assessments necessitates a comprehensive approach. This entails integration of aspects from conventional cybersecurity frameworks, such as CVSS, with specialized expertise in the life sciences and biotechnology domains. The goal is to tailor risk assessment methodologies to address the unique characteristics and challenges inherent in this field (Greenbaum, 2023).

In (Carreón et al., 2021), the authors present a medical vulnerability scoring system (MVSS) in their paper, which considers both the health impact and data sensitivity metrics. In this case, the authors have developed the Medical Vulnerability Scoring System (MVSS) by building upon CVSS. The goal of MVSS is to offer a vulnerability impact score designed specifically for medical devices.

In (Puzis and Veksler-Lublinsky, 2023), the authors contend that the intricacies of the biological domain introduce extra elements, including the possibility of biological harm, genetic manipulation, or environmental consequences, which the traditional CIA triad fails to fully address. Consequently, they advocate for a more customized and refined vulnerability scoring approach for cyber-biological systems, integrating biosecurity and biosafety considerations alongside conventional cybersecurity principles. Therefore, it can be observed that this is a debatable issue, and a more comprehensive and domain-specific approach is necessary to address the unique challenges of this emerging field.

4. Summary of contributions

Contribution 1: Components of Cyberbiosecurity:

The field of cybersecurity has emerged from a combination of three different fields: cybersecurity, cyber-physical security, and biosecurity. The literature review uncovered a range of definitions for the term Cyberbiosecurity, as described in the preceding section. These definitions and the applications of Cyberbiosecurity make it clear that numerous other areas also have a significant role in this field. Consequently, the components of Cyberbiosecurity (Duncan et al., 2019) can be modified and proposed as shown in Fig. 1.

The most significant change in the components of Cyberbiosecurity is the inclusion of information systems, biology, life sciences, and biotechnology. The tremendous development of information systems infrastructure has also paved the way for newer and modern security vulnerabilities in Cyberbiosecurity. The data source for the biosecurity component mainly comes from biology, biotechnology, and life sciences.

The inclusion of information systems, biology, life sciences, and biotechnology can have significant implications for assessment techniques, detection, and mitigation of various issues. Some concrete actionable insights that can be derived from their integration:

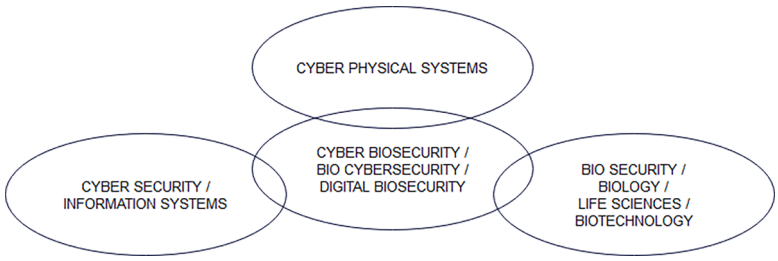

Fig. 1. Components of cyberbiosecurity.

- Assessment - Biometric security (Hu et al., 2015) can be considered as a security assessment technique.
- Detection - Biological signatures, akin to biological markers used in medicine, can be applied to detect malware based on unique characteristics (Grigorieva and Petrenko, 2023).
- Mitigation - Biological Inspired Incident Response strategies can be designed to detect, isolate, and contain threats quickly and efficiently (Nespoli et al., 2021).

Contribution 2: Architecture of Cyberbiosecurity:

After examining the security challenges in the various cyber-physical system layers (Ashibani and Mahmoud, 2017), Ashibani and Mahmoud presented a three-layer architecture for these systems. The layers are the perception layer, the transmission layer, and the application layer, based on the functions at each layer. This design can be modified and defined by the devices within it and the corresponding functions that are implemented, as shown in Fig. 2 which had been adopted from (Ashibani and Mahmoud, 2017). This is done by taking into consideration the numerous developments that have been made.

The proposed application layer includes smart health, smart manufacturing, smart agriculture, and smart cyberspace. During the COVID-19 pandemic, health care systems faced significant cybersecurity challenges (Majumder and Veilleux, 2021). Smart health and cybersecurity are prioritized in the developing field of Artificial Intelligence (Majumder and Veilleux, 2021). In smart manufacturing, Cyberbiosecurity plays an important role in securing biomedical and biotechnology products and data (Millett et al., 2019). The vulnerabilities in the deployment of smart farming ecosystems should be addressed for the existence of smart agriculture (Sontowski et al., 2020). The common challenges and solutions to advance the role of Cyberbiosecurity in the food and agricultural sector are addressed in the application layer (Duncan et al., 2019). Increasing cyber-attacks on synthetic DNA pose a threat to DNA synthesizers that should be addressed and prevented for the survival of smart cyberspace (Puzis et al., 2020).

The transmission layer consists of Wi-Fi, the Internet, and LAN, which are involved in data transmission, while the perception layer comprises sensors, RFID, clinical data, and genomic data, which act as the input layer.

Many defense techniques have been developed to protect Big Data against a variety of security threats (Liu et al., 2018). Vulnerabilities in Cyberbiosecurity can cause harm to human health and the environment, either intentionally or unintentionally. Intentional manipulation of genetic data can lead to the generation of harmful organisms, and the unintentional or accidental release of genetically modified organisms (GMOs) or pathogens into the environment can cause serious issues.

Contribution 3: Security goals of Cyberbiosecurity:

The security goals of Cyberbiosecurity (referred to as Logical Cyberbiosecurity) can be defined in accordance with the goals of Cyber-Physical Systems which are centered on data protection, system protection, and device protection (Yaacoub et al., 2020). This view of goals, such as confidentiality, integrity, and availability can be expanded in the context of cyber biosecurity by including the data model protection goal as well. This concept is illustrated in Fig. 3. The diagram is an enhanced version of (Yaacoub et al., 2020).

Contribution 4: Characteristics of cyber-attacks:

Understanding the various characteristics of cyber-attacks is

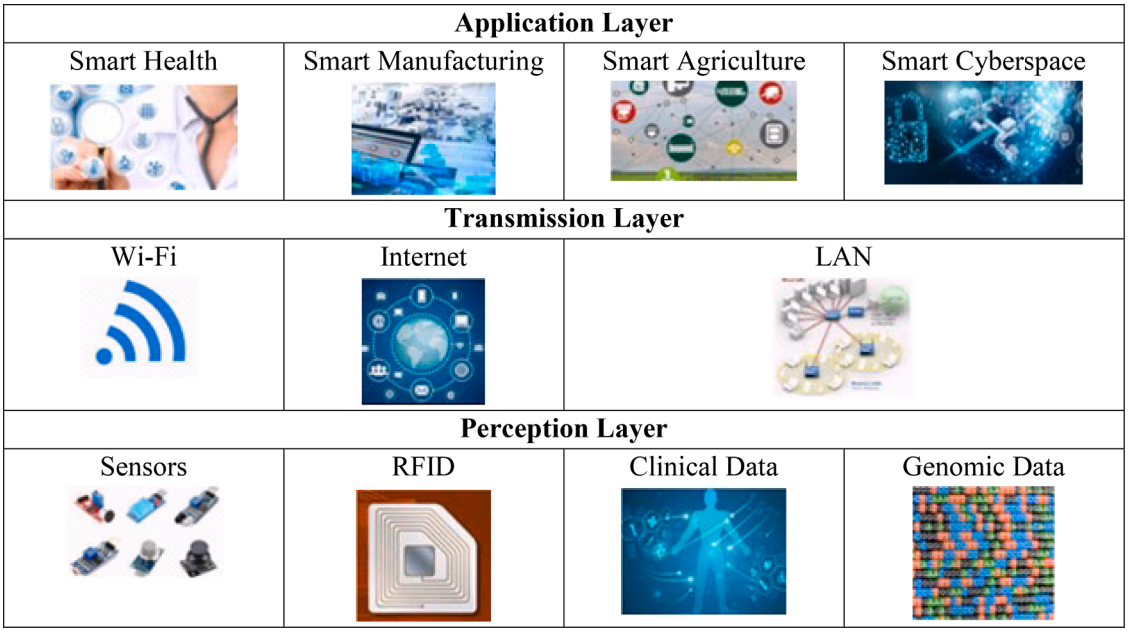

Fig. 2. Proposed three layer architecture for cyberbiosecurity.

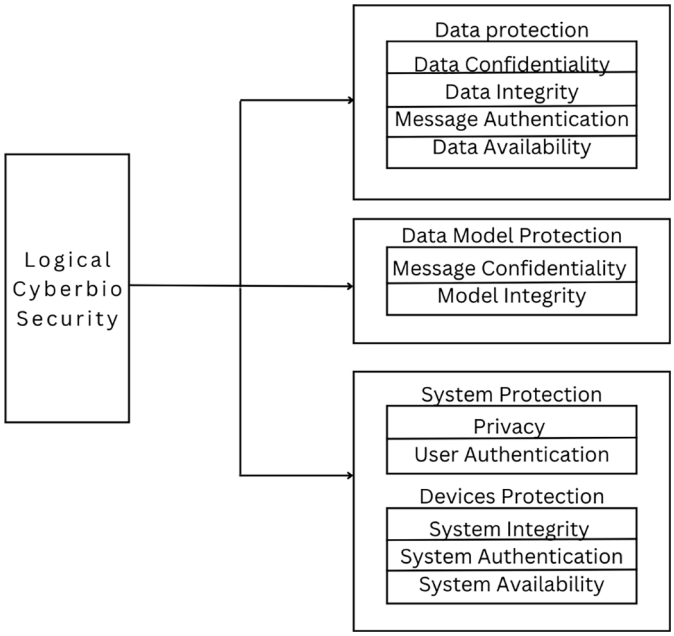

Fig. 3. Proposed goals of logical cyberbiosecurity.

essential before identifying and classifying a specific attack (Yaacoub et al., 2020). In general, attacks can be classified into one of five major categories, as illustrated in Fig. 4. Furthermore, attacks can be classified based on their characteristics such as nature, target, scope, capacity, impact, as well as attacker's skills, knowledge, experience, available tools, and resources, as illustrated in Fig. 4. In the domain of Cyberbiosecurity, attacks are primarily targeted in fields such as smart health, smart manufacturing, and so on. This represents a significant difference in the characteristics of cyber-attacks in Cybersecurity compared to other domains, and this is depicted in Fig. 4. The diagram is an enhanced version adopted from (Yaacoub et al., 2020).

5. Research issues

The survey has identified three key issues related with CBS:

1. Over the last decade, cyber-attacks on the biological domain have increased with alarming frequency and catastrophic consequences, especially in the domain of healthcare. The healthcare industry possesses significant vulnerabilities in terms of its cybersecurity defense, making it a potential target for cyberattacks. In the past three years, an alarming 93 % of healthcare organizations have faced a breach of their data security (ABC 2023).This has led to the development of Cyberbiosecurity measures based on data mining techniques. Despite the plethora of literature on the efficacy of this technology is available, the authors intend to review the literature on Cyberbiosecurity from 2018 onwards to gauge the data mining technique's effectiveness in mitigating cyber-attacks on biological domains. Cyber-attack categorization and solutions will be based on keyword index and abstracts gathered for this study.
2. It is possible that some articles on data mining solutions might not have appeared in the authors' radar screen due to keyword search limitations. The authors' omission of these reference sources could be attributed to their own limitations.
3. This study excluded non-English publications; however, it's conceivable that articles on Cyberbiosecurity have been published in other languages as well.

Identifying gaps in CBS can provide valuable guidance for future research within this domain. A research gap is an unknown topic uncovered during a literature review that needs further research. The current review has identified multiple gaps that can be explored using data mining solutions in the field of Cyberbiosecurity. These findings are summarized in Table 8.

6. Discussion

Several research efforts have been made towards Cyberbiosecurity solutions, as discussed in the sections above. This paper provides an in-depth analysis of Cyberbiosecurity data science, and to achieve this, we conducted a literature review to gain insights into cybersecurity defense

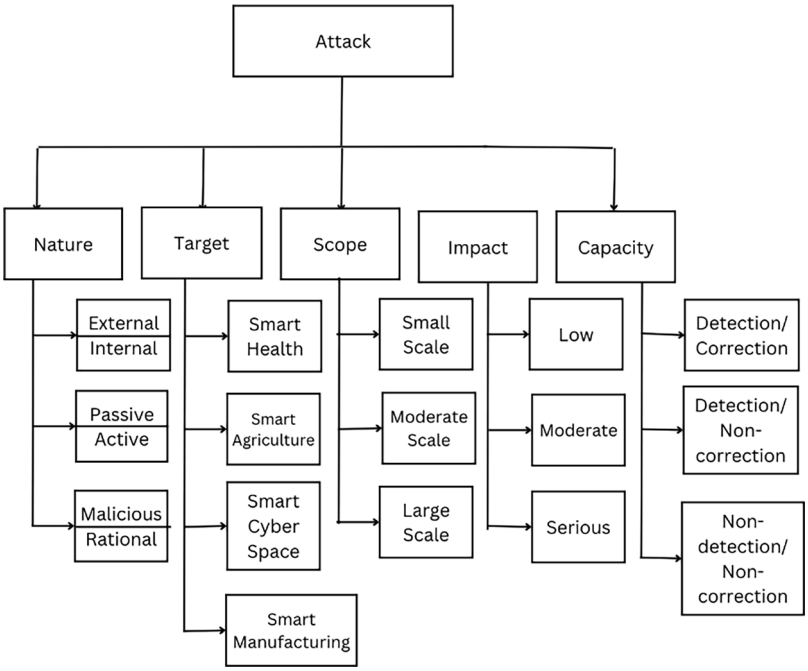

Fig. 4. Proposed characteristics of cyber attacks.

Table 8
Gaps identified for future work.

Work	Purpose	Existing Solution	Gap identified for future work
(Islam et al., 2022)	Safeguard DNA sequencing against Bio-Cyber-attacks.	Deep Learning technologies and an extension of the DNA Steganography technique.is used.	Use of adversarial machine learning
(Khan et al., 2020)	Ransomware Detection Using Machine Learning.	Classification algorithms Naïve Bayes (NB), Random Forest (RF) and Sequential Minimal Optimization (SMO) are used to investigate the ransomware family.	Enhancement using deep learning
(Farbiash and Puzis, 2020; Islam et al., 2019)	Detection of malicious DNA injection.	An improved screening protocol that considers in-vivo gene editing and recommends data mining solution in future.	Apply machine learning/deep learning

strategies aimed at mitigating Cyberbiosecurity threats. Additionally, ML and DL techniques are immensely common in the mitigation of Cybersecurity threats, and the possibility of the same in CBS is thoroughly examined in this review.

Following our analysis of previous research, we have identified multiple research challenges associated with biological datasets, data encoding problems, malware encoding strategies, Steganography verification matrix, learning methods, feature engineering through deep learning, and security alert generation. These areas require further research attention within the domain of Cyberbiosecurity data science.

Cyberbiosecurity data science has an extensive scope, involving numerous data-driven functions, such as detecting and preventing malware injections, managing access controls, generating security policies, identifying anomalies, filtering data, preventing, and detecting fraud, and deploying diverse defense strategies. These tasks leverage advanced machine learning and deep learning algorithms. These categorized tasks can aid security professionals, including researchers and practitioners, who have a keen interest in the bio-domain-specific aspects of security systems.

Cyberbiosecurity data science has a wide range of application areas, including synthetic biology, network security, cloud security, and other relevant cyber areas where malware injection attacks are prevalent. The outputs of Cyberbiosecurity data science are utilized in these domains to enhance security measures.

In this paper, our focus has been on the use of Cyberbiosecurity data science for examining raw biological data and making data-driven decisions for synthetic biology-related security solutions. However, it is worth noting that Cyberbiosecurity data science can also be related to big data analytics since biological data falls under the category of big data. Big data analytics deals with large or complex data sets characterized by high volume, velocity, and variety. Therefore, the techniques and methods used in Cyberbiosecurity data science can be applied to big data analytics as well.

The analysis typically involves examining these datasets to identify patterns, undisclosed relationships, rules, and valuable insights. As a result, various sophisticated data analysis methods like machine learning and deep learning can be vital in handling big data by decomposing extensive tasks into smaller components. To achieve this, potential strategies such as divide-and-conquer, feature extraction, sampling, and feature or instance selection can be employed to improve decision-making, reduce costs, and enable more efficient processing. In similar scenarios, the concept of Cyberbiosecurity data science, particularly advanced machine learning/deep learning-based modeling, could be helpful in automating processes and making intelligent decisions for security solutions.

7. Conclusion

Cyberbiosecurity, which is the intersection of cyber security, cyber physical security, and biosecurity, faces vulnerabilities due to the proliferation of Do It Yourself (DIY) kits. To improve security in this field, several suggestions were proposed based on the extensive review conducted in this paper. These include:

a. Modification of Components in Cyberbiosecurity
b. A new three-layer architecture for Cyberbiosecurity
c. Goals for security aspects in Cyberbiosecurity
d. Characteristics of the security aspects in Cyberbiosecurity
e. The identification of open questions (Gaps) in Cyberbiosecurity

The main gap identified was the lack of appropriate protection against cyberspace attacks in the biological data domain. Data mining has been proven to be a factor in mitigating these solutions, but further research is essential to successfully achieving cyber security goals. Alternative methods of mitigation can include regulation, enterprise support, and data owner activities (Mueller, 2019).

In essence, the mitigation of cyber-bio attacks involves two primary aspects: reducing the probability of an attack and minimizing the adverse impact of any occurred attacks. Important factors that contribute to potential mitigation are deterrence and prevention capabilities, the ability to detect an attack, attribution capabilities, and consequence management capabilities. It is becoming apparent that many of the tools used to mitigate natural infectious diseases are also relevant to mitigating an intentional biological attack. Therefore, the role of advanced data mining tools and techniques needs to be further explored to see how they can be used for this purpose.

This review serves as a call to action for researchers, policymakers, and industry professionals to prioritize this emerging field and harness the power of data mining to ensure a secure future.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgement

The authors would like to acknowledge the financial support provided by the Research Office, Abu Dhabi University for the grant 19300613.

References

ABC, "Safety Detectives," 2023. [Online]. Available: https://www.safetydetectives.com/blog/healthcare-cybersecurity-statistics/.
Abdullah, D.M., Abdulazeez, A.M., 2021. Machine learning applications based on SVM classification a review. Qubahan Acad. J. 81–90.
Adams, S., Carter, B., Fleming, C., Beling, P.A., 2018. Selecting system specific cybersecurity attack patterns using topic modeling. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12t. August.
Ahmadzadeh, E., Kim, H., Jeong, O., Moon, I., 2021. A novel dynamic attack on classical ciphers using an attention-based LSTM encoder-decoder model. IEEE Access 9, 60960–60970.
AL MOGBIL, R., AL ASQAH, M., EL KHEDIRI, S., 2020. Iot: security challenges and issues of smart homes/cities. In: 2020 International Conference on Computing and Information Technology (ICCIT-1441). IEEE, pp. 1–6.

Albattah, W., Nawaz, M., Javed, A., Masood, M., Albahli, S., 2022. A novel deep learning method for detection and classification of plant diseases. Complex Intell. Syst. 1–18.

Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T., Aljaaf, A.J., 2020. Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber attacks. Nature-Inspired Computation in Data Mining and Machine Learning. Springer, Cham, pp. 47–76.

Alperovitch, D., 2011. Revealed: Operation Shady RAT, 3. McAfee, p. 2011.

Aminanto, M.E., Kim, K., 2016. Detecting impersonation attack in WiFi networks using deep learning approach. In: International Workshop on Information Security Applications. Cham. Springer, pp. 136–147. August.

Anu, P., Vimala, S., 2017. A survey on sniffing attacks on computer networks. In: 2017 International Conference on Intelligent Computing and Control (I2C2). IEEE, pp. 1–5. June.

Ashibani, Y., Mahmoud, Q.H., 2017. Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. 68, 81–97.

Baig, Z.A., Amoudi, A.R., 2013. An analysis of smart grid attacks and countermeasures. J. Commun. 8 (8), 473–479.

Baitha, A.K., Vinod, S., 2018. Session hijacking and prevention technique. Int. J. Eng. Technol. 7 (2.6), 193–198.

D. Balaban, September 2019. [Online]. Available: https://www.cyberdefensemagazine.com/?s=Ransomware+and+the+internet+of+things+%7C+cyber+defense+magazine. [Accessed 11 5 2022].

Bellare, M., Kohno, T., 2004. Hash function balance and its impact on birthday attacks. In: International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg. Springer, pp. 401–418. May.

Berger, K.M., Schneck, P.A., 2019. National and transnational security implications of asymmetric access to and use of biological data. Front. Bioeng. Biotechnol. 7, 21.

Bhuyan, M.H., Kashyap, H.J., Bhattacharyya, D.K., Kalita, J.K., 2014. Detecting distributed denial of service attacks: methods, tools and future directions. Comput. J. 537–556.

Boyd, S.W., Keromytis, A.D., 2004. SQLrand: preventing SQL injection attacks. In: International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg. Springer, pp. 292–302. June.

Braun, L., Didebulidze, A., Kammenhuber, N., Carle, G., 2010. Comparing and improving current packet capturing solutions based on commodity hardware. In: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pp. 206–217. November.

Bruce, N.I., Murthi, B.P.S., Rao, R.C., 2017. A dynamic model for digital advertising: the effects of creative format, message content, and targeting on engagement. J. Mark. Res. 54 (2), 202–218.

Carl, G., Kesidis, G., Brooks, R.R., Rai, S., 2006. Denial-of-service attack-detection techniques. IEEE Internet Comput. 10 (1), 82–89.

Carreón, N.A., Sonderer, C., Rao, A., Lysecky, R., 2021. A medical vulnerability scoring system incorporating health and data sensitivity metrics. Int. J. Comput. Inf. Eng. 15 (8), 458–466.

Caswell, J., Gans, J.D., Generous, N., Hudson, C.M., Merkley, E., Johnson, C., Xie, G, 2019. Defending our public biological databases as a global critical infrastructure. Front. Bioeng. Biotechnol. 7, 58.

Chen, Y., Zheng, W., Li, W., Huang, Y., 2021a. Large group activity security risk assessment and risk early warning based on random forest algorithm. Pattern Recognit. Lett. 144, 1–5.

Chen, X., Liu, Z., Yang, Y., Lv, X., Li, D., Li, X., 2021b. Predicting algorithm of DNA recombination site based on machine learning. In: 2021 17th International Conference on Computational Intelligence and Security (CIS). IEEE, pp. 65–69. November.

Cho, J.S., Yeo, S.S., Kim, S.K., 2011. Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value. Comput. Commun. 34 (3), 391–397.

Coleman, D.D., Westcott, D.A., 2012. Cwna: Certified Wireless Network Administrator Official Study guide: Exam Pw0-105. John Wiley & Sons.

Cooke, E., Jahanian, F., McPherson, D., 2005. The zombie roundup: understanding, detecting, and disrupting botnets. SRUTI 5, 6-6.

B. Dickson, "Blog," 22 August 2016. [Online]. Available: https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/. [Accessed 20 5 2022].

Diggans, J., Leproust, E., 2019. Next steps for access to safe, secure DNA synthesis. Front. Bioeng. Biotechnol. 7, 86.

Dixon, T.A., Williams, T.C., Pretorius, I.S., 2021. Sensing the future of bio-informational engineering. Nat. Commun. 12 (1), 1–12.

Duncan, S.E., Reinhard, R., Williams, R.C., Ramsey, F., Thomason, W., Lee, K., Murch, R., 2019. Cyberbiosecurity: a new perspective on protecting US food and agricultural system. Front. Bioeng. Biotechnol. 7, 63.

Edwards, S., Profetis, I., 2016. Hajime: analysis of a decentralized internet worm for IoT devices. Rapidity Networks 16, 1–18.

El-Hajj, W., Aloul, F., Trabelsi, Z., Zaki, N., 2008. On detecting port scanning using fuzzy based intrusion detection system. In: 2008 International Wireless Communications and Mobile Computing Conference. IEEE, pp. 105–110. August.

Elgabry, M., 2023. Biocrime, the Internet-of-Ingestible-Things and Cyber-Biosecurity. Cyber Biosecurity. Springer, pp. 135–146.

Falliere, N., Murchu, L.O., Chien, E., 2011. W32. stuxnet dossier. White Paper, Symantec Corp., Security Response 5 (6), 29.

Farbiash, D., & Puzis, "Cyberbiosecurity: DNA injection attack in synthetic biology.," *arXiv preprint arXiv:2011.14224.*, p. 14224, 2020.

Fatima, N., Liu, L., Hong, S., Ahmed, H., 2020. Prediction of breast cancer, comparative review of machine learning techniques, and their analysis. IEEE Access. 8, 150360–150376.

Ferrag, M.A., Shu, L., Yang, X., Derhab, A., Maglaras, L., 2020. Security and privacy for green IoT-based agriculture: review, blockchain solutions, and challenges. IEEE Access 8, 32031–32053.

Fujibayashi, D., Sakaguchi, H., Ardakani, I., Okuno, 2021. Nonlinear registration as an effective preprocessing technique for Deep learning based classification of disease. In: 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC). IEEE, pp. 3245–3250. November.

George, A.M., 2019. The national security implications of cyberbiosecurity. Front. Bioeng. Biotechnol. 7, 51.

Giaretta, A., Balasubramaniam, S., Conti, M., 2015. Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks. IEEE Trans. Inf. Forensics Secur. 11 (4), 665–676.

Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G., 2006. Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A 73 (2), 022320.

Greenbaum, D., 2023. Cyberbiosecurity: A New Field to Deal with Emerging Threats. Springer Nature.

Grigorieva, Natalie M., Petrenko, Sergei A., 2023. Biological Metaphor for Cyber Immunity. IEEE.

Grover, K., Lim, A., Yang, Q., 2014. Jamming and anti-jamming techniques in wireless networks: a survey. Int. J. Ad Hoc Ubiquitous Comput. 17 (4), 197–215.

L. Grunwald, "New attacks against RFID-systems.," *GmbH Germany,* 2006.

Gu, J., Lu, S., 2021. An effective intrusion detection approach using SVM with naïve Bayes feature embedding. Comput. Secur. 103, 102158.

Guo, C., Rana, M., Cisse, M., & Van Der Maaten, L., "Countering adversarial images using input transformations," *arXiv preprint arXiv:1711.00117,* 2017.

Guttieres, D., Stewart, S., Wolfrum, J., Springs, 2019. Cyberbiosecurity in advanced manufacturing models. Front. Bioeng. Biotechnol. 7, 210.

Halevi, T., Memon, N., Nov, O., 2015. Spear-phishing in the wild: a real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. In: Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015).

Handa, A., Sharma, A., Shukla, S.K., 2019. Machine learning in cybersecurity: a review. Wiley Interdiscipl. Rev.: Data Mining Knowl. Discov. 9 (4), e1306.

Hao, W.T., Lu, Y., Dong, R.H., Shui, Y.L., Zhang, Q.Y., 2022. Adaptive intrusion detection model based on CNN and C5. 0 classifier. Int. J. Network Secur. 24 (4), 648–660.

He, D., Chan, S., Guizani, M., 2017. Drone-assisted public safety networks: the security aspect. IEEE Commun. Mag. 55 (8), 218–223.

Heartfield, R., Loukas, G., 2015. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Comput. Surv. (CSUR) 48 (3), 1–39.

Heys, H.M., 2002. A tutorial on linear and differential cryptanalysis. Cryptologia 26 (3), 189–221.

Hu, J., Ngo, D.C.L., Teoh, A.B.J., 2015. Biometric Security. Cambridge Scholars Publishing.

Ignaczak, L., Goldschmidt, G., Costa, C.A.D., Righi, R.D.R., 2021. Text mining in cybersecurity: a systematic literature review. ACM Comput. Surv. (CSUR) 54 (7), 1–36.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., Pu, C., 2011. Reverse social engineering attacks in online social networks. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, pp. 55–74. July.

Islam, M.S., Ivanov, S., Doolin, K., Coffey, L., Dooley-Cullinane, T.M., Berry, D., Balasubramaniam, S., 2019. Trojan bio-hacking of DNA-sequencing pipeline. In: Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, pp. 1–7. September.

Islam, M.S., Ivanov, S., Awan, H., Drohan, J., Balasubramaniam, S., Coffey, L., Srisaan, W., 2022. Using deep learning to detect digitally encoded DNA trigger for Trojan malware in Bio-Cyber attacks. Sci. Rep. 12 (1), 1–13.

Jain, A.K., Ross, A., Prabhakar, S., 2004. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 14 (1), 4–20.

Jain, V., Sahu, D.R., Tomar, D.S., 2015. Session hijacking: threat analysis and countermeasures. In: Int. Conf. on Futuristic Trends in Computational Analysis and Knowledge Management. February.

Jamal, T., Haider, Z., Butt, S.A., & Chohan, "Denial of service attack in cooperative networks," *arXiv preprint arXiv:1810.11070,* 2018.

Jose, A.C., Malekian, R., Ye, N., 2016. Improving home automation security; integrating device fingerprinting into smart home. IEEE Access 4, 5776–5787.

Joshi, M., & Hadi, T.H., "A review of network traffic analysis and prediction techniques," *arXiv preprint arXiv:1507.05722,* 2015.

Jothi, Neesha, Rashid, Abdul, 2015. Data Mining in Healthcare – A Review. Procedia Comput. Sci 72, 306–313.

Juuti, M., Szyller, S., Marchal, S., Asokan, N., 2019. PRADA: protecting against DNN model stealing attacks. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 512–527. June.

Kambourakis, G., Kolias, C., Stavrou, A., 2017. The mirai botnet and the iot zombie armies. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, pp. 267–272. October.

Kantarcioglu, M., Xi, B., 2016. Adversarial data mining: big data meets cyber security. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1866–1867. October.

Kaur, J., Ramkumar, K.R., 2021. The recent trends in cyber security: a review. J. King Saud Univ.

Kausar, F., Aljumah, S., Alzaydi, S., Alroba, R., 2019. Traffic analysis attack for identifying users' online activities. IT Prof 21 (2), 50–57.

Kavakiotis, I., Tsave, O., Salifoglou, A., Maglaveras, N., Vlahavas, I., Chouvarda, I., 2017. Machine learning and data mining methods in diabetes research. Comput. Struct. Biotechnol. J. 15, 104–116.

Khan, F., Ncube, C., Ramasamy, L.K., Kadry, S., Nam, Y., 2020. A digital DNA sequencing engine for ransomware detection using machine learning. IEEE Access 8, 119710–119719.
Kolias, C., Kambourakis, G., Stavrou, A., Voas, 2017. DDoS in the IoT: mirai and other botnets. Computer (Long Beach Calif) 50 (7), 80–84.
Koyun, A., Al Janabi, E., 2017. Social engineering attacks. J. Multidiscipl. Eng. Sci. Technol. (JMEST) 4 (6), 7533–7538.
Kronberg, D.A., 2014. A simple coherent attack and practical security of differential phase shift quantum cryptography. Laser Phys. 24 (2), 025202.
Kumar, P., Lee, S.G., Lee, H.J., 2012. E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors 12 (2), 1625–1647.
J. Kurdan,"watermark risk management," [Online]. Available: https://wrmi-llc.com/behavioral-aspects-of-biosecurity/#:~:text=Threat%20actors%20impacting%20biosecurity%20risk,diversion%2C%20misuse%20or%20intentional%20release.
Kuswanto, D., Anjad, M.R., 2021. Application of improved random forest method and C4. 5 algorithm as classifier to ransomware detection based on the frequency appearance of API calls. In: IEEE 7th Information Technology International Sem.
Lütkenhaus, N., Jahma, M., 2002. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New J. Phys. 4 (1), 44.
Latino, M.E., Menegoli, 2020. Biosafety and biosecurity in containment: a regulatory overview. Front. Bioeng. Biotechnol. 8, 650.
Latino, M.E., Menegoli, 2022. Cybersecurity in the food and beverage industry: a reference framework. Comput. Ind. 141 (103702).
Lee, Y., Kozar, K.A., 2005. Investigating factors affecting the adoption of anti-spyware systems. Commun. ACM 48 (8), 72–77.
Lee, C., Hong, D., Lee, S., Lee, S., Yang, H., Lim, J., 2002. A chosen plaintext linear attack on block cipher CIKS-1. In: International Conference on Information and Communications Security. Berlin, Heidelberg. Springer, pp. 456–468. December.
T. Lee, T., Edwards, B., Molloy, I., Su, D., 2019. Defending against neural network model stealing attacks using deceptive perturbations. In: 2019 IEEE Security and Privacy Workshops (SPW), pp. 43–49. May.
LeMoyne, R., Mastroianni, T., 2020. Network centric therapy for machine learning classification of hemiplegic gait through conformal wearable and wireless inertial sensors. In: 2020 International Conference on e-Health and Bioengineering (EHB). IEEE, pp. 1–4.
Lerman, L., Bontempi, G., Markowitch, O., 2011. Side channel attack: an approach based on machine learning. Center for Advanced Security Research Darmstadt, p. 29.
Leung, M.K., Delong, A., Alipanahi, B., Frey, B.J., 2015. Machine learning in genomic medicine: a review of computational problems and data sets. Proc. IEEE 104 (1), 176–197.
Liang, B., Su, M., You, W., Shi, W., Yang, G., 2016. Cracking classifiers for evasion: a case study on the google's phishing pages filter. In: Proceedings of the 25th International Conference on World Wide Web, pp. 345–356.
Lin, J., Yang, C.W., Tsai, C.W., Hwang, T., 2013. Intercept-resend attacks on semi-quantum secret sharing and the improvements. Int. J. Theor. Phys. 52 (1), 156–162.
Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., Nazir, S., 1407. An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs. Sensors 22 (4), 2022.
Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. (TISSEC) 14 (1), 1–33.
Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., Leung, V.C., 2018. A survey on security threats and defensive techniques of machine learning: a data driven view. IEEE access 6, 12103–12117.
Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., Lin, Z., 2021. When machine learning meets privacy: a survey and outlook. ACM Comput. Surv. (CSUR) 54 (2), 1–36.
Lobo, D., Watters, P., Wu, X.W., Sun, L., 2010. Windows rootkits: attacks and countermeasures. In: 2010 Second Cybercrime and Trustworthy Computing Workshop. IEEE, pp. 69–78. July.
Lou, X., Tran, C., Tan, R., Yau, D.K., Kalbarczyk, Z.T., Banerjee, A.K., Ganesh, P., 2019. Assessing and mitigating impact of time delay attack: case studies for power grid controls. IEEE J. Sel. Areas Commun. 38 (1), 141–155.
Lv, B., Chai, G., Sheng, X., Ding, H., Zhu, X., 2021. Evaluating user and machine learning in short-and long-term pattern recognition-based myoelectric control. IEEE Trans. Neural Syst. Rehabil. Eng. 29, 777–785.
Madaan, V., Goyal, 2020. Predicting ayurveda-based constituent balancing in human body using machine learning methods. IEEE Access 8, 65060–65070.
Mahmud, M., Kaiser, M.S., McGinnity, T.M., Hussain, A., 2021. Deep learning in mining biological data. Cognit. Comput. 13 (1), 1–33.
Majumder, A.J.A., Veilleux, C.B., 2021. Smart health and cybersecurity in the era of artificial intelligence. Computer-Mediated Communication. IntechOpen.
Malik, A.M., Miguez, R.A., Li, X., Ho, Y.S., Feldman, E.L., Barmada, 2018. Matrin 3-dependent neurotoxicity is modified by nucleic acid binding and nucleocytoplasmic localization. eLife 7, e35977.
Mantle, J.L., Rammohan, J., Romantseva, E.F., Welch, J.T., Kauffman, L.R., McCarthy, J., Lee, K.H, 2019. Cyberbiosecurity for biopharmaceutical products. Front. Bioeng. Biotechnol. 7, 116.
McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., Chen, H., 2017. Assessing medical device vulnerabilities on the internet of things. In: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, pp. 176–178. July.
Millett, K., Dos Santos, E., Millett, P.D., 2019. Cyber-biosecurity risk perceptions in the biotech sector. Front. Bioeng. Biotechnol. 7, 136.
Moorman, A., Samaniego, C.C., Maley, C., Weiss, R., 2019. A dynamical biomolecular neural network. In: 2019 IEEE 58th Conference on Decision and Control (CDC). IEEE, pp. 1797–1802.
Mueller, S., 2019. On DNA signatures, their dual-use potential for GMO counterfeiting, and a cyber-based security solution. Front. Bioeng. Biotechnol. 7, 189.
Mueller, 2021. Facing the 2020 pandemic: what does cyberbiosecurity want us to know to safeguard the future? Biosafety Health 3 (01), 11–21.
Murch, R., Di Euliis, 2019. Mapping the cyberbiosecurity enterprise. Front. Bioeng. Biotechnol. 7, 235.
Murch, R.S., So, W.K., Buchholz, W.G., Raman, S., Peccoud, J., 2018. Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Front. Bioeng. Biotechnol. 39.
Murugan Bhagavathi, S., Thavasimuthu, A., Murugesan, A., George Rajendran, C.P.L., Raja, L., Thavasimuthu, R, 2021. Weather forecasting and prediction using hybrid C5. 0 machine learning algorithm. Int. J. Commun. Syst. 34 (10), e4805.
Nam, J., Paik, J., Kang, H.K., Kim, U.M., Won, D., 2009. An off-line dictionary attack on a simple three-party key exchange protocol. IEEE Commun. Lett. 13 (3), 205–207.
Narayanan, A., Shmatikov, V., 2005. Fast dictionary attacks on passwords using time-space tradeoff. In: Proceedings of the 12th ACM conference on Computer and communications security, pp. 364–372. November.
Naser, M., Mohamed, M.N., & Shehata, L.H., "Artificial intelligence in assisted reproductive technology.," 2021.
Nespoli, P., Mármol, F.G., Vidal, J.M, 2021. A bio-inspired reaction against cyberattacks: AIS-powered optimal countermeasures selection. IEEE Access 9, 60971–60996.
Ney, P., Koscher, K., Organick, L., Ceze, L., Kohno, T., 2017. Computer security, privacy, and {DNA} sequencing: compromising computers with synthesized {DNA}, privacy leaks, and more. In: 26th USENIX Security Symposium (USENIX Security 17), pp. 765–779.
P.M. Ney, " Securing the future of biotechnology," *A study of emerging bio-cyber security threats to DNA-information systems (Doctoral dissertation),* 2019.
Noman, H.A., Abdullah, S.M., Mohammed, H.I., 2015. An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks. Int. J. Comput. Sci. Issues (IJCSI) 12 (4), 107.
E. Pauwels, "The New Geopolitics of Converging Risks," 2019.
Pirandola, S., Braunstein, S.L., Lloyd, S., 2008. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. Phys. Rev. Lett. 101 (20), 200504.
Pries, R., Yu, W., Fu, X., Zhao, W, 2008. A new replay attack against anonymous communication networks. In: 2008 IEEE International Conference on Communications. IEEE, pp. 1578–1582. May.
Proano, A., Lazos, L., 2010. Selective jamming attacks in wireless networks. In: 2010 IEEE International Conference on Communications. IEEE, pp. 1–6. May.
Puzis, R., Veksler-Lublinsky, I., 2023. Applying CVSS to vulnerability scoring in cyber-biological systems. Cyberbiosecurity 115–134.
Puzis, R., Farbiash, D., Brodt, O., Elovici, Y., Greenbaum, D., 2020. Increased cyber-biosecurity for DNA synthesis. Nat. Biotechnol. 38 (12), 1379–1381.
Qi, B., Fung, C.H.F., Lo, H.K., & Ma, X., "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/0512080,* 2005.
Rahman, M.A., Mohsenian-Rad, H., 2012. False data injection attacks with incomplete information against smart power grids. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 3153–3158. December.
Rashed-Al-Mahfuz, M., Haque, A., Azad, A., Alyami, S.A., Quinn, J.M., Moni, M.A., 2021. Clinically applicable machine learning approaches to identify attributes of Chronic Kidney Disease (CKD) for use in low-cost diagnostic screening. IEEE J. Transl. Eng. Health Med. 9, 1–11.
Reed, J.C., Dunaway, N., 2019. Cyberbiosecurity implications for the laboratory of the future. Front. Bioeng. Biotechnol. 7, 182.
Richardson, L.C., Connell, N.D., Lewis, S.M., Pauwels, E., Murch, R.S., 2019a. Cyberbiosecurity: a call for cooperation in a new threat landscape. Front. Bioeng. Biotechnol. 7, 99.
Richardson, L.C., Lewis, S.M., Burnette, R.N, 2019b. Building capacity for cyberbiosecurity training. Front. Bioeng. Biotechnol. 7, 112, 2019.
Salem, M.B., & Stolfo, S.J., "Masquerade attack detection using a search-behavior modeling approach," *Columbia University, Computer Science Department, Technical Report CUCS-027-09*, 2009.
Sanicola, H.W., Stewart, C.E., Mueller, M., Ahmadi, F., Wang, D., Powell, S.K., Brafman, D.A., 2020. Guidelines for establishing a 3-D printing biofabrication laboratory. Biotechnol. Adv. 45, 107652.
Schabacker, D.S., Levy, L.A., Evans, N.J., Fowler, J.M., Dickey, E., 2019. Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. Front. Bioeng. Biotechnol. 7, 61.
P. Schaumont, "Fault Attacks on Embedded Software: threats, Design, and Mitigation," 2018.
Schmale III, D.G., Ault, A.P., Saad, W., Scott, D.T., Westrick, J.A., 2019. Perspectives on harmful algal blooms (HABs) and the cyberbiosecurity of freshwater systems. Front. Bioeng. Biotechnol. 7, 128.
Shah, Y.C., Schmidt, A., Choyi, V.K., Subramanian, L., & Leicher, A., U.S. Patent Application No. 14/786,688, 2016.
Smmarwar Smmarwar, S.K., Gupta, G.P., Kumar, S., 2022. Research trends for malware and intrusion detection on network systems: a topic modelling approach. Adv. Malware Data-Driven Network Security 19–40, 2022.
Snigdha, Farjana, et al., 2020. Obstructive sleep apnea (OSA) events classification by effective radar cross section (ERCS) method using microwave Doppler radar and machine learning classifier. In: IEEE MTT-S International Microwave Biomedical Conference (IMBioC). IEEE.
Son, J., Kim, D., Hussain, R., Tokuta, A., Kwon, S.S., Seo, J.T., 2015. Privacy aware incentive mechanism to collect mobile data while preventing duplication. In: MILCOM 2015-2015 IEEE Military Communications ConferenceIEEE, pp. 1242–1247. October.

Sontowski, S., Gupta, M., Chukkapalli, S.S.L., Abdelsalam, M., Mittal, S., Joshi, A., Sandhu, R, 2020. Cyber attacks on smart farming infrastructure. In: 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), pp. 135–143. December.
Sood, A.K., Zeadally, S., 2016. Drive-by download attacks: a comparative study. IT Prof. 18 (5), 18–25.
Spiekermann, S., 2015. Ethical IT innovation: A value-Based System Design Approach. CRC Press.
Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Vigna, G., 2009. Your botnet is my botnet: analysis of a botnet takeover. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 635–647. November.
Sulaiman, M.A., 2012. Doctoral Dissertation. King Fahd University of Petroleum and Minerals, Saudi Arabia.
Szychlinska, M.A., D'Amora, U., Ravalli, S., Ambrosio, L., Di Rosa, M., Musumeci, G., 2019. Functional biomolecule delivery systems and bioengineering in cartilage regeneration. Curr. Pharm. Biotechnol. 20 (1), 32–46.
Tahir, R., Hu, H., Gu, D., McDonald-Maier, K., Howells, G., 2013. Resilience against brute force and rainbow table attacks using strong ICMetrics session key pairs. In: 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA). IEEE, pp. 1–6. February.
Tamaki, K., Koashi, M., Imoto, N., 2003. Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. Phys. Rev. A 67 (3), 032310.
Tandon, A., Nayyar, A., 2019. A comprehensive survey on ransomware attack: a growing havoc cyberthreat. Data Manag., Anal. Innov. 403–420.
Tasevski, P., 2011. Password Attacks and Generation Strategies. Tartu University: Faculty of Mathematics and Computer Sciences.
Tawalbeh, M., Quwaider, M., Lo'ai, A.T., 2021. IoT cloud enabeled model for safe and smart agriculture environment. In: 2021 12th International Conference on Information and Communication Systems (ICICS). IEEE, pp. 279–284.
Tempola, F., Muhammad, M., Maswara, A.K., Rosihan, R., 2022. Rule formation application based on C4. 5 algorithm for household electricity usage prediction. Trends Sci. 19 (3), 2167-2167.
Ten, C.W., Manimaran, G., Liu, C.C., 2010. Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans. Syst., Man, Cybernetics-Part A: Syst. Humans 40 (4), 853–865.
Teo, L., 2000. Port scans and ping sweeps explained. Linux J. *2000.80es: 2-es*.
Tong, L., Li, B., Hajaj, C., Xiao, C., Zhang, N., Vorobeychik, Y., 2019. Improving robustness of {ML} classifiers against realizable evasion attacks using conserved features. In: 28th USENIX Security Symposium (USENIX Security 19), pp. 285–302.
Vadlamani, S., Eksioglu, B., Medal, H., Nandi, A., 2016. Jamming attacks on wireless networks: a taxonomic survey. Int. J. Prod. Econ. 172, 76–94.
Vangala, A., Das, A.K., Kumar, N., Alazab, M., 2020. Smart secure sensing for IoT-based agriculture: blockchain perspective. IEEE Sens. J. 21 (16), 17591–17607.
Varga, P., Plosz, S., Soos, G., Hegedus, C., 2017. Security threats and issues in automation IoT. In: 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). IEEE, pp. 1–6.
Vinatzer, B.A., Heath, L.S., Almohri, H.M., Stulberg, M.J., Lowe, C., Li, S., 2019. Cyberbiosecurity challenges of pathogen genome databases. Front. Bioeng. Biotechnol. 7, 106.
Vivaldi, N., Caiola, M., Solarana, K., Ye, M., 2021. Evaluating performance of eeg data-driven machine learning for traumatic brain injury classification. IEEE Trans. Biomed. Eng. 68 (11), 3205–3216.
Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., Vigna, G., 2007. Cross site scripting prevention with dynamic data tainting and static analysis. In: NDSS, 2007, p. 12. February.
Walsh, P.F., 2022. Securing the bioeconomy: exploring the role of cyberbiosecurity. The Handbook of Security Palgrave Macmillan, Cham, pp. 335–355.
Wang, Huiyong, Zhang, Minglu, Wang, Jingyang, 2010. Design andimplementation of an emergency search and rescue system based onmobile robot and wsn. In: Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on, volume 1. IEEE, pp. 206–209.
Wang, H., Liu, X., Xiao, Y., Xu, M., Xing, E.P., 2017. Multiplex confounding factor correction for genomic association mapping with squared sparse linear mixed model. In: 2017 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). IEEE, pp. 194–201. November.
Wex, P., Breuer, J., Held, A., Leinmuller, T., Delgrossi, L., 2008. Trust issues for vehicular ad hoc networks. In: VTC Spring 2008-IEEE Vehicular Technology Conference.IEEE, pp. 2800–2804. May.
Wong, K., Wong, A., Yeung, A., Fan, W., Tang, S., 2014. Trust and privacy exploitation in online social networks. IT Prof 16 (5), 28–33.
Wu, WT., Li, YJ., Feng, AZ, 2021. Data mining in clinical big data: the frequently used databases, steps, and methodological models. Military Med. Res. 8 (44).
Wunsch, D.C., Hier, D.B., 2021. Subsumption reduces dataset dimensionality without decreasing performance of a machine learning classifier. In: 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC). IEEE, pp. 1618–1621. November.
Xie, Y., Sekar, V., Maltz, D.A., Reiter, M.K., Zhang, H., 2005. Worm origin identification using random moonwalks. In: 2005 IEEE Symposium on Security and Privacy (S&P'05). IEEE, pp. 242–256. May.
Xiong, L., Yao, Y., 2021. Study on an adaptive thermal comfort model with K-nearest-neighbors (KNN) algorithm. Build. Environ. 202, 108026.
Xue, M., Yuan, C., Wu, H., Zhang, Y., Liu, W., 2020. Machine learning security: threats, countermeasures, and evaluations. IEEE Access 8, 74720–74742.
Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020a. Cyber-physical systems security: limitations, issues and future trends. Microprocess. Microsyst. 77, 103201.
Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R., Chehab, A., 2020b. Securing internet of medical things systems: limitations, issues and recommendations. Future Generat. Comput. Syst. 105, 581–606.
Yadav, S., Bohra, B., 2015. A review on recent phishing attacks in Internet. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, pp. 1312–1315. October.
Yang, C.W., Hwang, T., Lin, T.H., 2013. Modification attack on QSDC with authentication and the improvement. Int. J. Theor. Phys. 52 (7), 2230–2234.
Yang, X., Zhang, Z., Yang, R., Huang, D., Yang, G., Gong, L., 2017. Using deep learning to recognize biomedical entities. In: 2017 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE). IEEE, pp. 1–4.
Yang, X.S., He, X., Yang, S., 2020. Nature-Inspired Computation in Data Mining and Machine Learning. Springer.
Yaqoob, I., Ahmed, E., ur Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M., Guizani, M., 2017. The rise of ransomware and emerging security challenges in the internet of things. Computer Networks 129, 444–458.
Maria Yatsenko, "Using data mining techniques in cybersecurity solutions," 2022. [Online]. Available: https://www.apriorit.com/dev-blog/527-data-mining-cyber-security. [Accessed 31 July 2022].
Yeh, S.J., Chen, B.S., 2021. Systems medicine design based on systems biology approaches and deep neural network for gastric cancer. IEEE/ACM Trans. Comput. Biol. Bioinf.
Yuan, Z.L., Dynes, J.F., Shields, A.J., 2010. Avoiding the blinding attack in QKD. Nat. Photonics 4 (12), 800–801.
B. Yuce, "Fault attacks on embedded software: new directions in modeling, design, and mitigation (Doctoral dissertation, Virginia Tech)," 2018.
Zahra, S.R., Chishti, M.A., 2019. Ransomware and internet of things: a new security nightmare. In: 2019 9th international conference on cloud computing, data science & engineering (confluence). IEEE, pp. 551–555. January.
Zhang, L., Yu, S., Wu, D., Watters, P, 2011. A survey on latest botnet attack and defense. In: 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, pp. 53–60. November.
Zhou, J., Lu, Q., Xu, R., Gui, L., Wang, H., 2018. EL_LSTM: prediction of DNA-binding residue from protein sequence by combining long short-term memory and ensemble learning. IEEE/ACM Trans. Comput. Biol. Bioinf. 17 (1), 124.

Dr. Deepa D. Shankar's research is in the field of Cybersecurity with the specialization in the domain of Steganalysis

Ms Adresya Suresh Azhakath's research is in the field of Bio Informatics and Systems Biology

Ms Nesma Khalil's research is based on Cybersecurity and statistical Steganalysis

Dr Sajeev has a vast experience in Bio Informatics.

Dr Mahalakshmi's research domain is in the field of Bio Informatics.

Dr Sheeba's experience is based on the research in the field of Bio Technology.