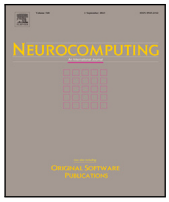
Neurocomputing 581 (2024) 127427

Contents lists available at ScienceDirect

Neurocomputing

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



Survey Paper

The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research

Bruno Ramos-Cruz [a,*], Javier Andreu-Perez [a,b], Luis Martínez [a]

[a] Computer Science Department, University of Jaen, Jaen, 23071, Spain
[b] Centre for Computational Intelligence, School of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom

ARTICLE INFO

Communicated by N. Zeng

Keywords:
Cybersecurity mesh
Federated learning
Blockchain technology
Swarming intelligence
Cryptographic protocols

ABSTRACT

In today's world, it is vital to have strong cybersecurity measures in place. To combat the ever-evolving threats, adopting advanced models like cybersecurity mesh is necessary to enhance our protection. Cybersecurity mesh is an architecture scalable, flexible, composable, robust and resilient and allows the interoperability and coordination between intelligent systems to provide security services. Designing a cybersecurity mesh faces three major challenges: scalability, distributed or federated systems, and technology integration. For the design, it is necessary to apply security tools that support scalability because millions and millions of data are stored, processed, and analysed. Federated systems are needed to improve interoperability in a decentralized cybersecurity mesh. However, it can be tough to integrate different security tools and communication protocols. Cryptographic algorithms and AI models like federated learning, swarming intelligence and blockchain technologies are useful for security services. It is essential to study the integration of existing methods to determine the best technology for the job. We conduct a comprehensive analysis of intelligent systems, including federated learning, blockchain technology, and swarming intelligence, with a particular focus on how they have been and can be used to enhance cybersecurity. We examine the latest trends in these technologies, explore their connections, and weigh the pros and cons of each approach. To conduct this review, we utilized the Web of Science and Scopus databases and followed the PRISMA guidelines.

1. Introduction

Currently, the number of electronic devices connected to the Internet increases day by day; according to the annual report of Cisco for this year 2023, 29.3 billion connected devices are expected [1]. From a business point of view, this represents an increase in the global economy. However, from a security point of view, it represents multiple security challenges [2].

Within the global context of international security, espionage, and privacy, cybersecurity has become a significant concern for the community. Cybersecurity is a key area to safeguard our data from attacks and communicate securely between different devices on a network. In [3], the author defines cybersecurity as the ability of information systems to resist any action compromising the security services of processed data or the related services offered by those systems. Recently, the most important security services are confidentiality, authenticity, integrity, non-repudiation, and availability.

Nowadays, most cyberattacks use sophisticated malicious software that is installed on the user's electronic device by using messages, email, text, or call. It only needs the user to interact with any of these items, for instance, clicking on them to open an IP connection where the malicious infection script is located, which subsequently exploits vulnerabilities of the target operating system (OS) to embed the malicious software (malware) into the terminal and run in the background stealth mode for not being detected. Still, even more compromising are new advanced attacks called "zero-click", in which the users' installation does not even need to interact with the malware, becoming pertinaciously invisible and even more challenging to track their sources.

In addressing these kinds of challenges, the community employs different security models. The most widely used approach is centralized control technologies, where the devices, applications, users, and data exist within the security perimeter of the network. In this model, users are only authenticated when they enter the network; once inside, they can violate security services with minimal effort. Furthermore, devices

* Corresponding author.
E-mail address: brcruz@ujaen.es (B. Ramos-Cruz).

https://doi.org/10.1016/j.neucom.2024.127427
Received 8 August 2023; Received in revised form 17 January 2024; Accepted 17 February 2024
Available online 21 February 2024

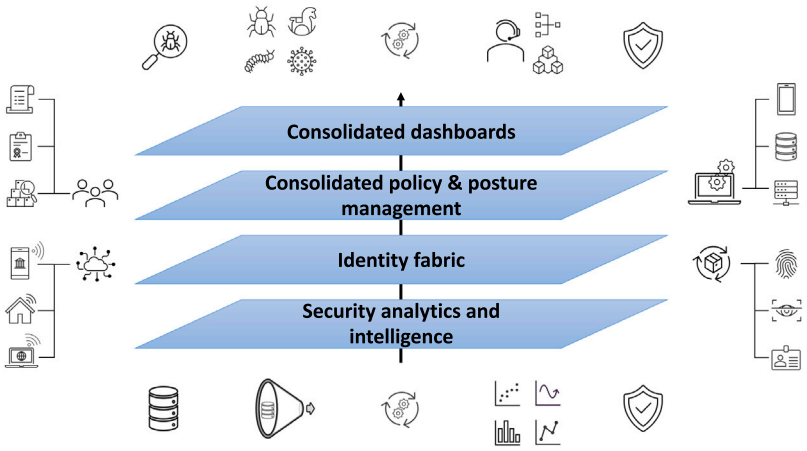


Fig. 1. The figure displays the cybersecurity mesh layers, for instance, the layer of security analytics and intelligence collects, the identity fabric layer, and the layer of centralized policy and posture management. Finally, the dashboard layer is depicted.

operate independently of one another. Consequently, each device represents a single point of failure, increasing complexity and reaction time.

Currently, the approach to cybersecurity is changing, and new paradigms are emerging. For example, the zero trust model is a new trend and implies that all users and devices inside or outside the network are authenticated, authorized, and validated before they have access to data and applications. When working on this model, it is assumed that the network is unreliable and has no traditional network perimeter. That means, in this model, it is possible to work with security tools anywhere; the network can be local, in the cloud, or hybrid.

Recently, a popular cybersecurity concept is the *mesh* because it focuses on making connections between different devices, applications, and users, among others, in order to work collaboratively and thus obtain a better performance in network security technologies. Given the relationship that exists between the concept of cybersecurity and mesh, a new paradigm called cybersecurity mesh emerges.

In [4], cybersecurity mesh is defined as an architecture that integrates disparate security tools to work as a cooperative ecosystem. This architecture provides an approach to security-based characteristics such as scalability and interoperability to improve security services. Unlike previous security systems such as SIEM (Security Information and Event Management), cybersecurity mesh involves different security layers [4]; for instance, the layer of security analytics and intelligence collects, stores, and analyzes large-scale data in real-time in a central location to improve risk analysis and reaction times to threats. The identity fabric layer allows access from anywhere and also manages and performs identity tests. The layer of centralized policy and posture management identifies regulatory compliance risks and incorrect configuration problems. Finally, the dashboard layer is used to detect security events more efficiently and implement the right responses. The layers are summarized in Fig. 1. With the integration of these concepts, cybersecurity mesh is a new paradigm that has gained popularity nowadays.

Nevertheless, considering that the primary goal of this approach is the integration of various security tools into one, the entity that manages these systems itself would be a single point of failure. This brings us to speak of a centralized cybersecurity mesh, returning to the issue of centralization. Another alternative is to create a Decentralized Cybersecurity Mesh. The approach of this new paradigm is to develop a fully decentralized network of security tools. A first effort that falls in this area is the Naoris Protocol, which is a decentralized cybersecurity mesh to protect the users and devices on the network using Blockchain technology and swarm intelligence.

Designing a decentralized cybersecurity mesh faces three major challenges: scalability, distributed or federated systems, and technology integration. For the design, it is necessary to apply security tools that support scalability because millions and millions of data are stored, processed, and analysed. However, most of the tools that exist in the literature do not have a scalability property [5,6]. Therefore, the community is working to develop new scalable security tools [7,8]. Federated systems play an important role in designing decentralized cybersecurity mesh because they allow for better interoperability. Achieving the correct fusion of security tools and orchestrating different communication protocols to work together and improve security services is difficult because it is necessary to consider efficiency and security as design lines.

Usually, to provide security services and create new security systems, the community uses cryptographic algorithms such as hash functions, cryptographic primitives, and signature chains, among others. All these algorithms are well-defined and have a strong security level because they were designed specifically to provide security services and have been tested under rigorous security standards. However, recently, artificial intelligence models such as federated learning, swarming intelligence, and blockchain technologies have been used to provide security services and are gaining popularity despite the fact that they were not created to provide security services. Thus, studying the different tools in the literature is quite important to have a referent and choose the best technology.

In this work, we show and describe the traditional cryptographic algorithms. Moreover, this survey aims to study the different types of security tools that, in some way or another, contribute to the construction of a decentralized cybersecurity mesh architecture. We focus on federated learning, blockchain technologies, and swarming intelligence.

Subsequent to this introduction, the document is organized as follows: Section 2 presents an overview of the most popular security tools, such as cybersecurity mesh, cryptography, and probabilistic data structures. Section 3 discusses the survey methodology. Section 4 shows the results of federated learning for the cybersecurity mesh. Section 5 depicts the outcomes of blockchain technologies for the cybersecurity mesh. Section 6 illustrates the results related to swarming intelligence for the cybersecurity mesh. Section 7 gives important discussions focusing on the advantages and disadvantages of each research area. Section 8 displays the trends, future direction, and open challenges based on this research. Finally, Section 9 concludes this article. For the convenience of the readers, the nomenclature is given at the end of the paper.

2. Overview of security tools

In this review, to avoid ambiguity, the concept of cybersecurity tools is defined as a set of software applications or programs designed to protect the security of computer systems and digital data against cyber threats and attacks. These tools are crucial to resist any action compromising the security services. This section revises concepts about security tools such as cybersecurity mesh, cryptographic data structure, probabilistic data structures, and detection and prevention systems for cybersecurity.

2.1. Cybersecurity mesh

Cybersecurity Mesh is a paramount and emerging concept in the field of cybersecurity that aims to transform traditional centralized approaches into a more dynamic, distributed, and flexible security model [9]. In a conventional approach, organizations typically rely on a centralized security perimeter to protect their data or assets. However, this approach can be limited by invalid static network boundaries in an interconnected environment.

Cybersecurity mesh addresses these limitations by protecting individual assets or data, regardless of location or network boundary. At its core, Cybersecurity mesh promotes the idea of a decentralized security architecture where security controls are embedded directly into the assets themselves, creating a self-protecting ecosystem. This emphasizes a zero-trust model, where each asset is considered untrusted by default, and access is granted based on continuous authentication, authorization, and risk assessment [10].

By implementing cybersecurity mesh, organizations can achieve several benefits. Firstly, it enables a more granular and fine-grained security approach, allowing organizations to protect their critical assets individually rather than relying solely on network perimeters. Secondly, it supports a more dynamic and adaptable security posture, where security controls can be applied and adjusted based on real-time threat intelligence and risk assessments.

Another advantage of cybersecurity mesh is its ability to enable secure collaboration and information sharing across diverse environments and platforms. It facilitates secure communication and data exchange between assets, regardless of location or ownership, while maintaining high protection. To implement cybersecurity mesh, organizations utilize various technologies such as software-defined perimeters, microsegmentation, strong encryption, multi-factor authentication, and continuous monitoring [4]. These technologies work together to establish a robust security structure that covers different environments, including local infrastructure and cloud services.

Cybersecurity mesh represents a paradigm change in the approach to cybersecurity. It moves from a centralized network model to a security model with a decentralized approach. Moreover, it provides organizations with greater flexibility, adaptability, and resilience to face cyber attacks because it embeds security controls directly into assets and promotes the zero-trust model.

The cybersecurity mesh relies and is closely on the mesh topology concept, which is used to create a resilient and flexible framework against cyber attacks. In network architecture, the mesh topology is a set of nodes interconnected with each other to share information, resources, and/or offer different services. The design of this topology has the purpose of guaranteeing a more significant number of possible communications regardless of the existence of downed nodes. This is because nodes in this mesh network have multiple connections to each other, allowing alternatives to be found in case the communication path fails. The capability of a mesh topology to create and modify routes dynamically increases the reliability of the connections. Mesh topology may be classified into three categories: star, partial, and full mesh. Fig. 2 shows the diagram for these categories, respectively.

As shown in Fig. 2(a), the star topology has a central node that orchestrates the communication between the different nodes. In this topology, direct communication between nodes is not allowed. The central node is the only entity that manages the sending and receiving of information. Since the central node is the one that receives all the requests and responds to each of the nodes in the network, it can lead to network overload, with the central node being a bottleneck for service requests. Furthermore, from a security perspective, it constitutes a single point of failure.

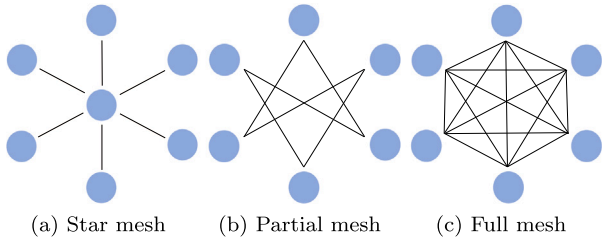


Fig. 2. The figure shows the most popular kind of mesh topology in the network architecture.

Fig. 2(b) shows the representation of a partial topology where a node can be connected to one or two nodes, a node can be connected to multiple nodes, but not all nodes are connected to each other. Unlike the star topology, the partial topology allows direct communication between the different nodes of the network. However, it may be the case that when trying to communicate one node with another, it is necessary to carry out the communication process through other nodes. This is because this type of topology presents less redundancy than the complete topology, which is defined below.

In the full mesh topology shown in Fig. 2(c), each node in the network is connected to the other, creating connections between all nodes in the network. In this topology, there is a higher degree of redundancy than in any other. Redundancy is an important feature because it allows you to find an alternative path for communication in case any node fails.

One of the problems in the mesh topology is how to design an optimal communication topology. There are some results of optimization to find the best communication route between the different nodes. For instance, in [11], the author explores a scenario where the traditional communication with the orchestrator is replaced by direct peer-to-peer communications between individual nodes named silos. The impact of the communication topology on the training duration is examined, considering two contrasting effects. Firstly, a more connected topology results in faster convergence regarding iterations or communication rounds. However, secondly, a more connected topology also increases the duration of each communication round. The primary goal of this paper is to explore the effect of topology on the duration of communication rounds. To achieve this, the author employs the linear systems theory in the max-plus algebra to design cross-silo federated learning topologies, minimizing the duration of communication rounds or, well, maximizing the number of completed rounds per time unit.

2.2. Cryptographic data structures

According to [12], to achieve information security in an electronic society where significant amounts of data are stored in electronic devices and transmitted through the Internet are necessary technical and legal skills. Cryptography provides the technical means through mathematical techniques related to aspects of information security such as:

1. *Confidentiality* helps protect the information or system from unauthorized entities.
2. *Integrity* focuses on knowing if the data or system has been modified.

Fig. 3. This taxonomy classifies attacks according to security services. The most common attacks used to violate these services are display. Man in the Middle attack (MitM), Denial of Service attack (DoS), Root to Local attack (R2L), User to Root attack (U2R), Probe (Probing attacks), and Structure Query Language Injection attack (SQL injection).

3. *Authentication* allows identification and exists two types: entity authentication and data origin authentication.
4. *Non-repudiation* prevents any entity from denying previous commitments or actions.
5. *Availability* ensures timely and reliable access to information and systems to an authorized entity [13].

Fig. 3 shows a taxonomy of the most relevant and intelligent cyber-attacks that have been deployed by adversaries to violate some security services discussed above. In this taxonomy, the attacks are grouped according to security services.

Computing relies on data structures to manage vast resources efficiently. Cryptographic data structures, a recent development, leverage cryptographic primitives to offer enhanced security features. One of the primary advantages of cryptographic structures is their ability to enable authenticated and protected query processing (AQP). This means that a user can safely interact with an encrypted database or registry by extracting, deleting, and modifying data. However, specific algorithms are necessary to preserve privacy to manipulate these encrypted databases without decryption, using measures like signatures or certificates to prevent theft. Some commonly used data structures include signature chains, trees, bitmaps, and skip lists.

A signature chain is an asymmetric cryptographic algorithm that provides authentication, integrity, and no repudiation and was introduced by [14]. Let $A = \{a_1, a_2, \ldots, a_n\}$ be a set of elements. The signature chain corresponding to set A is computed as follows:

$$Sign_n(h(h(a_1) \parallel h(a_2) \parallel \cdots \parallel h(a_n)))$$

where $Sugn_a$ is the signature and h is a hash function. Signature chains are commonly used in systems such as blockchain, where they are crucial to ensure the security and immutability of the ledger. Besides, can also be used for other purposes, for instance, verifying the identity of participants in a communication network.

Regarding tree data structure, there are many kinds of trees, such as Merkle hash tree, MB-tree, Red tree, and Black tree, which are used mainly to verify service integrity efficiently. For instance, the Merkle hash tree is a binary hash tree as depicted in Fig. 4. The basic idea is to create a hierarchical structure of hash values, where each node in the tree represents the hash of its children using the concatenate operator. The leaf nodes of the tree contain the data that needs to be verified, and the internal nodes and root nodes hold the cryptographic hash values, with the difference that only the root node is signed. These types of trees are very useful in the databases as a service model to provide databases security [6,15].

A bitmap index is another data structure used to provide integrity service, usually in database applications, to answer queries effectively that provide an enormous amount of data [16]. The author in [17] defines a bitmap index as a bit string to describe if the value of an attribute at any relation (table) R_{mn} is related to a specific value or not. This relationship is given through the following encoding: $\{=, <, \leq, >, \geq\}$. The encoding determines the bits that are set to 1. For instance, let a_j be an attribute of relation R_{mn} and v_{lj} its value. The bitmap in equality encoding is

$$Bitmap_{R_{mn}}(a_j, v_{lj}) = X_l$$

where X_l is computed according to the following equation:

$$bit_k\left(X_l\right) = \begin{cases} 1 & if\, R_{mn}\left(t_k, a_j\right) = v_{lj} \\ 0 & otherwise \end{cases}$$

with $\mid X_l \mid = m$ and for $1 \leq k \leq m$. Since the bitmaps are bit strings, logic operations such as the union, intersection, complement, and negation are easy to compute.

2.3. Probabilistic data structures

There are probabilistic data structures, such as filters, that are used to represent any set of items and allow membership tests with false positive rates. The research literature presents two popular approaches, Bloom and Cuckoo filters.

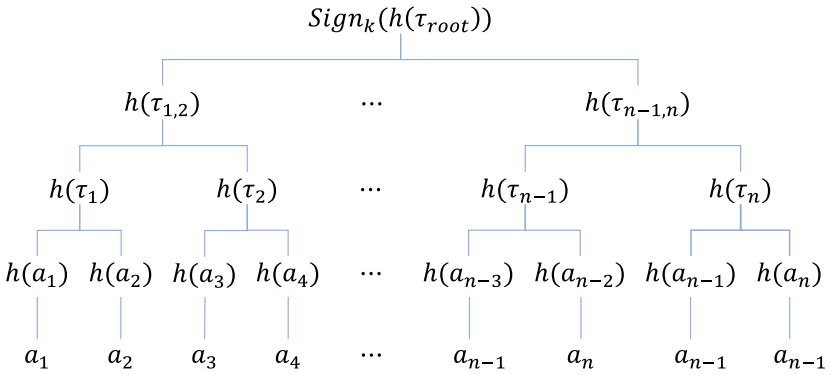


Fig. 4. Figure depicted Merkle hash tree, where $Sign_k$ is the signature applying the key k, h is hash function, $\tau_{root} = h(h(\tau_{1,2}) \parallel h(\tau_{n-1,n}))$, $\tau_{1,2} = h(h(\tau_1) \parallel h(\tau_2))$, $\tau_{n-1,n} = h(h(\tau_{n-1}) \parallel h(\tau_n))$, $\tau_1 = h(h(a_1) \parallel h(a_2))$, $\tau_2 = h(h(a_3) \parallel h(a_4))$, $\tau_{n-1} = h(h(a_{n-3}) \parallel h(a_{n-2}))$, and finally $\tau_n = h(h(a_{n-1}) \parallel h(a_n))$.

While Bloom-based filters [18] have been considered the traditional method for implementing these checking approaches, Cuckoo-based filters have gained popularity in recent years due to reported lower false positive rates, membership test in constant time and the capacity of offering deletion operators [5]. However, cuckoo-based filters have several drawbacks, such as a slow insertion process and lower tolerance to insertions.

These filters can be built across hash functions used in data management [19] as well as cryptographic hash functions. The cryptographic hash functions provide security elements and satisfy certain properties (collision-free, strongly collision-free, one way) in order to prevent various forgeries [12]. Consequently, the probability of a cryptographic hash function collision is very small compared to non-cryptographic hash functions. If the probability of collisions decreases, then the false positives rate also decreases. Thus, the community is investigating the pros and cons of the technical aspects of each filter method.

Nowadays, there are many different application areas, such as secure digital communications [20,21], where probabilistic data structures called filters have played a crucial role. The filters are a common approach to reducing cost and improving the performance of set membership tests. There are works such as [22], which have explored the viability of applying membership tests in Network Security Monitoring (NSM) applying cuckoo filters to enhance space efficiency.

For example, in [23], it designs a real-time anomaly malware detection scheme, utilizing collaborative Virtual Machine (VM) communities as a system call monitoring where anomalous sequences. They use cuckoo filters in each community to reduce the streaming and capture normal behaviour. If any sequence does not pass the membership test, then it is considered an anomalous sequence. Then, all anomalous sequences are inserted in a new cuckoo filter called anomaly filter with the intention of generating a vaccine that protects from attacks. Other works, such as [24], proposed a scope query searchable encryption scheme based on the cuckoo filter and blockchain to preserve privacy.

In addition to filters, there are other approaches in the literature, such as [25], where the author detects and classifies malware network traffic using a data flow network. Machine learning has been used to provide security services, in [8] it proposes a learned Bloom filter to detect malicious IP connection activity, combining machine learning models and Bloom filters. Another example is [26], which presents a set of applications and opportunities where the cuckoo search filter can be applied, which is a bioinspired metaheuristic algorithm that can be used in areas such as cryptanalysis and cyber–physical system [27].

This section previously discussed two filters. However, recent literature introduces a variety of filters, such as the Counting Bloom Filter [28], Bloom Filter Trie [29], and Sliding Bloom Filter [30], among others. These filters find applications in numerous fields, including cybersecurity.

2.4. Detection and prevention systems for cybersecurity

System detection for cybersecurity involves various techniques and tools used to identify potential threats, vulnerabilities, or malicious activities within a computer system. The goal is to minimize cyberattack's impact by detecting and responding promptly to security incidents [31]. The following paragraphs show an overview of the Intrusion Detection System (IDS) and Intrusión Prevention System (IPS).

An intrusion detection system is a passive supervision method that detects threats, analyses network traffic, and compares it against known patterns to generate alerts. IDS does not provide real protection to the network or endpoint because it only monitors network traffic or system activity for suspicious patterns that may indicate unauthorized access, malware infections, or other security breaches [32]. In this approach, there are different systems, such as anomaly detection, malware detection, and attack detection.

Unlike IDS, which merely alerts upon detecting suspicious activities, an intrusion prevention system immediately follows the rules set to prevent unauthorized access, attacks, and malicious behaviour [33]. IPS can actively block or mitigate suspicious traffic, thus preventing potential security breaches and minimizing the impact of cyberattacks.

IDS and IPS are based on artificial intelligence techniques such as machine learning, deep learning, statistical models, and neural networks. These kinds of systems involve two more techniques because no single technique is sufficient to ensure complete system security. An effective cybersecurity strategy involves a combination of detection techniques, along with prevention measures and incident response capabilities.

3. Survey methodology

The current systematic literature review is based on the guidelines set by Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [34]. It is a widely recognized and adopted guideline for conducting systematic reviews in the field of academic research. The main objective is to ensure transparency and completeness in reporting research findings, thereby promoting the quality and reliability of systematic reviews. To do so, this methodology provides a series of steps, including formulating research questions, establishing inclusion criteria, devising a search strategy, conducting study selection, data extraction methods, and analysis results, which are summarized in the flow diagram of Fig. 5.

This study analysed articles focusing on intelligent systems, such as federated learning, blockchain technologies, and swarming intelligence, within the context of cybersecurity mesh. The primary objective is to highlight the application of these three technologies in the field of cybersecurity. The research questions illustrated in Table 1 were formulated to achieve this.

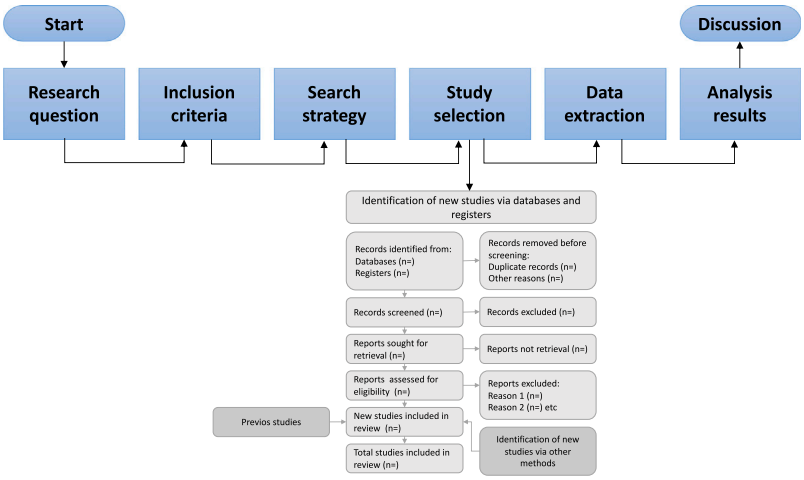


Fig. 5. This figure summarizes the PRISMA methodology.

Table 1
Table depicts the research queries proposed to perform the study and analysis of articles focusing on federated learning, blockchain technology, and swarming intelligence in the field of cybersecurity.

Notation	Research questions
RQ1	What are the application areas where federated learning, blockchain technology, and swarming intelligence are applied as security tools?
RQ2	What algorithms are used to provide security services?
RQ3	What kind of security violations or attacks resolve the proposed algorithms in RQ2?

We conducted a literature search on the Web of Science and Scopus databases. Our search was conducted from 2018 to 2022, mainly because cybersecurity mesh is a concept that was popularized by Gartner in 2020 [4]. To ensure the relevance of our analysis, the articles published before 2018 were excluded. The search did not have specific restrictions based on country or region. In this way, capturing the variety and diversity of articles was possible. Initially, we used keywords such as "Federated learning cybersecurity mesh", "Federated Blockchain Cybersecurity mesh", and "Swarming intelligence cybersecurity mesh". However, the search generated a limited number of articles or no results. As a result, we changed the keywords to "Federated learning cybersecurity", "Federated Blockchain Cybersecurity", and "Swarming intelligence cybersecurity".

The search was classified into three case studies. The initial case study (CS1) was oriented to map the existing literature concerning federated learning and cybersecurity in the Web of Science and Scopus resources. The second case study (CS2) was focused on blockchain technologies, and the third case study (CS3) was related to swarming intelligence. The search process is illustrated in the diagram in Fig. 6 and was developed as follows:

1. In the first step, the articles in WoS and Scopus were identified.
2. Next, in the second step, duplicate articles that surfaced during the search were removed, avoiding redundancy.
3. In the third step, the recovered articles that did not relate to the concept of federated learning were excluded.
4. Finally, aspects of cybersecurity were considered, and articles that did not provide insights into security services were omitted from the final selection.

The data extracted from the selected studies included key information such as author(s), publication year, the specific application area, algorithms employed, and details pertaining to security services or attacks.

For each case study, CS1, CS2, and CS3, the research question were analysed. The outcomes of these case studies were presented using tables, cloud graphs, and plots. The tables were used to depict all the works that were studied. The results of the research question R1 were shown with the help of a clustered column plot together with a cloud graph. For research question R2, the results were depicted through a pie plot. Finally, the results of research question R3 were illustrated with a sunburst plot. The findings from this comprehensive search will be presented in Section 4 and will cover results related to federated learning, where 153 articles were found, of which 83 were selected. Section 5 will focus on blockchain technology, in this case of study, 136 articles were found which 60 were selected. Section 6 will show the information related to swarming intelligence; in this scenario, 48 articles were found, of which 29 were selected. In total, 337 articles were identified, and 165 articles were analysed.

4. Federated learning for the cybersecurity mesh

Federated learning is a new artificial intelligence model with the main characteristics of decentralized and private data. This new approach to machine learning has drawn a lot of attention in different areas, such as cybersecurity, where this model is mainly used to provide confidentiality service.

This model works under the premise that sensitive data should not be sent to an external entity because this entity could obtain benefits of any kind. To avoid this type of problem, federated learning allows learning models to be trained locally in an iterative process between a global model and the different local models. The first selects the pre-training parameters to send to the local models. These participants train the model using their local data and obtain new parameters, which are then sent back to the global model. The global model updates and initiates a new iteration upon receiving these parameters. This iterative process leads to the continuous improvement of the global model. In the following sentences and based on [35], the steps of federated learning are summarized:

1. Selection of model. The global statistical model W and the set of k node users are selected by the central server. It pre-trains the model W with initial parameters and sends it to the node clients.
2. Training locally. Each node client k updates the local model w_k with the individual data.
3. Aggregating the local model. After completing the training of the local model, the updated parameters are sent go back to the central server. It collects all the updating parameters and then updates the global model. After that, the central server sends the new parameters to the local users to initiate a new iteration. This process is stopped when the loss function converges.

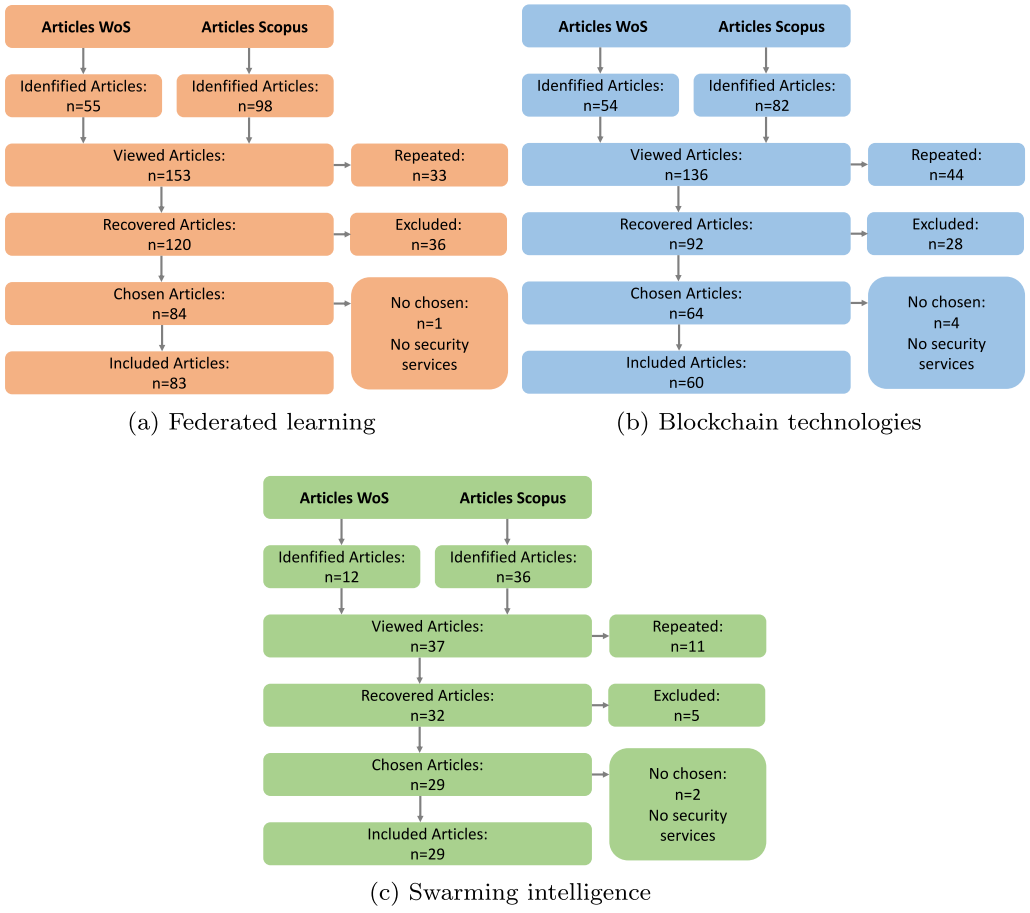


Fig. 6. Figures (a), (b), and (c) display the process that was carried out to filter the articles recovered from the Web of Science and Scopus resources. The repeated category involves duplicated articles; within the excluded category are articles not recovered and articles unrelated to the federated concept. Finally, if the articles did not match cybersecurity, it was not chosen.

Furthermore, according to [36], the formulation of the federated learning model can be expressed as follows:

$$f(w) = \sum_{K}^{k=1} \frac{n_k}{n} F_k(w) \quad \text{where} \quad F_k(w) = \frac{1}{n_k} \sum_{i \in P_k} f_i(w) \tag{1}$$

where

$F_k(w)$ is local objective function,
$f_i(w)$ represent a prediction loss function,
K is the set of node clients that participate in the current round,
n defines the sample's total number,
n_k is the samples number that has each k th participant locally,
P_k is the partitioned assigned to the k th participant from the whole data set P.

The federated learning model presents some challenges and considerations. For instance, managing the heterogeneity of devices, ensuring the integrity and authenticity of model updates, addressing communication and synchronization issues, and handling potential adversarial behaviour within the federated learning process in Section 7 will be discussed in detail. Despite these challenges, the community carefully assesses these factors and implements appropriate security measures to utilize federated learning in different areas effectively. The next section shows the most common application areas where federated learning is used as a new paradigm to provide security services.

4.1. Application areas where federated learning provides security services

Federated learning has recently gained popularity in the field of machine learning, offering a new opportunity for collaborative model training across various application areas. This decentralized approach enables organizations to harness the collective intelligence of their data sources without compromising sensitive information. This particular characteristic represents advancements in multiple domains. Federated learning can potentially revolutionize areas such as healthcare, the financial sector, telecommunications, and more. This section shows the application areas where federated learning is used to provide security services.

The outcomes of this research are reported through Tables 2–4. These tables have five columns; the first column presents the author's name, followed by the publication year. The third column displays the areas where federated learning is used. The fourth column has the main algorithms, schemes, or models that are used to design detection systems, attack prevention, or provide security services. The final column illustrates threats and security services.

There exist different works that take advantage of the properties of federated learning to design models, schemes, and architectures, among others, with the objective of protecting and providing security services in different areas. Addressing the research question RQ1, the areas where federated learning is applied as a security tool to provide security services were identified. These areas are grouped into 8 categories: Internet of Things (IoT), General Security (GS), Secure Communication (SC), Smart Environments (SE), Cyber–Physical Systems (CPS), Healthcare, Self Sovereign Identity (SSI), and Recommendation Systems (RS). These categories were shown in the graph of Fig. 7. In this graph, the X-axis represents the category's name, and the Y-axis is the publication number.

Notice that the IoT category is bigger than other areas. This is possible because, recently, the number of devices connected to the

Table 2
The table displays the works related to federated learning and cybersecurity. The first column shows the author's name and the publication year. The third column contains the application areas. The fourth column depicts the algorithms, and the last column illustrates the security services, attacks, or system detection.

Author	Year	Area	Tools	Security services
Ghimire and Rawat [36]	2022	IoT	ML, AFL	Confidentiality
de Oliveira Silva [37]	2022	CPS	FL	Confidentiality
Alazab et al. [35]	2022	Multi	FL, AFL	C&A
Singh et al. [38]	2022	Smart grid	SCP, Blockchain	Confidentiality
Chowdhury et al. [39]	2022	Healthcare	DL, FL	Confidentiality
Singh and Saxena [40]	2022	SC	ML, VC, ECC	C&A
Gosselin et al. [41]	2022	Multi	FL	Backdoor, GAN
Kwon et al. [42]	2022	SC	FHC	Anomaly detection
Ferrag et al. [43]	2022	IoT, IIoT	ML	Intrusion detection
Vaiyapuri et al. [44]	2022	IoT	FLIDS-BSAFSC,	Intrusion detection
Popoola et al. [45]	2022	IoT-ED	DL, FDL	Zero-day botnet
Li et al. [46]	2022	IoT, Fog/Edge	FLEAM	DDoS
Driss et al. [47]	2022	VSN	GRU, RF	Anomaly detection
Campos et al. [48]	2022	IoT	FL, Multiclass	Anomaly detection
Chen [49]	2022	Smart home	RCNN	C&A
Ravi et al. [50]	2022	IoMT, CPS	MDL, ELF	Malware detection
Naseri et al. [51]	2022	FL	CERBERUS, FL, CRNN	Intrusion prevention
Yazdinejad et al. [52]	2022	IIoT	Block Hunter, Blockchain, FML	Anomaly detection
Abdel-Basset et al. [53]	2022	IIoT, IEoT	BoEI, Fed-Trust, TCGN	Confidentiality
Tahir and Tariq [54]	2022	SSC	mf-FDIA,	Anomaly detection
Sarhan et al. [55]	2022	IoT	Fl, Blockchain, smart contract	Intrusion detection
Moayyed et al. [56]	2022	Smart grid	Fl, CNN	Confidentiality
Qammar et al. [57]	2022	FL	FL-models	CAIN
Liu et al. [58]	2022	AI	PMLM, Federated forest	Confidentiality
Guo et al. [59]	2022	CPS	DFL	Confidentiality
Aurisch [60]	2022	Military Networks	FL-MA	Anomaly detection
Madala et al. [61]	2022	CPS	FL	Intrusion detection
Kumar et al. [62]	2022	Healthcare	FL, AI, Blockchain	C&A
Anastasakis et al. [63]	2022	IoT	FL, DP	Intrusion detection
Thi et al. [64]	2022	SDN	ML, DL	Attack detection
Ridhawi et al. [65]	2022	Industry 4.0 (IoT,SPC)	FL, Blockchain	C&A
Anwer et al. [66]	2022	IoT	FL	Zero day attack detection
Chen et al. [67]	2022	CNID	FL	Intrusion detection
Moustafa et al. [68]	2022	IoT-SN	FL, DDL-RNN, DFSat	Intrusion detection
Huang et al. [69]	2022	CPS	FL, EEFED	Intrusion detection
Datta et al. [70]	2022	IoT	FL, IDAM	Anomaly detection
Aliyu et al. [71]	2022	IoV	BFF, Blockchain	Intrusion detection

internet has increased, and most electronic devices are connected to send and receive information. In this review, the IoT category appears with 35 publications, which include works focused on Industrial Internet of Things (IIoT) [43,52,95,106], Internet of Medical Things (IoMT) [38,50], Internet of Vehicles [71], Edge of things [45,53,92], Fog computing [46], IoT in satellite and mobile networks [68,82].

The General Security category has 16 articles, all of which focus on the correct performance and improvement of the federated learning model [72,89,93], for example, in [96] propose Asynchronous FL using Temporal Weighted Averaging (TWA), and in [57], the author test different models to train the data in a decentralized manner. In [117], it proposed a jamming defence strategy based on adaptive federated reinforcement learning focused on Flying Ad-Hoc Networks (FANETs) consisting of Unmanned Air Vehicle (UAV) nodes. In [51], a novel Intrusion Detection System (IDS) named CERBERUS is presented. This system is based on the collaborative recurrent neural network (CRNN). In [85] design IDS using Random Forest (RF), [113] combined RF with blockchain technology, even just blockchain [116]. Other as [114] use Long Short-Term Memory (LSTM) to provide confidentiality, and [94] use FL to develop secure query language in databases.

The Secure Communication category has 15 articles, of which 4 focus on secure communication in a general way [38,42,73,111]. The rest are divided into work that includes Local Area Networks (LANs) that are shown in [110,112], military networks [60], Software Defined Networking (SDN) [64], Campus Network Intrusion Detection (CNID) [49], Vehicular Ah-Hoc Networks (VANETs) [83], Vehicular Sensor Network (VSN) [47], Electric Vehicle Charging Ecosystems (EVCEs) [75] and Connected and Automated Vehicles (CAVS) [90].

Another interesting category is Smart Environment, which involves 9 publications. One of them is focused on smart cities [111]. Other areas include in this category are Smart transport [58,83], smart grids [38,56,91], and smart home [101]. One more related to general smart environment [77].

CPS category involved [37,59,61,74] and CPS in industry 4.0 [65]. The healthcare category is essential, and usually, in this area, most of the time, the data are sensitive, and FL is a great approach to provide confidentiality [39,62,95,102], for instance, [102] propose an identity management framework using homomorphic encryption to provide confidentiality and authentication. SSI category is a new area that is essential in the process of distributed identity [73,99]. The last category is RS, where the author in [104] uses Federated Knowledge Distillation (FKD) to provide confidentiality. And [118] it proposes a federated fuzzy neural network (FedFNN) with the idea to handle data uncertainties and non-IID issues, applying evolutionary rule learning (ERL).

Table 3
The table displays the works related to federated learning and cybersecurity. The first column shows the author's name and the publication year. The third column contains the application areas. The fourth column depicts the algorithms, and the last column illustrates the security services, attacks, or system detection.

Author	Year	Area	Tools	Security services
J. Alyamani [72]	2022	FL	AI, ML	Anomaly detection
Bandara et al. [73]	2022	CTI	FL, Blockchain, SSI, CTI-P	Attack detection
De Benedictis et al. [74]	2022	CPS, DT	FL, Blockchain	Anomaly detection
Islam et al. [75]	2022	EVCS	FL, DP	Intrusion detection
Arisdakessian et al. [76]	2022	IoT	FL, GT, SP, AI	Intrusion detection
Fadi et al. [77]	2022	Smart environments	Blockchain, ML, DL, FL	Anomaly detection
Khoa et al. [78]	2022	IoT	DTL	Anomaly detection
Amit and Mohan [79]	2022	AIA	FL	Object detection
Sedjelmaci et al. [80]	2022	IoT-6G	MFL	Attack detection
He et al. [81]	2022	IoT-AUV	FL, BT, LSTM, CGAN	Intrusion detection
Pasdar et al. [82]	2022	IoT-MN	DNN	Malware detection
Moulahi et al. [83]	2022	ITS-VANET	FL, BT	Anomaly detection
Singh et al. [84]	2022	IoMT	HFL, HLSTM	Anomaly detection
Markovic et al. [85]	2022	FL	Fl, RF	Intrusion detection
Liu et al. [86]	2022	MTS	FL, CNN-MLP, FedBach	Intrusion detection
Lalouani and Younis [87]	2022	EoT	FL, Louvain	Intrusion detection
Sedjelmaci and Ansari [88]	2022	MEC	FedGAN	Attack detection
Ganjoo et al. [89]	2022	FL	FL	Poisoning attacks
Hussain et al. [90]	2022	CAVs	FL	C&A
Boudko. et al. [91]	2021	Smart grid	AFL	Anomaly detection
Zago et al. [92]	2021	IoT ED	DC, FL	DGA-based botnet
Mallah et al. [93]	2021	FL	FL	Monitoring detection
Liu et al. [94]	2021	FL	SQL-DB, ML,	C&A
Siniosoglou et al. [95]	2021	Healthcare, MCPS	GANs	Intrusion detection
Agrawal et al. [96]	2021	FL	AsynFL	Intrusion detection
Kumar et al. [97]	2021	5G-N	PHE, DF	Intrusion detection
Attota et al. [98]	2021	IoT	MV-FLID	Intrusion detection
Martín et al. [99]	2021	FIM	UEBA, ML	Anomaly detection
Al Mallah et al. [100]	2021	AVNs	MWN, RSU	C&A
Piasecki et al. [101]	2021	Smart home	EC	Confidentiality
Farid et al. [102]	2021	Healthcare	HE	C&A
Shukla et al. [103]	2021	IoT	FL, ML	Malware detection
Chen et al. [104]	2021	RS	FL, FKD	Confidentiality
Zhang et al. [105]	2021	IoT	FL, FedDetect (Adam-Cross-round)	Anomaly detection
Duy et al. [106]	2021	IIoT	FL, ML	Intrusion detection
Siniosoglou et al. [95]	2021	IIoT	FL, DL, FIH	Confidentiality
Shahid et al. [107]	2021	IoT	FL	Intrusion detection
Bandara et al. [108]	2021	SC	FL, BT	Integrity
Ferrag et al. [109]	2021	IoT	FL, FDL, RNN, CNN, DNN	CAINA
Sun et al. [110]	2021	LANs	Segmented-FL	Intrusion detection

Table 4
The table displays the works related to federated learning and cybersecurity. The first column shows the author's name, followed by the publication year. The third column contains the application areas. The fourth column depicts the algorithms, and the last column illustrates the security services, attacks, or system detection.

Author	Year	Area	Tools	Security services
Demertzis et al. [111]	2021	Smart cities	FL, BT	Confidentiality
Sun et al. [112]	2020	LANS	SFL	Intrusion detection
de Souza et al. [113]	2020	FL	DML, FL, RF, Blockchain	Confidentiality
Zhao et al. [114]	2020	FL	IID, FL-LSTM	Intrusion detection
Khoa et al. [115]	2020	IoT	Smart filters	Intrusion detection
Preuveneers et al. [116]	2018	FL	PBlockchain, FL	Anomaly detection

For a comprehensive overview of federated learning applications, Fig. 8 provides a visual summary of where federated learning has been used as a cybersecurity tool to provide security services.

4.2. Main algorithms used by federated learning to provide security services

For research question RQ2, Fig. 9 shows a summary of the algorithms and models presented in the fourth column of the Tables 2–4. The percentage was calculated considering 83 articles described in Fig. 6(a). This graph illustrates that FL is the most popular algorithm to provide security services with 28%, the works that employ FL are [37,41,49,61,66,79,89,90,93]. Blockchain technologies occupy the second places with the 17% of all articles. In [55,62,65,71,73,74,77,116] the author combined Fl with blockchain technologies. Other works, such as [52,113] mixed Federated Machine Learning (FML) with blockchain. In third place appears FML with 9%; this group involves different works such as [43,72,103,106], where are using FML as a flexible learning paradigm in secure communication networks. The neuronal network is an important tool for designing anomaly and intrusion detection systems. In this review, Deep Neuronal Networks (DNN) has the 8% with works as [39,45,64,82,95]. With 6% are RF and Recurrent Neuronal Networks (RNN). In [85] uses RF with FL, and in [47], the author applies RF with Gated Recurrent Units (GRU) to design an anomaly detection system. To RNN, there are different works as [51,68,109] where the author proposes new alternatives such as CERBERUS and DFSat for intrusion detection to provide confidentiality. LSTM [38,81] and Serverless Cloud Computing (SCC) both have 5%. Convolutional Neuronal Network (CNN) obtained the 4%, and there are works such as [49,56,58,109]. Finally, with 3% of the total show Adaptive Federated Learning (AFL) [35,36], Differential Privacy (DP) [63,75], Smart

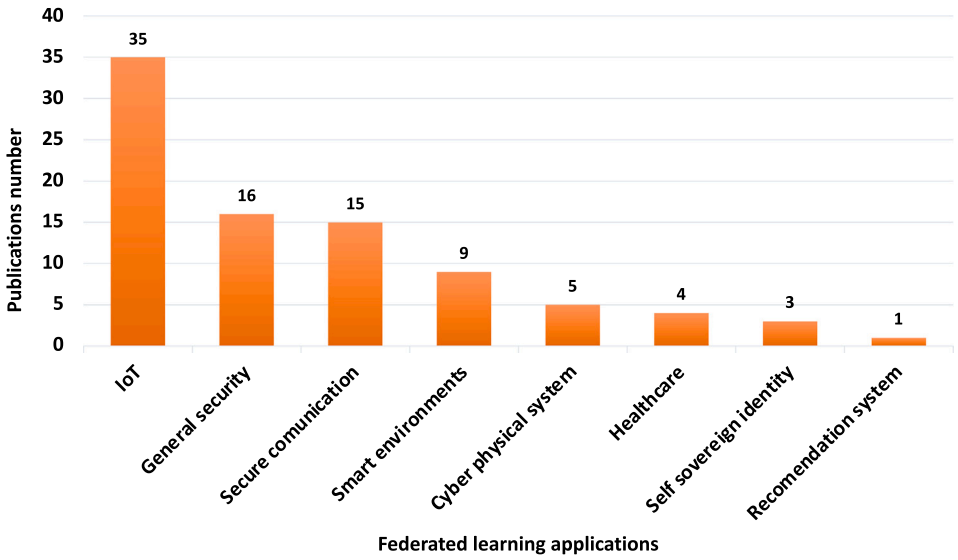


Fig. 7. Existing areas where federated learning is used to provide security services. The X-axis shows the name of the areas classified into 8 categories: Internet of Things (IoT), General Security (GS), Secure Communication (SC), Smart Environments (SE), Cyber–Physical Systems (CPS), Healthcare, Self Sovereign Identity (SSI), and Recommendation Systems (RS). The Y-axis presents the publication number obtained from the Web of Science and Scopus resources.

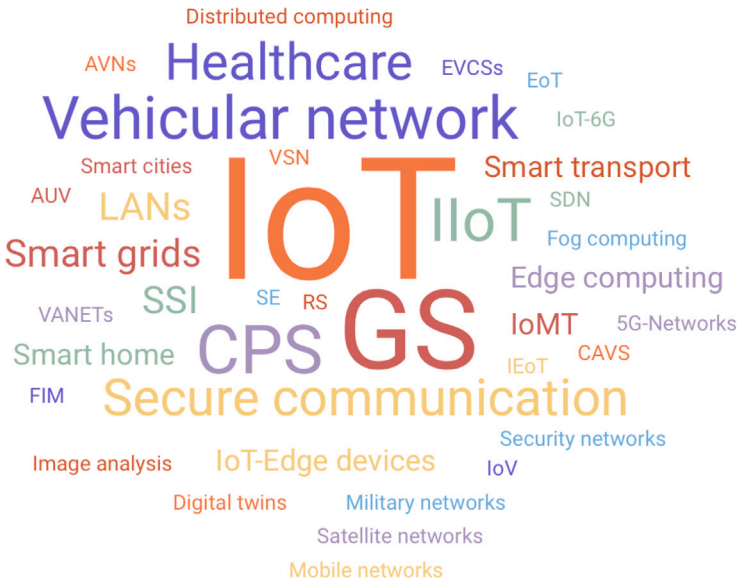


Fig. 8. This cloud graph depicts the most common areas where federated learning is applied to provide security services. There are many areas, such as the Internet of Things (IoT), General Security (GS), Cyber–Physical Systems (CPS), Industrial Internet of Things (IIoT), Internet of Medical Things (IoMT), Internet of Vehicles (IoV), Edge of Things (EoT), Smart Environments (SE), Vehicular networks like Electric Vehicle Charging Ecosystems (EVCEs), Vehicular Ad-hoc Networks (VANETs), Connected and Automated Vehicles (CAVs), Vehicular Sensor Networks (VSN), Unmanned Air Vehicles (UAVs). Federated Identity Management (FIM), Self Sovereign Identity (SSI), Recommendation System (RS), Software Defined Networking (SDN), and Local Area Networks (LANs).

Filters (SF) [115] and VC-ECC-FHC [38]. It is important to mention that there exist works that combine different algorithms; for example, [81] combine FL, BT, LSTM and Conditional Generative Adversarial Network (CGAN) to generate an IDS. Also, from the articles reviewed, eight articles are surveys. All the surveys are focused on federated learning. The main difference is that in some works such as [35,36,41,48,57,109] compare algorithms of Deep Learning (DL) and Machine Learning (ML), analyse the performance and chose the best option for the design of the federated learning model under the premise to improve it. The same idea is applied by [76], where the author combines blockchain with ML and DL. In [75], the author uses Game Theory (GT), Social Psychology (SP), ML, and DL to provide security tools in the IoT area.

4.3. Systems, attacks and services that solve federated learning

The federated learning algorithms are built with security as a design line. These algorithms aim to generate new security tools, such as detection systems and schemes resilient to attacks that provide security services. Research question RQ3 is related to these security tools; Fig. 10 presents the systems, attacks, and security services that are provided for the algorithms in research query RQ2. In graph 10, most of the articles design detection systems; for instance, intrusion detection occupied the first place with 31%, followed by anomaly detection with 18%. After, appear attacks detection with 5% and malware detection with 4%. In the end, object and monitoring detection is shown with 1%. Other publications supply security services. The graph shows confidentiality as a major security service with 17% after confidentiality and

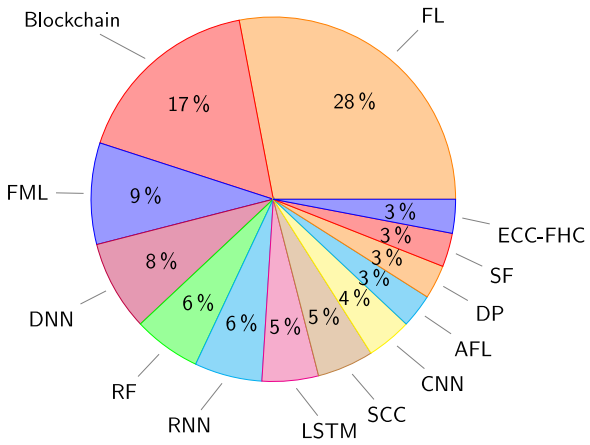


Fig. 9. This graph shows the algorithms, schemes, and models used to build the federated learning for cybersecurity mesh. The percentage was calculated considering 84 articles described in Fig. 6(a).

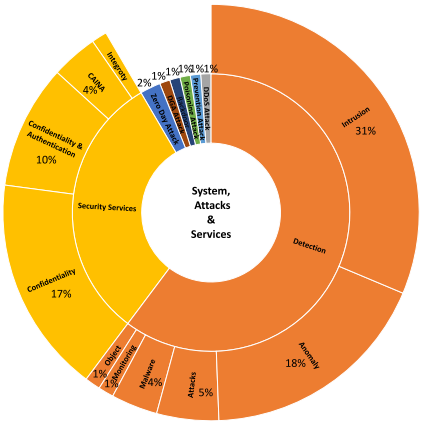


Fig. 10. This graph shows the systems and attacks found in the review to provide security services using the federated learning for cybersecurity mesh. Confidentiality, Authentication, Integrity, Non-repudiation, and Availability (CAINA). The percentage was calculated considering 83 articles described in Fig. 6(a).

authentication services represent 10%. Confidentiality Authentication Integrity No-repudiation and Availability (CAINA) denotes all security services and, in this review, has a 4%, whereas integrity service has a 1%. Some recovered articles focus on particular attack solutions such as zero-day attacks that represent 2%, DDoS, Backdoor, Domain Generation Algorithms (DGAs), and poisoning attacks at 1%. Finally, prevention attacks show the 1%. Unlike detection systems, prevention systems can take actions to reduce risks and even prevent them before they happen. Detection systems are only responsible for monitoring and reporting to another system. Nevertheless, by itself, a detection system does not provide security services.

Notice that most articles reviewed in the literature provide confidentiality services. This happens because the federated learning model is an area that is focused on resolving the privacy problem (confidentiality), and most of the algorithms are designed to identify anomalies and intrusion detection. To solve the authentication and integrity problem, cryptography algorithms are commonly used as a signature or cryptography and probabilistic data structure. In this review, just in [38], the author uses FL with Voting Classifier (VC), Elliptic Curve Cryptography (ECC), and Full Homomorphic Encryption (FHE).

In summary, federated learning has applications in various domains, including healthcare, finance, telecommunications, and edge computing, where privacy, data ownership, and network constraints are significant concerns. It enables the development of models that generalize well across distributed data sets while preserving data privacy and security.

5. Blockchain technology for the cybersecurity mesh

Blockchain can be seen as a decentralized database that records and stores transactions in objects named blocks across multiple computers or nodes in a network, designed to be transparent, secure, and immutable, among other properties. Each block has a time-stamped and is linked to the previous block through hash functions to build a blockchain, which is supported by a consensus mechanism where participating nodes verify the transactions block and may agree on the validation or not. If the block is validated, then it is added to the blockchain [119].

The distinctive aspect of blockchain technology lies in its decentralized structure. Traditional systems depend on central authorities like banks or governments to validate and record transactions. On the contrary, blockchain enables a peer-to-peer network of participants to verify and maintain the integrity of the ledger collectively. Through this decentralization and the application of cryptographic techniques, any transaction recorded on the blockchain becomes extremely difficult to modify or tamper with. As a result, blockchain has become an attractive solution for many applications in the financial sector, supply chains, and digital authentication, among others, where trust, transparency, and security are paramount.

Blockchain technology provides different categories, such as public blockchain, private blockchain, hybrid blockchain, and federated blockchain. In the following paragraphs, an overview is shown.

Public blockchains, known as permissionless blockchains, are open and permissionless networks where anyone can participate as a node, validate transactions, and contribute to the consensus process [120]. These blockchains are decentralized and do not rely on a central authority. Moreover, it offers transparency and security but can have scalability limitations due to the high computational requirements and consensus mechanisms.

Private blockchains are restricted networks where access and participation are controlled, also it is known as permissioned blockchains. In this kind of blockchain, only authorized participants can join the network, validate transactions, and generally maintain the blockchain's correct functioning [120]. Besides, they are typically used in organizations or specific groups where the participants want to hold more control over the network. Even more, it offers higher scalability and faster transactions than public blockchains; however, it sacrifices some decentralization and transparency [121].

A hybrid blockchain combines the features of public and private blockchains where specific parts of the blockchain are open to the public, while other sections are restricted and accessible only to authorized participants [122]. This design allows for increased privacy and control over sensitive information, making it suitable for applications where a balance between transparency and confidentiality is necessary.

Federated blockchains are a hybrid approach like hybrid blockchain that combines elements of both public and private blockchains, also known as consortium blockchains. In a consortium blockchain, multiple organizations or entities form a consortium and jointly collaborate to maintain and validate the blockchain network [123]. The consensus process and network maintenance are shared among the consortium members, who are typically known and trusted entities. Consortium blockchains offer a balance between decentralization and control, which are more suitable for industries where collaboration among multiple parties is required. The key distinction lies in the level of decentralization and control, unlike hybrid blockchains which maintain a mix of public

and private features, potentially using different consensus mechanisms for each part, federated blockchains are essentially private blockchains controlled by a consortium of trusted participants using a consensus mechanism.

Blockchain technology offers paramount benefits such as decentralization, immutability, and transparency. Despite this, It should be emphasized that its adoption in cybersecurity is still evolving. When some entities wish to do blockchain implementations, they need to consider aspects such as scalability, performance, and privacy challenges, as these factors may impact its practicality in certain scenarios. Additionally, integrating blockchain into existing cybersecurity architectures requires careful planning, interoperability considerations, and collaboration with the industry to establish standardized frameworks and protocols.

5.1. Application areas where blockchain technology provides security services

Blockchain technologies are a trending topic in cybersecurity because they apply advanced cryptographic algorithms such as hash functions, HMAC, Merkle hash tree, and Homomorphic encryption algorithms, among others. The most important characteristic of these kinds of techniques is that they are designed specially to provide security services.

Tables 5–6 show the works that were recovered through the process illustrated in the diagram of Fig. 6(b) related to blockchain technologies for cybersecurity mesh. The first column presents the author's name, and the second column the publication year. The third column displays the areas where blockchain technology is used. The fourth column has the main algorithms, schemes, or models that are used to design detection systems, attack prevention, or provide security services. These types of systems, attacks, and security services are illustrated in the final column.

Addressing research question RQ1, in each retrieved article, the area where blockchain is used to develop new detection techniques, prevent security risks and increase security services is identified. Fig. 11 summarizes these found areas and groups them into 11 categories. The X-axis represents 11 categories, which are the Internet of Things (IoT), General Security (GS), Smart Environments (SE), Information Security (IS), Computing, Healthcare, Supply Chain (SC), Financial, Security Networks (SN), Big data, and Recommendation Systems (RS), and the Y-axis the publications number.

Blockchain technology is a key area in IoT because blockchain has specific properties, such as private data and decentralization, that are punctually adopted by IoT. There are works that focus on the general study of blockchain technology and cybersecurity in the IoT environments, such as [140,143,150,152,165,167]. Most of these works explore the opportunities and challenges of combining blockchain technologies with IoT as a new tool to resolve cybersecurity problems. Other publications tackle particular issues in IoT using blockchain as a solution to drone cybersecurity [147], the integrity of learning data [146], authentication method [176], and certification information using smart contracts [164]. In this work, [135] introduces a blockchain-based framework for establishing secure communication among IoT devices utilized in smart water utilities. This innovative approach incorporates Quantum-Inspired Quantum Walks (QIQW) to enhance system security and efficiency.

The IoT model greatly impacts critical infrastructures (IoTCI) such as energy, manufacturing, transportation, government, agriculture, and industry, among others. For instance, in [129], it designs a novel blockchain with deep learning to identify intrusion detection in the IoTCI. This paper [162] proposes a review of blockchain to analyse applications of blockchain in the IoTCI area, in particular, the energy sector where authors such as [178] provide confidentiality in the supply chain process. Industrial Internet of Things (IIoT) uses blockchain as a decentralization tool [136] and also in this area, there are works such as [126] that present a review of blockchain technology for cybersecurity in IIoT area, and [158] that explore the most important use of Blockchain technology in cybersecurity for the industry.

The general security category includes works such as [119,124,131,132,158,169,173,179,182] that are focused on studying blockchain technology in general as a solution for the existing widely unsolved problems of confidentiality, authentication, or even any other security violation. In [124], the author uses a Text Mining Algorithm, (LDA), to propose a semi-automatic literature approach on general security. In [119], it exposes the blockchain architectures and models for cybersecurity and [131,159] both works categorize various kinds of cybersecurity challenges and incidents in blockchain, respectively. Moreover, in [163] proposes a solution to prevent malicious actors from permanently embedding child pornography images onto the blockchain. [168,175] present an alternative methodology and control framework to cybersecurity management using blockchain technology.

Within the smart environment category are areas such as smart homes, smart cities, recently smart grids, and smart contracts. Smart grids are a new paradigm that increases daily because they are very useful in smart homes and cities. In this work [139,166], the authors present an overview of future research in blockchain for cybersecurity in the smart grid and simultaneously discuss blockchain and AI-based techniques to mitigate threats. Another publication, like [161], proposes a framework of stochastic energy management for Network Micro Grids utilizing the Directed Acyclic Graph (DAG) to provide authentication on smart grids. Regarding smart homes, in [144], it studied how to improve and ensure the mechanisms in smart home installations through blockchain framework. Similarly, smart cities use blockchain technologies to implement a control access system integrating Blockchain to provide confidentiality [174]. The smart contract category has one work [127], in which it discussed opportunities and challenges of integrating formal logic within the blockchain to improve the verification capacity and prove the correctness of smart contracts.

Information security is fundamental to protecting and sharing data on the network. Recently, the community has been developing a blockchain-based platform for information sharing in a trusted manner, for example, in [149] it creates a platform for information sharing from different countries that are interconnected by applying inter-ledger mechanisms. Unlike [149], in [155] design hyper ledger blockchain to share and protect the information. In [156,181] proposed an information-sharing framework named iShare and BloCyNfo-Share to preserve cybersecurity information sharing using blockchain technology. Ethereum is a popular blockchain and sometimes is a reference to implement a new model, for example, in [151] the author implemented a Cyber Threat Intelligence (CTI) sharing model through the Ethereum blockchain. Websites store a lot of information and even share it among users without knowing their identity, which implies security risks. Thus, [133] introduces a Web Based on Blockchain (WBCA) to provide cybersecurity between different users.

The computing category in this research involves three areas: cloud computing, edge computing, and worm computing. The cloud computing model offers multiple services, one of which is databases as a service (DaaS), where the client delegates the information to the server for storage and manages the information. Thus, the exchange of information is frequent and may be susceptible to attacks; therefore, it is necessary to monitor the network traffic against cyberattacks. In [177], using the Dempster–Shafer theory, a novel blockchain federated cloud computing framework is introduced for network traffic monitoring. Other works, such as [125], introduce one blockchain solution that allows achieving security against cyber attacks utilizing cyber soldiers who work jointly to update the framework based on the Artificial Neural Network (ANN). The author in [130] shows a general description of the integration of blockchain technology with edge computing to develop a trusted environment in cloud computing. A new approach named worm computing is introduced by [134], where

Table 5
The table displays the works related to blockchain and cybersecurity. The first column shows the author's name, followed by the publication year. The third column contains the application areas. The fourth column depicts the algorithms, and the last column illustrates the security services, attacks, or system detection.

Author	Year	Area	Tools	Security services
Prakash et al. [124]	2022	GS	GBT	CAINA
Yadav et al. [125]	2022	Cloud computing	ANN, BT	Cyber-attacks
Lucio et al. [126]	2022	IIoT	GBT	CAINA
Kshetri et al. [119]	2022	GS	GBT	CAINA
Tamani and El-Jaouhari [127]	2022	Smart contract	Formal logic	Correctness
Lakhan et al. [128]	2022	Healthcare	CPS	Malware detection
Ragab and Altalbe [129]	2022	IoTCI	DNN, ECOA	Intrusion detection
Hazra et al. [130]	2022	EC, IoT	GBT	CAINA
Mahmood et al. [131]	2022	GS	GBT	CAINA
Gimenez-Aguilar et al. [132]	2021	GS	GBT	C&A
Razaque et al. [133]	2021	IS	BT	Bottlenecks attack
Shi et al. [134]	2021	WC	BT	URLs detection
Abd El-Latif et al. [135]	2021	IoT, SC	QW, BT	C&I
Lage and Saiz-Santos [136]	2021	IIoT	GBT	Confidentiality
Etemadi et al. [137]	2021	SC	BT	CAINA
Mittal et al. [138]	2021	Pedagogical	AI, SG	Confidentiality
Mengidis et al. [139]	2021	Smart grids	AI, GBT	Attacks detection
Trung et al. [140]	2021	IoT	GBT, AI	C&I
Ahmed et al. [141]	2021	GS	GBT	Mitigation attacks
Zhuang et al. [142]	2021	Smart grids	GBT	CAINA
Daim et al. [143]	2020	IoT, BT	GBT	Confidentiality
Giannoutakis et al. [144]	2020	Smart home	Smart contract	Integrity
Smith and Dhillon [145]	2020	Economy	GBT	Confidentiality
Kim and Park [146]	2022	IoT	ML, BT	Integrity
Ossamah [147]	2020	IoT	FL, BT	C&I
Wang et al. [148]	2020	Vehicular Networks	GBT	C&A
Neisse et al. [149]	2020	IS	Smart contract	Confidentiality
Bansal et al. [150]	2020	IoT	GBT	CAINA
Riesco et al. [151]	2020	IS	BT, Smart contract	Confidentiality
Asuquo et al. [152]	2020	IoT	GBT	C&I
Etemadi et al. [153]	2020	FSC	GBT	Confidentiality
Moriggl et al. [154]	2020	Healthcare	GBT	Confidentiality
ParkDea-woo [155]	2020	IS	Smart contract	C&I
Badsha et al. [156]	2020	Information Sharing	BT	Confidentiality
Serrano [157]	2020	SC	RandomNN, BT	Authentication
Mentsiev et al. [158]	2019	GS	GBT	Confidentiality
Alkhalifah et al. [159]	2019	GS	GBT	CAINA
Zola et al. [160]	2029	Bitcoin network	CML, BT	C&I
Wang et al. [161]	2019	Smart grids	DAG, BT	Authentication
Vance and Vance [162]	2019	IoTCI	GBT	CAINA
Cremona et al. [163]	2019	GS	GBT	Images detection
Neisse et al. [164]	2019	IoT	Smart contract	Authentication
Sharma [165]	2019	IoT	GBT	C&I
Moradi et al. [166]	2019	Smart grids	GBT	C&I
Abdulkader et al. [167]	2019	IoT	GBT, DH	C&A

Table 6
The table displays the works related to blockchain and cybersecurity. The first column shows the author's name, followed by the publication year. The third column contains the application areas. The fourth column depicts the algorithms, and the last column illustrates the security services, attacks, or system detection.

Author	Year	Area	Tools	Security services
White and Daniels [168]	2019	GS	GBT	Confidentiality
Rot and Blaicke [169]	2019	GS	GBT	Authentication
Akarca et al. [170]	2029	Healthcare	BT	C&I
Alexander and Wang [171]	2019	Big data	GBT	Confidentiality
Gupta Gourisetti et al. [172]	2019	DM	GBT	Authentication
Hasanova et al. [173]	2019	GS	GBT	CAINA
Mora et al. [174]	2019	Smart cities	GBT	Confidentiality
Canelón et al. [175]	2019	GS	GBT	Mitigation attacks
Serrano [176]	2019	IoT	RandomNN, BT	Authentication
Malomo et al. [177]	2018	Cloud computing	DF, BT	Detection attacks
Mylrea and Gourisetti [178]	2018	EIoT	GBT	Monitoring attacks
Gorog and Boult [179]	2018	GS	GBT	CAINA
Kiš and Singh [180]	2018	Financial industry	GBT	Prevention attacks
Rawat et al. [181]	2018	IS	GBT	Confidentiality
Axon et al. [182]	2018	GS	GBT	Confidentiality

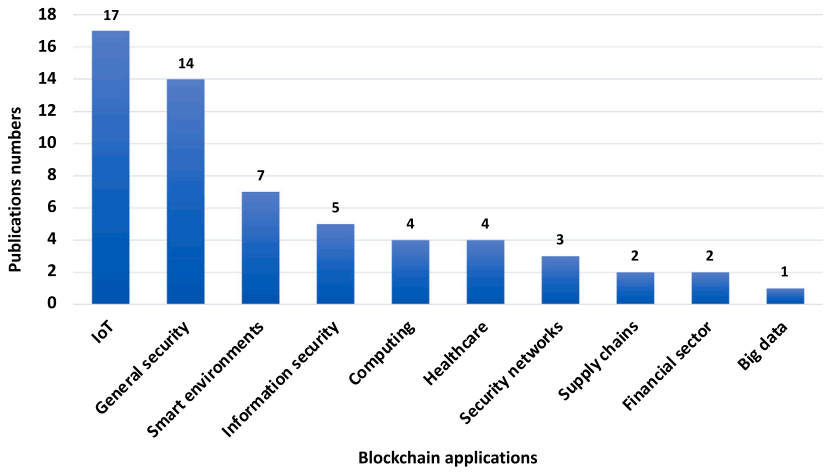


Fig. 11. Existing areas where blockchain technology provides security services. The X-axis represents eight categories, which are the Internet of Things (IoT), General Security (GS), Smart Environments (SE), Information Security (IS), Computing, Healthcare, Security Networks (SN), Supply Chain (SC), Financial Sector, Big Data. The Y-axis represents the publication number obtained from the Web of Science and Scopus resources.

Fig. 12. This cloud graph depicts the most common areas where blockchain is applied to provide security services. There are areas such as Internet of Things (IoT), General Security (GS), Smart Environments (SE), Industrial Internet of Things (IIoT), Internet of Things Critical Infrastructure (IoTCI), and Edge Internet of Things (EIoT).

the author proposes the concept of worm nodes to build a framework of distributed collaboration to ensure the traceability worm computing model.

Blockchain technologies represent a potential tool in the healthcare area because the main requirement in this area is data privacy, and blockchain is a great technology to provide privacy services. In [128], it designs a system for the Industrial Internet of Healthcare Things (IIoHT) utilizing a CPS as a blockchain method to detect malware attacks in networks. Other works like [154,170] investigate blockchain-based solutions to provide cybersecurity requirements in Electronic Health Records (EHR) and explore blockchain as a tool for the management of health data.

The supply chain is developing through multiple stages, and which one there exists the possibility of attacks that represent a security risk. Cyber Supply Chain Risk Management (CSCRM) is adopting blockchain and distributed ledgers technologies, and the author in [137] presents a study to identify the challenges affecting blockchain adoption in CSCRM using Interpretive Structural Modeling (ISM) and the approach named cross-impact matrix multiplication applied to classification (MICMAC). Another review is proposed in [153], which investigates and discloses the capabilities of blockchain technology to mitigate cyberattacks in international food supply chains.

Like healthcare, the financial sector handles a lot of sensitive data that are very attractive to malicious entities because money is usually involved. Blockchain is considered in financial systems as a crucial technology oriented to the protection of privacy and integrity data [180]. In [145], the author presents a review focusing on the financial sector and studies how to improve the cybersecurity of business institutions using Value Focused Thinking (VFT) as a multi-criteria decision analysis tool.

The security networks category contains vehicular networks [148] and bitcoin networks [160]. The first work provides a review of different mechanisms based on blockchain for vehicular networks. The second work focuses on Bitcoin networks and proposes to divide the blockchain into small temporal batches to detect changes in the behaviour of the nodes by means of cascade machine learning. In addition, [157] presents an authentication method to increase cybersecurity against rogue 5G nodes using blockchain with a Random Neural Network.

Within the big data category, one notable publication [171] introduces the applications and challenges of blockchain in big data

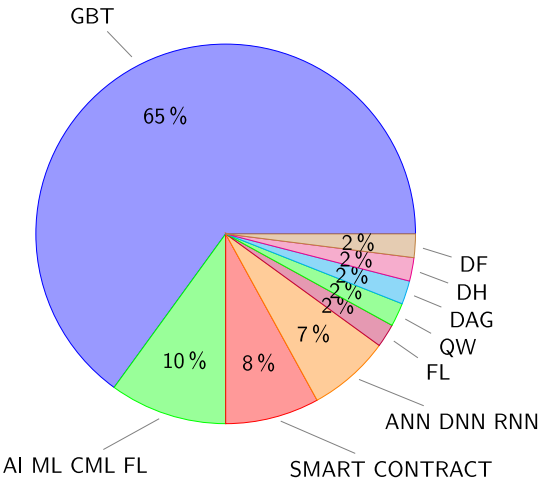


Fig. 13. This graph shows the algorithms, schemes, and models to provide Cybersecurity using Blockchain technology. The percentage was calculated considering articles described in Fig. 6(b).

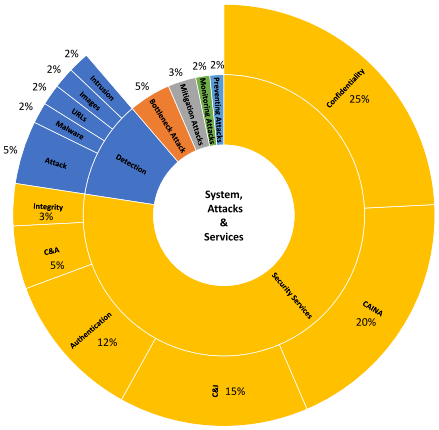


Fig. 14. This graph shows the systems and attacks that were found in the review to provide some security services using blockchain technology for cybersecurity mesh. Confidentiality Authentication, Integrity, Non-repudiation, and Availability (CAINA). The percentage was calculated considering 60 articles described in Fig. 6(b).

to provide cybersecurity services. Finally, in [138], it presents an innovative pedagogical tool that fosters blockchain education among students. Their approach involves an adversarial sandbox adaptive serious game designed to enhance learning experiences. For a comprehensive overview of blockchain technology applications, Fig. 12 provides a visual summary of where blockchain has been used as a cybersecurity tool to provide security services.

5.2. Main algorithms used by blockchain technology to provide security services

Research question RQ2 focuses on knowing the blockchain algorithms applied in different areas found in RQ1. Fig. 13 shows a graph with the algorithms used in this literature review related to blockchain technology to design new cybersecurity models that provide security services. The percentage was calculated considering 60 articles recovered from the Web of Science and Scopus resources. General Blockchain Technologies (GBT) refers to the works that study only blockchain. They did not combine blockchain with any other algorithm to generate a new one. They focus on studying and expanding blockchain in different areas, as explained in RQ1. GBT algorithm represents more than half of the algorithms analysed with 65%; this means that most of the publications are trying to propose new solutions only with blockchain. The smart contract is another algorithm that is very popular in blockchain technology. In this case, it has an 8%, followed by AI, ML, CML, and FL algorithms with 10%. After, ANN, DNN, and RNN combined with blockchain have a 7%. Finally, FL, QW, DAG, DH, and DF represent the 2%, respectively.

5.3. Systems, attacks and services that solve blockchain technology

Research question RQ3 is related to security tools that are used to generate new detection systems and schemes resilient to attacks that provide security services. Fig. 14 presents the systems, attacks, and security services that are provided for the algorithms in research query RQ2. Blockchain technology is based on cryptographic algorithms, and cryptography is developed to achieve information security through security services. Thus, confidentiality service is the most popular service provided and represents 25% of the revised articles. Also, some publications study different ways to provide all CAINA services, and this time, it has 20%, followed by confidentiality and integrity services with 15%. Authentication service has a 12%, confidentiality and authentication have a 5%, and integrity is the last service with 3%. Blockchain, combined with other models such as FL, ML, AI in general, or even cryptography and probabilistic data structures, contributes to developing new detection systems. On this occasion, detection attacks are the most useful with 5%. Followed by intrusion, malware, images, and URL detection with 2%, respectively. In addition to detection systems, different works design models against attacks; for instance, the graph shows that bottleneck attack has a 5%, after mitigation attacks with 3%, and finally, prevention and monitoring attacks with 2%, respectively.

6. Swarming intelligence for the cybersecurity mesh

Swarming intelligence can be defined as a set of decentralized algorithms inspired by the collective behaviour of a large number of relatively simple agents like insects and herd animals such as birds, fish, or ant colonies [183]. These algorithms follow and incorporate animal behaviour patterns across mathematical models which are used to solve optimization problems and design algorithms in dynamic environments.

In swarming intelligence, individual agents interact locally with their environment and with each other based on simple rules or heuristics. These interactions enable the emergence of complex and intelligent behaviour at the group level, even though no single agent possesses a global view or understanding of the system. Swarm intelligence systems often exhibit self-organization, robustness, adaptability, and scalability characteristics. They can solve complex problems by leveraging the group's collective intelligence, allowing for efficient decision-making, problem-solving, optimization, and coordination.

Swarming intelligence encompasses several algorithms that aim to mimic the collective behaviour observed in natural swarms [184]. Here are some of the main algorithms used in swarming intelligence :

Ant Colony Optimization (ACO) is an algorithm inspired by ants' foraging behaviour [185]. These involve a population of artificial ants that deposit pheromone trails on a graph while searching for optimal paths. These pheromones guide the subsequent ants to explore and exploit the best paths, resulting in very efficient solutions to optimization problems.

Particle swarm optimization (PSO) is an algorithm that follows the collective behaviour of herd animals like birds or fish. PSO involves a set of particles that move through a search space, adjusting their positions based on their own experience and the experience of neighbouring particles [186]. The particles search for optimal solutions jointly by updating their velocities and positions, converging towards the best solutions.

Bacterial Foraging Optimization (BFO) mimics the foraging behaviour of bacteria. It involves a population of virtual bacteria that navigate through a search space while optimizing a given objective function. The bacteria move by the movement of an organism or entity in response to a chemical stimulus, following chemical gradients that represent the objective function landscape [187]. Usually, BFO is often applied to optimization problems with continuous variables.

Artificial Bee Colony (ABC) is a metaheuristic algorithm designed for optimization problems that follow the foraging behaviour of honey bees [188]. It involves a population of three categories: employed bees exploring the search space by performing a local search and exchanging information through waggle dances. Then, onlooker bees select promising food sources, according to the information provided by employed bees. Scout bees perform random searches to discover new food sources.

These algorithms are just a few examples of the many techniques in swarming intelligence [189]. Each algorithm has its unique characteristics and is suited for different problem domains. Researchers continue to explore and develop new algorithms and variations to enhance the capabilities of swarming intelligence.

When incorporating swarming intelligence into a cybersecurity mesh, it is essential to take into account various factors such as communication protocols, coordination mechanisms, and trust management. It is crucial to establish secure communication among swarm agents, prevent any potential conflicts of interest or malicious behaviour, and safeguard the integrity of shared information. These are significant challenges that must be overcome to utilize swarming intelligence effectively in cybersecurity.

Swarm intelligence has been suggested as a methodology of network intelligence that lays the foundations for next-generation networks [190]. For example, Particle Swarm Optimization (PSO) is used in cyber security applications related to access control mechanisms based on malicious flow identification [25]. There is also previous evidence that swarm intelligence methods can also be designed with privacy-preserving collaborative tasks [191] such fuzzy logic-based algorithms [118,192], therefore providing a relevant operational base framework to define integration protocols that could be rooted on decision making or intelligent consensus algorithms [193].

6.1. Application areas where swarming intelligence provides security services

In numerous domains like IoT and other areas, the compact designs of devices are fundamental, limiting software, processing power, and resources. Consequently, swarming intelligence plays a vital role when the main objective is to optimize both hardware and software.

Table 7 shows the works that were recovered through the process illustrated in the diagram of Fig. 6(c) related to swarming intelligence for cybersecurity mesh. The first column presents the author's name, and the second column the publication year. The third column displays the areas where swarming intelligence is used. The fourth column has the main algorithms, schemes, or models that are used to design detection systems, attack prevention, or provide security services. These kinds of systems, threats, and security services are illustrated in the final column.

Swarming intelligence algorithms are a crucial area to develop new cybersecurity technologies in many fields; for instance, Fig. 15 shows a graph with the main areas classified into 9 categories: Security Networks (SN), General Security (GS), Internet of Things (IoT), Healthcare, Cloud and Quantum Computing, Websites, Cyber–physical Systems (CPS), Big Data, and Swarm Robots (SR). The above categories and article numbers are represented on the X and Y axes, respectively.

As a reference and addressing the RQ1 for swarming intelligence algorithms, different papers were analysed. In the Security Networks (SN) category, there are works related to secure communication, AUV networks, MANETs, swarm networks, wireless sensor networks, and computer networks. Within secure communication, there are works as [212] where the author tackles the vulnerability of secure communication design a better intrusion detection system and proposes a comparison between two classification techniques, PSO combined with decision tree and PSO with K-Nearest Neighbor. In [217] the author also focuses your work to secure communication, to do this, they propose an intrusion detection system called RNN-ABC that combines a Random Neuronal Network (RandomNN) with Artificial Bee Colony (ABC), the ABC algorithm is applied to optimize the weight of the RandomNN. AUV networks are also in the SN category; here, there are works such as [194], which proposed a technique using a Weighted Regularized Extreme Learning Machine (WRELM) where the parameters are adjusted by applying Swallow Swarm Optimization (SSO) to develop an intrusion detection in AUV networks. In [218], it proposed a flight control algorithm based on Game Theory (GT) and SI for swarm AUV networks, with the intention to protect against attacks like DoS and MitM. The same author but different work [219] proposed a review where ACO, ABC, and PSO were introduced to enhance cybersecurity in Movile Ad doc Networks (MANETs). Another area is swarm networks. According to [221], swarm networks are based on a decentralized network and proposed preventing attacks using the theoretical game model named Blockchain Governance Game (BGG), which allows predicting security actions before the security services are compromised. In [200] is focused on providing security services using a scanning tool called Orchestrated Continuous Vulnerability Assessment (OCVA)that provides multiple activities such as scans, monitors, visualizing, analysing, mitigating, and solving the vulnerabilities in both on-network and web applications. In [203], the author worked with Wireless Sensor Networks (WSNs) and proposed a framework named EEc-MA-PSOGA, where PSO is used to compute and determine the optimal SINK (Special node that collected the data from the different sensor nodes) location. Also, they test your framework against clone attacks. Computer networks are the last field in the SN category, for example, the author [207] suggested a methodology based on ML algorithm as Random Tree (RT), AdaBoost, KNN, SVM and PSO algorithm for intrusion detection in Computer Networks (CN). The ML algorithms are used for classification tasks, and the PSO is used for parameter optimization.

In the domain of general security, there are notable works such as [202], where the author focused on developing a model to find normal or malicious attacks using Deep Belief Network (DBN) to classify different attacks into 5 categories: normal, probe, DoS, U2R, R2L. In this paper, the PSO algorithm is applied to select and extract features, that are then the input to the DBN network. In [184], the author presented another review on the general security area, specifically focusing on malware detection. The author evaluates PSO, ACO, and SOMA algorithms to mitigate malware attacks. The last in this category is [205] which focused on solving sophisticated cyberattacks such as the problem of Advanced Persistent Threats (APT).

Just like federated learning and blockchain, swarm intelligence is another approach that seeks to address challenges within the Internet of Things (IoT) landscape. Several works have sought to create intrusion detection systems for IoT, including [197,206]. Both authors select the features using Aquila Optimizer (AQu) algorithm and then apply Convolutional Neural Networks (CNN) for feature extraction. Another study like [209] aims to secure modern vehicle systems in the Internet of Vehicles (IoV) area from network attacks. To do so, it employed an intrusion detection system utilizing CNN together with the PSO algorithm to optimize the parameters. Contrastingly, the research presented in [201] focuses on predicting attacks in IoT using both PSO and ACO algorithms. As per [201], the most prevalent types of attacks that compromise IoT systems include U2R, DoS, and data probing (Probe).

Another important area is healthcare security, in [208], which proposed a decentralized cybersecurity model using Belief Desire Intention (BDI) as a software model for programming intelligent agents and swarming intelligence. The main objective is to evict the propagation

Table 7
The table displays the works related to swarming intelligence and cybersecurity. The first column shows the author's name, followed by the publication year. The third column contains the application areas. The fourth column depicts the algorithms, and the last column illustrates the security services, attacks, or system detection.

Author	Year	Area	Tools	Security services
Rizwanullah et al. [194]	2022	AUV networks	WRELM SSO	Intrusion detection
Kim [195]	2022	Swarm networks	BGG, SABGG	Preventing attack
Alohali et al. [196]	2022	CCPS	FSO, RNN, LSTM, DBN	Intrusion detection
Nasir et al. [183]	2022	IoT CPS	PSO, ACO, ABC, FSO,	Intrusion detection
Fatani et al. [197]	2022	IoT	CNN, AQU	Intrusion detection
Dai and Boroomand [198]	2021	Big Data	PSO, ACO	CAINA
Yao et al. [199]	2022	Swarm networks	SCA	Spoofing attack
Chahal et al. [200]	2022	Swarm networks	OCVA, ACO, PSO	Scanning tool
Alterazi et al. [201]	2022	IoT	PSO, ACO	Anomaly detection
Sajith and Nagarajan [202]	2022	GS	DBN, PSO	Intrusion detection
Sreedevi and Venkateswarlu [203]	2022	WSNs	PSO	Clone attacks
Truong et al. [204]	2022	GS	ANN, SI	Mitigation attacks
Al Mamun et al. [205]	2022	APT	PSO	Attack detection
Vijayalakshmi et al. [206]	2022	IoT	CNN, AQU	Intrusion detection
Yilmaz [207]	2022	Computer networks	ML, PSO	Intrusion detection
Ribino et al. [208]	2022	Healthcare	SI	C&I
Yang and Shami [209]	2022	IoV	PSO	Intrusion detection
Rosch-Grace and Straub [210]	2022	Quantum computing	QN, ACO, PSO	Identify vulnerabilities
Alibrahim and Ludwig [211]	2021	DNS	Kmeans, PSO, ABC	C&I
Ogundokun et al. [212]	2021	SC	PSO+DT, PSO+KNN	Intrusion detection
Anupam and Kar [213]	2021	Website	BA, FA, GWO, WPA	Phishing attacks
Islam et al. [214]	2021	Healthcare	RandoomNN, ABC	C&I
Ahsan et al. [215]	2020	Cloud Computing	PSO, ACO, ABC, WPA	Intrusion detection
Truong et al. [216]	2020	GS	PSO, ACO, ABC, FSO, AQU	CAINA
Qureshi et al. [217]	2019	SC	RandomNN, ABC	Anomaly detection
Kusyk et al. [218]	2019	AUV networks	GT, SI	DoS, MitM
Thanh and Zelinka [184]	2019	GS	PSO, ACO, SOMA	Malware detection
Kusyk et al. [219]	2018	MANETs	ACO, ABC, PSO	CAINA
Hernández-Herrera et al. [220]	2018	Swarm robots	CRM	Availability

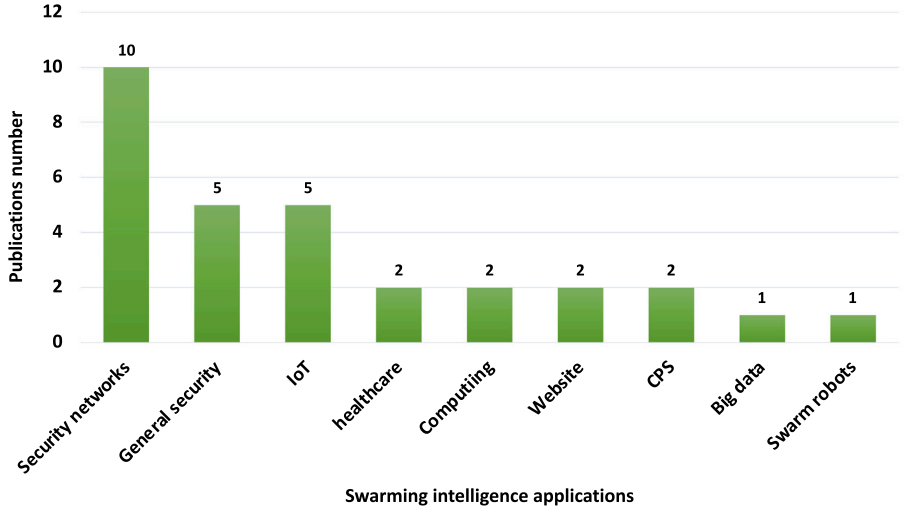


Fig. 15. The graph illustrates the areas where Swarming Intelligence is used to provide security services. The X-axis shows the names of the areas classified into 9 categories: Security Networks (SN), General Security (GS), Internet of Things (IoT), Healthcare, Computing, Websites, Cyber–Physical Systems (CPS), Big Data, Swarm Robots (SR). The Y-axis presents the article number obtained from the Web of Science and Scopus resources.

Fig. 16. This cloud graph depicts the most common areas where swarming intelligence is applied. Within these areas are General Security (GS), Internet of Vehicles (IoV), Maritimal Ad-Hoc Networks (MANETs), Advanced Persistent Threats (APT), Wireless Sensor Networks (WSN), Domain Name Systems (DNS), Cyber–Physical Systems (CPS).

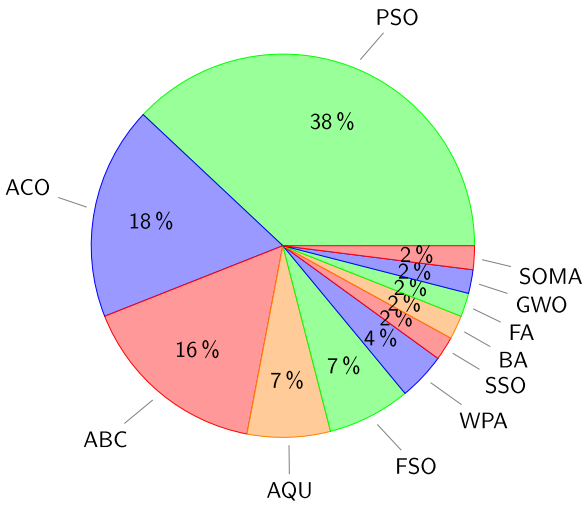


Fig. 17. This graph shows the swarming intelligence algorithms used to build systems and new models for cybersecurity. The percentage was calculated considering 29 articles described in Fig. 6(c).

of attacks inside healthcare organizations. In [214], it presents an innovative approach to fortify the security and resilience of Health Care Information Infrastructure (HCII). The proposed Dynamic Situational Awareness Framework (DSAF) integrates swarm intelligence as a central element for attack detection and risk assessment.

Cloud computing represents a model providing a range of services. A review pertinent to the security aspects of cloud computing was presented in [215]. This work explored the application of swarm algorithms to various security services and techniques. Another promising area lies in the intersection of quantum computing and swarm intelligence. For instance, [210] suggests the combined use of PSO and ACO algorithms along with Quantum Noise (QN). This combination could potentially bolster fuzzing cybersecurity, a method aimed at identifying software vulnerabilities.

In [213], the author developed a Phishing Website Detection (PWD). The system employs SVM to detect legitimate and illegitimate websites, classifying them into phishing and non-phishing categories. Like other works, to optimize the classifier, the author uses swarming intelligence algorithms such as Bat Algorithm (BA), Firefly Algorithm (FA), Grey Wolf Optimiser (GWO), and Whale Optimization Algorithm (WOA). They make a comparison and show the performance, respectively. In [211], the author converts alphabetic names into numeric IP addresses called Domain Name System (DNS), in addition to studying internet systems and focusing on clustering tasks. To provide confidentiality and aside from the crucial role of swarming intelligence in various application areas, it is also important to have knowledge of the algorithms utilized in designing new detection systems and cybersecurity models that offer top-notch security services. Addressing the research question RQ2 will enable us to gain insights into the swarming intelligence algorithms. 4.0, using RNN, Bi-LSTM, DBN and FSO algorithms, FSO is used to optimization of selection features. In [183], the authors develop a survey related to swarming intelligence focusing on CPS and IoT to intrusion detection systems and analyse different optimization algorithms such as PSO, FSO, ACO, ABO, among others.

In [198] it exposes a review of the main AI techniques such as swarming intelligence. This work analysed defence strategies, attacks, and security evaluation models for the big data area through PSO and ACO algorithms. The author provided a concise section that delved into works connected to swarming intelligence. In [220], the author proposed a mechanism based on the Cross Regulation Model (CRM) to preserve the availability in the swarm robots area.

Swarming intelligence is not only used to generate new security tools but also to develop new types of threats. The author in these works [204,216] argue that developing malware prototypes based on SI is a credible threat. They present a malware named X-ware that combines ANN and SI and proposed one kind of virus that is based on the swarm system also. In the same context, the work done by [199] creates a faulty sensor propagation attack classified as a physical attack in a drone swarms environment. This attack exploits the vulnerabilities in Swarm Control Algorithm (SCA) to disrupt the communication in drone swarms, by employing sensor spoofing techniques. Fig. 16 summarizes all application areas where swarming intelligence has been used as a cybersecurity tool to provide security services.

6.2. Main algorithms used by swarming intelligence to provide security services

Apart from the crucial roles played by swarming intelligence in various application areas, it is equally vital to understand the algorithms employed in developing innovative detection systems and cybersecurity models that offer reliable security services. In order to address the research question RQ2, the focus should be on gaining knowledge about swarming intelligence algorithms. Fig. 17 shows a graph with the algorithms used in this literature review related to swarming intelligence. The percentage was calculated considering 29 articles described in Fig. 6(c). As you can see, the most common algorithm used in swarming intelligence is PSO with 38% of articles [184,196,198,201,203,205,207,209–212,215,216,219]. After, the ACO algorithm has 18% [183,184,198,200,201,210,215,219,222], followed by ABC with 16% [183,211,214–216,219]. AQU and FSO both have a 7% [197,206,216], and continuing WPA has 4% [213,215] . Finally, SSO [194], BA, FA, GWO [213], and SOMA [184] have the same percentage at 2%. The graph only shows the swarm algorithms, however, there are other works such as [199,208,218,220,221] that not used swarm algorithms, however, they focus on swarm networks. For example, in [221] design a swarm network using Blockchain Governance Game (BGG). [218] used game theory to create an AUV network. In [220], the author uses Cross Regulation Model (CRM) to provide availability in the swarm robots.

6.3. Systems, attacks and services that solve swarming intelligence

The swarm algorithms are built, considering security as design lines. The objective of these algorithms is to generate new security tools, such as detection systems and schemes resilient to attacks that provide security services. Research question RQ3 is related to these security tools;

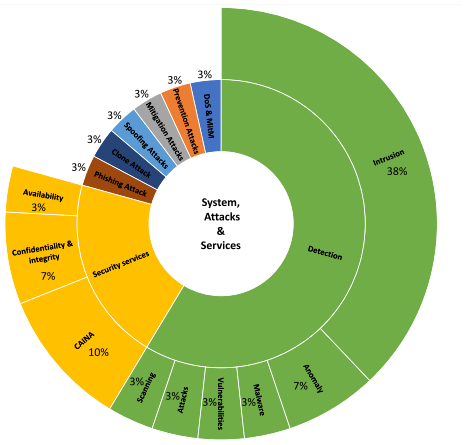


Fig. 18. This graph shows the systems and attacks that were found in the review to provide some security services using the swarming intelligence for cybersecurity mesh. Confidentiality Authentication, Integrity, Non-repudiation, and Availability (CAINA). The percentage was calculated considering 29 articles described in Fig. 6(c).

Fig. 18 presents the systems, attacks, and security services that are provided for the algorithms in research query RQ2. In graph 18, most of the articles design detection systems; for instance, intrusion detection occupied the first place with 38% [183,194,196,197,202,206,207,209,212,215], after anomaly detection with 7% [201,217], allowed by malware detection [184], vulnerability detection [210], attacks detection [205], and scanning detection [200] with 3%, respectively. Unlike detection systems that only detect threats, prevention [221] and mitigation attacks [204] actuate to prevent and decrease the threats. In this review, these kinds of tools represent 3%. Other works focus on resolving particular attacks, for instance, spoofing [199], cloning [203], phishing [213], DoS and MitM [218], which have 3% each one of the reviewed articles. Concerning security services, there are works that propose reviews of different security tools and tried to cover all security services CAINA [198], in this case, with 10%. Confidentiality and integrity with 7% [75,208,211], and availability with 3% [220].

In summary, the swarming intelligence algorithms are excellent for optimization parameters, for this reason, all of them work together with other algorithms such as FL, ML, and blockchain with the aim to improve their performance and get better results when extracting and selecting features is required. Also is important to mention that the swarming intelligence algorithms are very useful in designing decentralized swarm networks.

7. Discussion

The areas studied above are quite useful tools, and these may be applied in diverse areas. Federated learning is a trending topic because, unlike learning the classical model, the FL model does not require that the client delegate his data to an untrusted server. In this way, FL provides privacy and integrity data. Blockchain technology is a decentralized database designed considering cryptographic algorithms such as a hash function and encryption algorithms which allows for data safeguarding with different security services. Swarm intelligence algorithms are employed to tackle optimization problems based on bio-inspired AI algorithms that exhibit rapid adaptability in dynamic environments. Table 8 summarizes the advantages and disadvantages of federated learning, blockchain technology, and swarming intelligence.

Table 8
Table depicts a summary of the advantages and disadvantages of federated learning, blockchain technology, and swarming intelligence.

Area	Advantages	Disadvantages
Federated learning	Privacy data Decentralized data Low cost (train model) Customization of model Efficiency (learning process) Horizontal scalability	Non-IID issues Communication overhead Manipulated models Service provider delegates his model to the client Untrusted environments to train the models Non-standards to protect infrastructure implementation
Blockchain technology	Privacy data Decentralized protocol Secure communication Transparency Immutability Cryptographic algorithms	High processing cost Storage overhead Scalability Untrusted blockchain platforms DDoSS
Swarming intelligence	Decentralized system Highly robustness Efficiency Scalability Adaptability to new environment	High processing cost Complexity Transparency Applicability Unpredictable Manipulated environments

7.1. Federated learning

At the moment, federated learning can be seen as an intelligent method that could be used to provide security services or even properties such as scalability, and reliability, among others. However, there are security aspects that must be addressed for the model performs safely and efficiently. In the federated learning model, it may be the case where an attacker can intersect the information shared between the global and local models during the training process, this phenomenon is reduced in a man-in-the-middle attack. Another kind of attack can be identity theft, which can be the case where a local model pretends to be a trusted entity and then manipulates the parameters that will be sent to the global model. The worst case is when they usurp the identity of the global model because all the local models will receive the wrong parameters, causing dire predictions in their models and therefore wrong information. In the following paragraphs, some advantages and disadvantages will be discussed.

7.1.1. Advantages

Privacy data is the most important advantage related to cybersecurity, federated learning can be used with sensitive data, such as medical or financial information [39,62,95,102]. Since the data remains local and encrypted, this approach can protect sensitive data from unauthorized access and other privacy concerns, making FL a crucial tool for industries or institutions that handle sensitive data.

Decentralized data in federated learning refers to the distribution of data across multiple devices or nodes. Each participant manages their own information, which enhances data and information security, increasing privacy and decreasing data breaches [89]. Moreover, facilitates the inclusion of larger and more varied data sets to train models, leading to more robust and general models.

Federated learning provides an alternative to training the models using low-cost computational resources of individual devices or nodes participating in the training process [223]. Federated learning minimizes data transfer requirements; instead of moving large volumes of data to a central server, only model updates are shared. This process reduces bandwidth usage and associated costs, making federated learning more economical, particularly in scenarios with limited, expensive network connectivity or privacy requirements.

Federated learning has the ability to scale horizontally by adding more devices or participants to the training process [224]. Each device

contributes its computing power to the training process, allowing for parallelized training and faster model convergence. Another benefit of Federated Learning is its efficiency. By distributing the training process, Federated Learning can leverage the processing power of multiple devices to train models in parallel. This approach can lead to faster training times and lower computational costs than classical machine learning approaches.

The essence of federated learning lies in its ability to train models on data generated by local devices, which ensures the inclusion of diverse sources and enables the creation of highly customized models that are specifically designed to address unique use cases [57]. This customization leads to better performance and improved accuracy in prediction models.

7.1.2. Disadvantages

Despite these advantages, federated learning is not without its challenges. Designing and implementing FL systems can be complex and require sophisticated algorithms and coordination mechanisms. Besides, since each participant only has access to their local data, there is a risk of data imbalance. Federated learning assumes that the data on different devices is similar, which may not always be the case. In different parties, the data are non-Independent and Identically Distributed (Non-IID), which introduces specific issues; for instance, Non-IID data can hinder model convergence during federated learning [118]. The varying data characteristics and imbalances can lead to slower convergence, decreased model performance, and difficulty in reaching a consensus during the aggregation process.

Federated learning requires communication between the central server and the local devices that are used to exchange model updates and other information necessary for the federated learning process. This can result in significant communication overhead, which can lead to the training process more slowly. As the number of devices and participants grows, efficient strategies for aggregating model updates need to be implemented to minimize communication overhead and latency [51].

Federated learning aims to minimize communication overhead by local model training and exchanging updated models instead of processing all data. However, the upload and update time for models can depend on several factors, including the network conditions, model size, communication protocols, and the computational capabilities of the participating devices. Optimizing these factors can help reduce the overhead time and enhance the federated learning efficiency.

Protecting the infrastructure implementation in federated learning involves following best practices and adopting standards that address security, privacy, and reliability concerns [89]. FL lacks data governance standards that help ensure that data is collected, stored, and used in a responsible and compliant manner. It is important to consult relevant legal, regulatory, and industry-specific guidelines when selecting and implementing standards for federated learning infrastructure.

Delegating the model to the client raises concerns about model protection. The client has access to the model and its parameters, which could be reverse-engineered or compromised. The decision to delegate the model to the client should be made after careful consideration of the specific use case, for instance, the client's trustworthiness, the required computational resources, and the available protections to ensure model integrity and security. Therefore, should exist measures to protect the integrity and confidentiality of the model.

Another disadvantage lies in the untrusted environments to train the models [85]. Participants in federated learning cannot be fully trusted, either due to malicious intent or potential vulnerabilities in their systems. Dealing with an untrusted execution environment requires additional measures such as cryptographic techniques, privacy-preserving mechanisms, verification procedures, and secure communication protocols, to ensure that participants are not introducing malicious or erroneous updates into the federated learning process, and this way provides quality, integrity, and security of the contributed model updates.

Federated learning could lead to less accurate models because there exists limited control over the data used for training. This can be especially problematic in cases where the data is noisy or contains errors. Federated learning requires the sharing of models and updates between devices, which can pose security risks. These risks include the possibility of models being tampered with or manipulated or the possibility of sensitive data being leaked during the training process [72]. This can occur when participants aim to inject biases, introduce vulnerabilities, or compromise the integrity of the federated learning system.

7.2. Blockchain technology

Blockchain technology is a decentralized and secure system based on cryptographic algorithms to ensure the integrity and privacy of information, which provide transparency, immutability, and other advantages and disadvantages that will be elucidated in the following paragraphs.

7.2.1. Advantages

Blockchain technology encrypts and stores sensitive data on the blockchain. Besides, encryption techniques guarantee that data is transmitted in an encoded and secure form, providing more difficult for untrusted entities to access the information. This enhanced data protection helps to safeguard privacy and integrity to prevent unauthorized access to personal or sensitive information [158].

An additional benefit of blockchain technology lies in its decentralized architecture. In this approach, there is no central authority to verify transactions between nodes which enhances the system's resilience to attacks [182]. In addition, improves the security of communication and allows for faster and more efficient transactions because no need for third-party verification.

Secure communication is an essential advantage of blockchain technology. Across encryption, distributed architecture, consensus mechanisms, and cryptographic techniques, blockchain ensures the integrity, privacy, and authenticity of communication within its network. Each block in the chain contains a record of all previous transactions, and once data is recorded cannot be altered, tampered with, or deleted without the consensus of the network participants, this property is known as immutability. This property and other more such as transparency provide it an attractive solution for various industries that require secure and transparent transactions. Moreover, make it easier to track the flow of assets and reduce the risk of double spending [225].

Traditional centralized systems are vulnerable because if the central authority fails or gets compromised, the entire system can be disrupted. In contrast, blockchain operates on a network of multiple nodes that work together to validate and maintain the blockchain. Every node in the blockchain contains a complete copy of the blockchain, and all nodes communicate and reach a consensus to agree on the correct functioning. In this way, if any node fail or becomes compromised, the network can continue to function as long as there are enough functioning nodes to maintain the consensus. As a consequence of decentralization, this technology prevents a single entity or node from having full authority or control over the network.

The security and integrity of blockchain technology rely on cryptographic algorithms. These last, are employed in various aspects of blockchain technology such as including transaction validation, data integrity, identity verification, and privacy [159,162,179]. As a consequence, violating or corrupting the data on the blockchain is difficult for attackers. The choice of cryptographic algorithms depends on factors such as security requirements, performance considerations, and the specific use cases of the blockchain network. It is important for blockchain developers and users to stay updated with the latest advancements in cryptographic algorithms and adhere to best practices to ensure the security services of blockchain technologies.

7.2.2. Disadvantages

Blockchain technology provides paramount properties such as decentralization, transparency, and immutability, however, it also has certain disadvantages. Blockchain networks rely on complex cryptographic algorithms to secure and validate transactions. These algorithms require significant computational power and energy consumption to solve mathematical problems, verify transactions, and reach consensus. This can lead to high energy consumption and carbon emissions, which can be a concern in the context of climate change [226]. The community is studying and exploring alternative consensus mechanisms to mitigate high processing costs and make blockchain technology more efficient and sustainable.

Blockchain stores a complete history of all transactions ever made on the chain. Therefore, when the number of transactions increases, so does the amount of data that the nodes must store and replicate, leading to storage and scalability problems. Moreover, since the size of the blockchain increases with each transaction, then the time required to process and validate new transactions also increases, which produces an overhead in the verification process [167,227]. This requirement for extensive storage may be disadvantageous for individual nodes, especially those with limited resources or slower internet connections, limiting the adoption of the technology in some applications.

When considering blockchain platforms, it is crucial to be aware of the potential risks associated with untrusted platforms. While blockchain technology has many benefits, there are some platforms that may not uphold the desired level of trust and security. Certain blockchain platforms may not adequately address privacy requirements; as a consequence, the untrusted platforms may expose sensitive data to unauthorized parties or lack the necessary encryption and privacy features, putting user information at risk.

Blockchain networks have mainly an opponent that can be a significant challenge named Distributed Denial of Service (DDoS) attacks. A DDoS attack occurs when multiple computers or devices overload a target system using massive amounts of requests or data, which renders it unable to function properly [228]. The impact of DDoS attacks can vary depending on whether the blockchain is public or private. Public blockchains, which rely on a large and diverse network of nodes, may be more resilient to DDoS attacks due to their distributed nature. On the contrary, private blockchains with a limited number of participants may be more susceptible to disruption from DDoS attacks.

Currently, the regulatory environment for blockchain technology is still uncertain, as different countries have different laws and regulations governing cryptocurrencies and blockchain technology [229]. This can make it difficult to use blockchain technology for specific applications, such as financial transactions.

7.3. Swarming intelligence

Swarming intelligence has properties such as self-organized and decentralized systems that are used to achieve a common goal through the interaction of a large group of agents. These properties can be integrated into the cybersecurity area to enhance it. Nevertheless, it is important to explore the advantages and disadvantages that these systems are providing.

7.3.1. Advantages

In swarming intelligence, the decision-making and control are distributed among individual agents rather than being centralized in a single authority or control centre. In this approach, each agent has the ability to autonomously behave according to local information, local rules, and interactions with its neighbouring agents forming a collective behaviour [230]. After this, is possible to say that swarming intelligence systems can be cost-effective because they do not require a centralized control system or expensive infrastructure [231].

Another advantage of swarming intelligence systems is that are highly resilient to faults and disruptions. If one or more agents of the network fail, the swarm can continue to operate effectively because other agents can compensate for their absence. Then, the redundancy and parallelism in the system contribute to its resilience, allowing it to adapt to changes, recover from disturbances, and maintain functionality. Therefore, they also are highly adaptable to changing conditions, as they can quickly adjust to new situations and reorganize themselves [232].

With respect to scalability, swarming intelligence systems can easily scale up or down, as new individuals can join or leave the swarm without disrupting the overall system. Also, it can draw on the diverse skills and expertise of the individuals within the swarm, allowing the system to solve complex problems that no individual could solve alone. This scalability contributes to their robustness as they can adjust their size and density based on the requirements of the task or environment [233]. If some agents become unavailable, new agents can join the swarm to maintain its functionality.

Swarm intelligence systems are able to make fast decisions and act swiftly because the agents within the swarm are interconnected and can communicate with one another. Additionally, they have the capacity to tune their performance depending on the environment. [204]. Agents who participate in resolving some activity can continue with their activities even when some agents have a problem, therefore providing more robustness to failure.

7.3.2. Disadvantages

In swarming intelligence, agents must communicate with each other to coordinate their actions and maintain the environment working in the correct way. When the number of agents that participate in some task increases, the computational demands also increase, causing a communication overhead that leads to delays and slowing the system response time. Therefore, one of the disadvantages of swarming intelligence is the computational processing cost that results as a consequence to try of coordinating and synchronizing the behaviour of a large number of agents. Furthermore, the interaction between large amounts of agents can be highly complex. Under this scenario, coordinating the decision-making process introduces difficulties such as achieving consensus, managing conflicts, or balancing individual and collective objectives, which difficult to predict the behaviour of the system [194].

Another disadvantage of swarming intelligence systems is the lack of transparency. This property in swarming intelligence allows management and provides information into how the swarm operates, why certain behaviours occur, and how decisions are made. In certain domains, such as autonomous vehicles or robotics [218,220], regulations may require transparency in swarming systems, which allows regulatory authorities to evaluate the safety, compliance, and ethical standards of the system.

Besides standards, the applicability of swarming intelligence relies on the specific requirements and features of the problem to solve. The design and implementation of swarming systems must consider factors such as the size of the swarm, the nature of interactions, the scalability requirements, and the availability of computational resources, among others that on occasion are difficult to define [200]. Even more, swarming intelligence systems can be highly sensitive to their initial conditions, which can make it difficult to predict how the system will behave in the long term [234]. These systems can be vulnerable to external factors, like changes that affect the environment or interference from external agents, resulting in complex patterns, for instance, chaos.

With respect to security, swarming systems can be susceptible to adversarial attacks that aim to disrupt or manipulate the behaviour of the swarm. Attackers may exploit vulnerabilities in communication, sensing, or decision-making processes to subvert the swarm's goals or cause unintended consequences [202].

7.4. Contribution of each technology to the cybersecurity mesh

Federated Learning contributes significantly to the cybersecurity mesh by providing a decentralized and collaborative approach to model training and improvement. These models are employed to detect, mitigate and classify different kinds of attacks through decentralized nodes without the need to centralize data [235]. The learning process is distributed across multiple nodes, exchanging only essential information to update models, thus preserving the privacy of individual nodes and sensitive information. This decentralized approach not only enhances privacy but also increases resilience against attacks, as risks are mitigated during local learning. Consequently, this reduces the risk of data breaches, a crucial consideration in a cybersecurity mesh environment. Moreover, federated learning reduces the communication overhead, exchanging only model updates between nodes rather than raw data. This is particularly advantageous in resource-constrained environments or scenarios where bandwidth is limited [236], which is a common consideration in cybersecurity mesh implementations.

Like federated learning, blockchain contributes to the cybersecurity mesh in several ways. Blockchain is a decentralized technology that operates by distributing the control and storage of data through multiple nodes. Each node in the network may verify and validate transactions. A transaction is a set of records that are transparent to all the participants but, at the same time, are immutable; it cannot be altered or tampered with, maintaining data integrity. Therefore, blockchain enables secure and transparent data sharing among participants. This is particularly beneficial for the cybersecurity mesh, where different entities can contribute and access threat data without compromising the integrity or confidentiality of the information. Moreover, blockchain can be used to address the problem of Identity and access management by providing a secure and decentralized way to manage user identities, reducing the risk of identity theft, unauthorized access, and credential compromise [237]. Blockchain allows the deployment of smart contracts, which are self-executing codes on the blockchain and can be employed to automate and enforce security protocols. These contracts can define and execute predefined security measures, such as access control policies or incident response actions, based on specific conditions or triggers, thereby improving the overall responsiveness of the cybersecurity mesh [238]. The decentralized and distributed nature of blockchain reduces the risk of a single point of failure and enhances the security and resilience of the system in the cybersecurity mesh model.

Unlike federated learning and blockchain, swarming intelligence contributes to the cybersecurity mesh by providing a dynamic and adaptive approach to threat detection, response, and mitigation. This technology leverages the collective intelligence of a diverse group of agents or entities to detect and respond to cybersecurity threats [239]. The agents often exhibit self-organizing behaviour, allowing them to autonomously adapt to changes in the environment. This self-organization enhances the scalability and efficiency of the cybersecurity mesh infrastructure. The adaptive nature of swarming intelligence allows the cybersecurity mesh to respond dynamically to new and sophisticated cyber threats, improving resilience against rapidly changing attacks. Additionally, swarming intelligence enables dynamic resource allocation based on the current threat environment. Resources can be directed to areas that are under attack [240], ensuring an efficient and targeted response to security incidents within the cybersecurity mesh.

7.5. Summary

Federated learning, blockchain, and swarming intelligence are three technologies that have the potential to transform the way we collect and analyse data. While each technology has its unique strengths and weaknesses, they can also complement each other in various ways.

Federated learning enables data to be trained on decentralized devices rather than centralized servers. In federated learning, the data stays on the user's locally and is only used to train the learning model, increasing privacy and reducing communication costs. Blockchain technology provides a secure and decentralized approach to store and share data, ensuring the integrity of data which is ideal for use cases like supply chain and secure communication. Swarming intelligence is a technique that enables groups of agents to work together to solve complex problems, and by applying local interactions and simple rules, swarming intelligence can lead to emergent behaviours and self-organization, which can be beneficial in situations where centralized control is not possible.

Combining these technologies, a decentralized, secure, and privacy-preserving data analysis system can be created, which can be quite powerful. For instance, decentralized devices could be employed to train models of machine learning using the federated learning approach, and blockchain technology could be utilized to securely store and distribute the resulting models and data in a transparent manner. Additionally, swarming intelligence could coordinate the actions of agents in a decentralized network, leading to more efficient and effective data analysis.

The combination of federated learning, blockchain, and swarming intelligence presents promising opportunities for data-driven innovation. These technologies have the potential to provide increased privacy, security, and decentralization. Nevertheless, there are significant hurdles to overcome in terms of standardization, scalability, and interoperability. The integration and application of these technologies together in the real world are still under exploration. Nevertheless, there are scenarios where this integration of these technologies may be critical.

For instance, a healthcare consortium aims to enhance the security of patient data through various hospitals and clinics. Federated Learning is employed to train predictive models for disease diagnosis using decentralized patient records and blockchain is utilized to securely manage and authenticate access to patient records, ensuring data integrity [241]. As a future work, swarming intelligence may be implemented for collaborative anomaly detection, rapidly identifying potential security threats across the network.

Another scenario is about the financial sector. Financial institutions collaborate to create a more secure financial ecosystem [242]. Blockchain ensures the integrity of financial transactions and enhances identity management. Swarming Intelligence and federated learning could be used for real-time threat intelligence sharing, allowing financial institutions to collectively respond to emerging cyber threats.

A global supply chain network is a scenario where federated learning is integrated to predict and prevent disruptions in the supply chain without sharing proprietary information and blockchain is implemented for secure and transparent tracking of goods, ensuring the integrity of the supply chain data [243].

Nowadays, critical infrastructure is a research area where companies adopt different technologies such as federated learning for predictive maintenance of critical infrastructure components, optimizing operations without exposing sensitive data [244]. Blockchain is used to secure communication and control systems within the infrastructure, preventing unauthorized access [245].

8. Trends and future directions

Cryptographic algorithms and AI models like federated learning, swarming intelligence, and blockchain technologies are quite useful for security services and have ignited a new era of innovation and resilience. Federated learning, with its particular characteristics such as decentralized and privacy-preserving, allows us to collaborate and improve models on threat intelligence without compromising sensitive data. Blockchain technology offers an immutable and transparent framework for secure data storage, identity management, and decentralized consensus mechanisms, establishing robust trust. Swarming intelligence, inspired by the collective behaviour of natural systems,

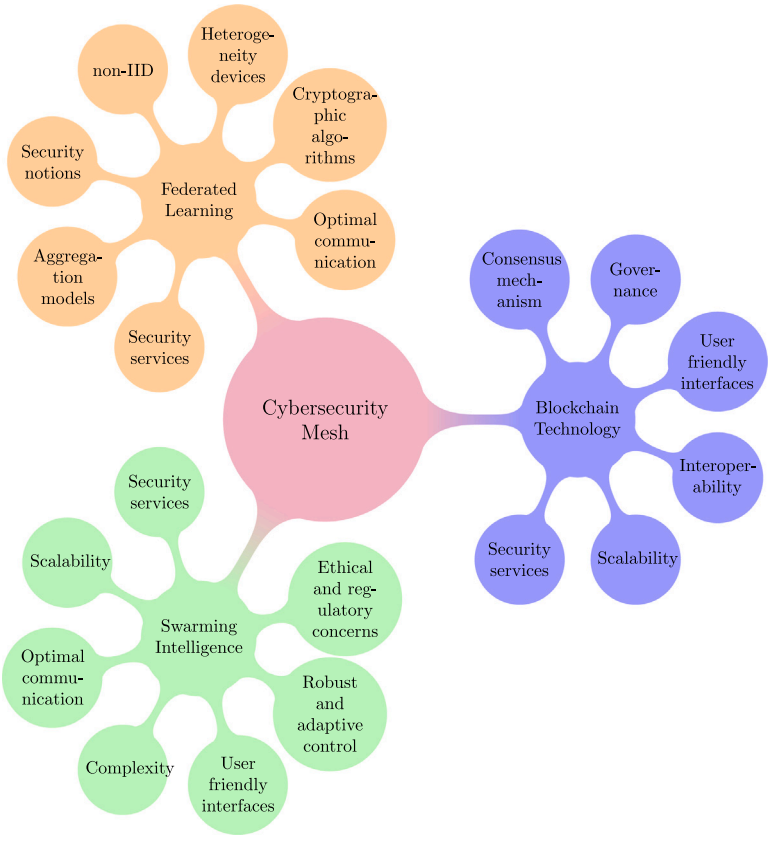


Fig. 19. Figure displays the open challenges of federated learning, blockchain technology, and swarming intelligence.

enables dynamic threat detection and may produce adaptive defence strategies. These trends represent new opportunities for cybersecurity with distributed defence, enhanced privacy, and collective intelligence to combat cyber attacks and/or any security risks.

According to [26] certain disciplines had been studied and there are numerous applications where they can be applied, while others have only a few case studies. Currently, federated learning has a great development in the security domain. However, it lacks a security analysis. Therefore, in accordance with [8], it is necessary to develop more research work in models where federated learning is used and to see the vulnerabilities that have not been studied yet. Unlike federated learning, cryptographic data structures are well-defined and normally use cryptographic primitives for their design. These primitives guarantee a higher level of security for any cryptographic schemes. Fig. 19 displays the open challenges for federated learning, blockchain technology, and swarming intelligence. The second level specifies the technology, while the second level shows the corresponding open challenges that will be discussed in the following sections.

8.1. Federated learning

As mentioned in this review, federated learning is a technology that offers many functionalities in different areas. The advantages that provide federated learning are a lot, however, concerning security is necessary to address some issues. Therefore, one of the key trends is to include cryptographic algorithms in the design of federated learning to design new aggregation models. Cryptographic algorithms in federated learning provide a robust framework for secure information sharing, data privacy and security, and other cybersecurity solutions to mitigating security violations. The use of cryptographic techniques such as signature chains, hash functions, homomorphic encryption, and differential privacy can safeguard sensitive data while enabling collaboration and sharing of information across multiple entities.

With federated learning is possible to achieve decentralized data without transferring sensitive information to a central entity. The data remains on local devices or servers, decreasing the risk of a single point of failure and minimizing the exposure of sensitive data to external threats. This decentralized approach not only enhances the privacy and integrity of the data but also reduces the potential for data breaches, as sensitive information is never concentrated in one location. With the help of cryptographic techniques and keeping data local is more complicated for attackers to compromise the privacy of people or institutions. Thus, the combination of federated learning and cryptographic algorithms presents a powerful solution for maintaining data privacy and providing other security services in collaborative machine-learning scenarios.

Federated learning itself has challenges that should be addressed, for instance, achieving heterogeneity between multiple parties that participate in the training process with different computing resources, data distributions, and communication capabilities. The management of non-IID data and the vulnerability of various types of failures, such as network, and device faults, are other kinds of problems. Therefore, when the community has tried to combine FL with cryptography algorithms finds many challenges, for instance, How to design efficient protocols to achieve the integration between FL and cryptography? How to design optimal communication between multiple parties? Trying to respond to these kinds of questions represents an area of opportunity and development for the scientific community.

Within the security context, the development of security analysis for the new proposed schemes, architectures, and algorithms is one of the most important things to do. For this reason, designing a security notion for the proposed scheme is another line to explore for the scientific

community. Since there exists an integration between different tools like FL and cryptographic algorithms, security analysis is a crucial part of the design of new security tools. Should consider all possibilities and ways where attackers may violate the security services.

8.2. Blockchain technology

Blockchain and cybersecurity are two rapidly evolving fields that are interrelated in many ways. Unlike federated learning, blockchain technology is based on cryptographic algorithms to create decentralized frameworks without central authorities, offering potential solutions to security threats. Nevertheless, existing domains where blockchain technology is vulnerable, such as 51% attacks, and social engineering attacks.

Blockchain enables the development of novel technologies such as smart contracts, which are self-executing agreements with predetermined rules and conditions directly into the blockchain. They allow secure and transparent transactions one which other without intermediaries and can be used to establish trust and enforce security measures automatically. Nowadays, the integration of smart contracts for secure and automated transactions is a new research line for the community with new opportunities. The community can use smart contracts to monitor and automatically respond to security incidents, trigger alerts or actions based on predefined criteria, and manage access control to sensitive systems and data, offering more efficient and reliable security mechanisms.

Scalability is another area where blockchain technology needs to work. When the number of transactions or/and participants increases on the network, the blockchain grows making it challenging to store and process [125]. Improving scalability while maintaining the security network and decentralization is crucial. Moreover, blockchain technology has multiple platforms, and they are not always compatible with each other. Interoperability between different blockchain platforms is essential for communication and data exchange between them.

The management of the energy that blockchain requires is a significant challenge that should be addressed to ensure its sustainability. Energy consumption is a crucial topic for the blockchain, the process of mining or validating blocks in a blockchain network requires a significant amount of energy. Whereby, new consensus algorithms with less energy consumption and more equitable should be developed, which represents a great area of opportunities for innovation and the creation of scientific research.

One important part of blockchain technology relies on user adoption. However, the technology is still not user-friendly, and many people find it challenging to understand and use. Improving the user experience and educating the public on the benefits of blockchain technology is crucial for its general adoption. From the business point of view, blockchain technology operates in a regulatory grey area, making it challenging for businesses to adopt it fully. Whereby, is necessary to establish regulatory frameworks to support the blockchain and promote innovation while ensuring the protection and privacy of the client. The community is working to develop and create new regulatory laws for blockchain technologies.

8.3. Swarming intelligence

Similarly to FL and Blockchain, Swarming intelligence also provides a decentralized approach, which can be leveraged to distribute detection and response capabilities across a network or system. Where individual nodes or entities collaborate to identify and respond to threats to improve and reduce the impact of potential threats. Even more, the main characteristic of swarming intelligence in cybersecurity is the ability to provide resilience and adaptability against threats in dynamic environments.

Swarming intelligence is a technology that is used in optimization problems, however, in cybersecurity, new applications of swarm-based algorithms for threat detection and mitigation are being developed. For instance, the community leverages the power of collective intelligence to analyse large amounts of data identifying patterns and detecting anomalies or cyber-attacks. This trend is expected to grow and may combine with cryptographic algorithms to generate more effective and robust frameworks than traditional ones to combat cyberattacks, mainly to provide security services.

The integration of swarming intelligence techniques in a cybersecurity environment has great potential for enhancing general security. Nevertheless, challenges like scalability may impede the application areas. When the number of agents in a swarm increases, the complexity of coordination and communication between them also increases. Scaling up swarming intelligence to large-scale systems is a significant challenge that requires innovative approaches. Thereby, achieving an analysis and study of how to resolve the scalability problem implies the effort and participation of the scientific community.

Swarming intelligence operates in dynamic and uncertain environments, where agents may encounter obstacles, communication failures, or sensor errors that affect the exchange of information, generating an environment vulnerable to privacy and security threats. For this, developing robust and adaptive control algorithms that can handle uncertainty while ensuring the privacy of the swarm is a paramount challenge and it is necessary for the intervention of the researchers to find new solutions.

Swarming intelligence may be quite an alternative to consider in many areas such as secure communication, security networks, and healthcare, nevertheless, it also raises ethical and regulatory concerns, like privacy, and liability. Developing ethical guidelines while ensuring public safety and privacy is a significant challenge. The interactions between agents and humans are very important, thereby creating intuitive and user-friendly interfaces that enable the interaction between both is another significant challenge that remains to be solved.

8.4. Integrations aspects of the technologies in cybersecurity mesh

As the number of devices connected to the internet increases, so does the volume of data. Designing technologies that facilitate the storage and communication of large datasets while concurrently providing robust security services poses a significant challenge. Scalability is a crucial factor in the development of these technologies, especially as the scale of the system expands. In the context of the proposed integration strategies for the cybersecurity mesh, scalability becomes a critical consideration, particularly with the growth in system size. The scalability of the entire cybersecurity mesh is contingent on the combined effects of federated learning, blockchain, and swarming intelligence. The efficiency of integration and communication protocols between these technologies can either positively or negatively impact scalability. Regarding computational and resource requirements, the integration of federated learning, blockchain, and swarming intelligence may increase overall computational and resource demands. Optimizing communication between these technologies and designing resource allocation strategies are essential to accommodate the expanding scale of the cybersecurity mesh.

Although there may be obstacles to deploying each technology on a large scale, employing distributed architectures, optimization techniques for communications, and parallelization could boost the scalability of the suggested cybersecurity mesh. These strategies help cybersecurity mesh to distribute computational tasks mitigating bottlenecks in large-scale deployments and allowing for efficient coordination and communication between nodes. Is important to mention that the particular demands and constraints will vary based on the integrated system's features and the specific cybersecurity issues being tackled. Organizations adopting these solutions should meticulously evaluate scalability based on their distinct use cases and deployment environments.

Fig. 20. Figure displays a set of steps that could help to design and implement the cybersecurity mesh model effectively.

The feasibility of practical adoption for the proposed cybersecurity mesh model depends on various factors, including technological maturity, organizational readiness, regulatory considerations, and the specific use cases and requirements of the adopting entities. For instance, the maturity of these technologies plays a crucial role. If these technologies have reached stability, security, and usability, it enhances the feasibility of practical adoption. Concerning the infrastructure, organizations must assess their existing infrastructure and determine the need for upgrades or modifications to support the computational and resource requirements of the cybersecurity mesh.

Fig. 20 displays a set of steps that organizations or researchers could take to implement the cybersecurity mesh model effectively [246]. In the initial phase, evaluating attack surfaces involves a meticulous examination of the various points where your organization could be vulnerable to cyber threats, considering human factors and potential weaknesses in processes. This foundational analysis sets the stage for the formulation of concrete security goals, providing a clear direction for the cybersecurity strategy. The next step is the evaluation of the current infrastructure to adapt and set up the software and hardware, that is necessary to do the integration of interoperable technologies. The next crucial step involves the preparation of a comprehensive risk management plan. This plan outlines strategies for mitigating identified risks, allocating resources effectively, and establishing protocols for incident response. Security measures, informed by the chosen framework and risk management plan, are deployed across the IT infrastructure. This implementation involves technological solutions and procedural enhancements. The final step is reviewing and refining the security strategy. Cyber threats are dynamic, thus periodic reviews ensure that the security posture remains adaptive and resilient. Monitoring incidents, technological advancements, and changes in the organizational landscape help to establish a robust cybersecurity framework.

For regulatory compliance, the proposed model involves the handling of sensitive data, and compliance with data privacy and security regulations is paramount. Organizations must ensure that the cybersecurity mesh aligns with regional and industry-specific regulatory requirements. The adoption of advanced technologies may involve initial high implementation costs. Organizations need to assess the cost implications and weigh them against the expected benefits and security enhancements offered by the cybersecurity mesh.

Finally, another important aspect to consider is how to elaborate on quantitative or qualitative metrics used for evaluating the effectiveness of each technology's integration into the cybersecurity mesh. The integration metrics are useful. Yet, creating new metrics for evaluating integration efficacy is outside the purview of this survey and would require a distinct, dedicated paper. However, in the following paragraph, we will review the current state-of-the-art integrative evaluation metrics, laying the groundwork for comprehending these qualitative or quantitative measures.

It can be used AI-based test automation for assessing the adequacy of the integration aspects of the technologies in cybersecurity mesh [247]. AI-based test automation operates as a dynamic tool, capable of simulating real-world scenarios and interactions between various technologies within the cybersecurity infrastructure. This simulation-driven assessment allows for the identification of potential vulnerabilities, validation of interoperability, and optimization of integration protocols. Complementing this approach it can use risk assessment tools when especially involved in machine learning technologies to evaluate the cybersecurity risk [248]. Last but not least it has been proposed adding dynamics of cyber risk analytics which could even work at the edge [249].

9. Conclusions

In this paper, we have studied three different wide-used technologies that can be useful in designing this new model named cybersecurity mesh: Federated Learning (FL) (CS1), Blockchain Technology (BT) (CS2), and Swarming Intelligence (SI) (CS3). For each study case CS1, CS2 and CS3, we have examined the different areas where each of these technologies has been applied to, as well as the algorithms that are used to provide security services, and it shows different kinds of security violations or attacks that are resolved.

Generally, when designing new cybersecurity tools are used hash functions, encryption schemes, and any other object whose security has been tested, and even more it worked under high-security standards. According to the outcomes obtained, FL and SI involve algorithms that were not designed to achieve information security. Nevertheless, they can be manipulated to design cybersecurity tools and provide security services. This approach to generating new cybersecurity tools represents opportunities for the scientific community such as achieving both the correct integration of different technologies and optimal communication, designing a formal analysis to define what is the security level of the proposed scheme, algorithm, and protocol, among others. Unlike FL and SI, BT has been developed considering security as design lines between other properties such as anonymity and immutability; and it is based on cryptography algorithms that were focused to protect security services. Despite this, trying to achieve the correct integration with other areas represents a big challenge and the same time provides new opportunities to open possible research lines.

While each area functions independently, their combined use enhances their effectiveness. Swarming intelligence algorithms can optimize and select features, which are then input into algorithms that train the model using a federated learning approach. Additionally, blockchain technology can establish secure communication and exchange information between nodes participating in the federated learning model, ensuring sensitive data is kept private during the training process. This research has presented the advantages and disadvantages of each intelligent method. Disadvantages provide an area where it is possible to explore new research lines such as obtaining more distributed and scalable cybersecurity tools, another line may be the seeking strategies and mechanisms that allow exploiting the advantages of each intelligent system in a joint environment, with the main objective of designing more robust frameworks.

The development of cybersecurity tools is fundamental to multiple application areas, for instance, this work has illustrated both the most popular sectors such as IoT, security networks, smart cities, and smart homes, among others, and the most recent sectors such as healthcare, finance, smart grids, supply chain, vehicles autonomous, education, among others where security is a crucial factor. Recently, cybersecurity has been bolstered not only by cryptographic algorithms but also by other technologies that do not inherently provide security services. Nevertheless, when these technologies are combined, it is possible to obtain comprehensive security services. Therefore, the integration of different technologies is a crucial alternative to developing new cybersecurity tools in the next years. Actually, cybersecurity mesh is a new cybersecurity model that integrates different technologies to tackle and mitigate different cyberattacks. Then, combining intelligent systems to develop new cybersecurity tools is a big challenge, and the community has begun to look at alternatives considering security and effectiveness as the main design line.

Nomenclature

AIA	Airport Image Analysis
AsynFL	Asynchronous Federated Learning
BoEI	Blockchain Orchestrated Edge Intelligence
BT	Blockchain Technology
CAVs	Connected and Automated Vehicles
CGAN	Conditional Generative Adversarial Nets
CNID	Campus Network Intrusion Detection
CRNN	Collaborative Recurrent Neuronal Network
CTI-P	Cyber Threat Intelligence Platform
DANN	Deep Adversarial Neuronal Network
DC	Dew Cloud
DML	Distributed Machine Learning
DTL	Deep Transfer Learning
DTs	Digital Twins
EC	Edge Computing
ECC	Elliptic Curve Cryptographic
ELF	Executable and Link-able Format
EoT	Edge of Things
EVCEs	Electric Vehicle Charging Ecosystems
FDIA	False Data Injections Attacks
FedGAN	Federated Generative Adversarial Network
FHC	Federated Hipersphere Classifier
FIM	Federates Identity Management
FKD	Federated Knowledge Distillation
FL-MA	Federated Learning Movil Agents
GAN	Generative Adversarial Network
GT	Game Theory
HLSTM	Hierarchical Long Short-Term Memory
IIoT	Industrial Internet of Things
IoMT	Internet of Medical Things
IoT-CI	Internet of Things Critical Infrastructure
IoT-ED	Internet of Things Edge Devices
IoT-MN	Internet of Things Mobile Networks
IoT-SN	Internet of Things Satellite Networks
ITS	Intelligent Transport Systems
KD	Knowledge Distillation
LSTM	Long Short-Term Memory
MDL	Multidimensional Deep Learning
MEC	Multi-access Edge Computing
MFL	Multilevel Federated Learning
MTS	Maritime Transportation Systems
PMLM	Preserving Machine Learning Model
RF	Random Forest
RS	Recommendation System
SC	Secure Communication
SCC	Serverless Cloud Computing
SDN	Software Defined Networking
SFL	Segmented federated Learning
SP	Social Psychology
TCGN	Temporal Convolutional Generative Network
UEBA	User and Entity Behaviour Analytics
VC	Voting Classifier
VSN	Vehicular Sensor Network

CRediT authorship contribution statement

Bruno Ramos-Cruz: Data curation, Formal analysis, Investigation, Methodology, Writing – original draft. **Javier Andreu-Perez:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Supervision, Writing – original draft, Writing – review & editing. **Luis Martínez:** Supervision, Validation, Writing – review & editing.

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

No data was used for the research described in the article.

Acknowledgement

We would like to express our profound gratitude to the reviewers and editor for their helpful and constructive comments. This work was supported in-part by The Talentia Senior Program by The Regional Ministry of Economy, Innovation, Science and Employment of Andalusia (reg. 201899905497765). As well as is partially supported by the Junta de Andalucía through the project ProyExcel_00257. Finally, by the University of Jaen through research supports operational plan via action 8a to the first author.

References

[1] Cisco, Hacia un futuro digital más inclusivo, 2020, [Online], Last accessed 2022-06-17, https://news-blogs.cisco.com/emear/es/2020/05/12/hacia-un-futuro-digital-mas-inclusivo/.
[2] Cisco, The future of work, 2021, [Online], Last accessed 2022-06-17, https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2021.pdf.
[3] F. Radoniewicz, National cybersecurity system act, in: Cybersecurity in Poland, Springer, Cham, 2022, pp. 93–109.
[4] Gartner, Top strategic technology trends for 2022: Cybersecurity mesh, 2022, [Online], Last accessed 2022-06-24, https://www.gartner.com/en/doc/756665-cybersecurity-mesh.
[5] B. Fan, D.G. Andersen, M. Kaminsky, Cuckoo filter: Better than bloom, USENIX Program. 38 (4) (2013) 36–40.
[6] M. Etemad, A. Küpçü, Verifiable database outsourcing supporting join, J. Netw. Comput. Appl. 115 (2018) 1–19, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804518301322.
[7] P. Reviriego, D. Larrabeiti, Denial of service attack on cuckoo filter based networking systems, IEEE Commun. Lett. 24 (7) (2020) 1428–1432.
[8] P. Reviriego, J.A. Hernández, Z. Dai, A. Shrivastava, Learned bloom filters in adversarial environments: A malicious URL detection use-case, in: 2021 IEEE 22nd International Conference on High Performance Switching and Routing, HPSR, IEEE, 2021, pp. 1–6.
[9] Gartner, Cybersecurity mesh, 2022, [Online], Last accessed 2023-03-28, https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh.
[10] N.F. Syed, S.W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, R. Doss, Zero trust architecture (ZTA): A comprehensive survey, IEEE Access 10 (2022) 57143–57179.
[11] O. Marfoq, C. Xu, G. Neglia, R. Vidal, Throughput-optimal topology design for cross-silo federated learning, 2020, CoRR, abs/2010.12229. [Online]. Available: https://arxiv.org/abs/2010.12229.
[12] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2018.
[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, Provable data possession at untrusted stores, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007, pp. 598–609.
[14] M. Narasimha, G. Tsudik, Authentication of outsourced databases using signature aggregation and chaining, in: M. Li Lee, K.-L. Tan, V. Wuwongse (Eds.), Database Systems for Advanced Applications, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, pp. 420–436.
[15] P. Devanbu, M. Gertz, C. Martel, S.G. Stubblebine, Authentic data publication over the Internet 1, J. Comput. Secur. 11 (3) (2003) 291–314.
[16] K. Wu, W. Koegler, J. Chen, A. Shoshani, Using bitmap index for interactive exploration of large datasets, in: 15th International Conference on Scientific and Statistical Database Management, 2003, IEEE, 2003, pp. 65–74.
[17] L.M.X. Rodríguez-Henríquez, Security Services on Outsourced Databases (Ph.D. dissertation), INSTITUTO POLITÉCNICO NACIONAL, 2015.
[18] B.H. Bloom, Space/time trade-offs in hash coding with allowable errors, Commun. ACM 13 (7) (1970) 422–426.
[19] A. Silberschatz, H.F. Korth, S. Sudarshan, et al., Database System Concepts, vol. 5, McGraw-Hill, New York, 2002.

[20] M. Kumar, A. Singh, Probabilistic data structures in smart city: Survey, applications, challenges, and research directions, J. Ambient Intell. Smart Environ. (Preprint) (2022) 1–56.

[21] S.S. Moni, D. Gupta, Secure and efficient privacy-preserving authentication scheme using cuckoo filter in remote patient monitoring network, in: 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, TPS-ISA, 2022, pp. 208–216.

[22] J. Grashöfer, F. Jacob, H. Hartenstein, Towards application of cuckoo filters in network security monitoring, in: 2018 14th International Conference on Network and Service Management, CNSM, IEEE, 2018, pp. 373–377.

[23] R. Tahir, A. Raza, M. Naqvi, F. Zaffar, M. Caesar, An anomaly detection fabric for clouds based on collaborative VM communities, in: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID, IEEE, 2017, pp. 431–441.

[24] Q. Tang, J. Shen, Z. Cao, X. Dong, PSSBP: A privacy-preserving scope-query searchable encryption scheme based on blockchain for parking lots sharing in vehicular networks, in: 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing, EUC, IEEE, 2021, pp. 1–8.

[25] M. Piskozub, F. De Gaspari, F. Barr-Smith, L. Mancini, I. Martinovic, MalPhase: Fine-grained malware detection using network flow data, in: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, 2021, pp. 774–786.

[26] X.-S. Yang, S. Deb, Cuckoo search: state-of-the-art and opportunities, in: 2017 IEEE 4th International Conference on Soft Computing & Machine Intelligence, ISCMI, IEEE, 2017, pp. 55–59.

[27] Z. Cui, B. Sun, G. Wang, Y. Xue, J. Chen, A novel oriented cuckoo search algorithm to improve DV-Hop performance for cyber–physical systems, J. Parallel Distrib. Comput. 103 (2017) 42–52.

[28] F. Bonomi, M. Mitzenmacher, R. Panigrahy, S. Singh, G. Varghese, An improved construction for counting bloom filters, in: Y. Azar, T. Erlebach (Eds.), Algorithms – ESA 2006, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, pp. 684–695.

[29] G. Holley, R. Wittler, J. Stoye, Bloom Filter Trie: an alignment-free and reference-free data structure for pan-genome storage, Algorithms Mol. Biol. 11 (2016) 3, [Online]. Available: https://doi.org/10.1186/s13015-016-0066-8.

[30] M. Naor, E. Yogev, Sliding bloom filters, in: L. Cai, S.-W. Cheng, T.-W. Lam (Eds.), Algorithms and Computation, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 513–523.

[31] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, H. Han, A systematic literature review of methods and datasets for anomaly-based network intrusion detection, Comput. Secur. 116 (2022) 102675, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822000736.

[32] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, M. Seale, Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities, IEEE Access 10 (2022) 112392–112415.

[33] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, R. Kinta, A deep study of novel intrusion detection systems and intrusion prevention systems for internet of things networks, Procedia Comput. Sci. 210 (2022) 94–103, The 13th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN) / The 12th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2022) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050922015800.

[34] M.J. Page, D. Moher, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, et al., PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews, Bmj 372 (2021).

[35] M. Alazab, S.P. RM, P. M, P.K.R. Maddikunta, T.R. Gadekallu, Q.-V. Pham, Federated learning for cybersecurity: Concepts, challenges, and future directions, IEEE Trans. Ind. Inform. 18 (5) (2022) 3501–3509.

[36] B. Ghimire, D.B. Rawat, Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things, IEEE Internet Things J. 9 (11) (2022) 8229–8249.

[37] H. de Oliveira Silva, CSAI-4-CPS: A cyber security characterization model based on artificial intelligence for cyber physical systems, in: 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume, DSN-S, 2022, pp. 47–48.

[38] P. Singh, M. Masud, M.S. Hossain, A. Kaur, G. Muhammad, A. Ghoneim, Privacy-preserving serverless computing using federated learning for smart grids, IEEE Trans. Ind. Inform. 18 (11) (2022) 7843–7852.

[39] D. Chowdhury, S. Banerjee, M. Sannigrahi, A. Chakraborty, A. Das, A. Dey, A.D. Dwivedi, Federated learning based Covid-19 detection, Expert Syst. (2022) e13173.

[40] A.K. Singh, D. Saxena, A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment, J. Appl. Secur. Res. 17 (3) (2022) 385–412, [Online]. Available: https://doi.org/10.1080/19361610.2020.1870404.

[41] R. Gosselin, L. Vieu, F. Loukil, A. Benoit, Privacy and security in federated learning: A survey, Appl. Sci. 12 (19) (2022) [Online]. Available: https://www.mdpi.com/2076-3417/12/19/9901.

[42] J. Kwon, B. Jung, H. Lee, S. Lee, Anomaly detection in multi-host environment based on federated hypersphere classifier, Electronics 11 (10) (2022) [Online]. Available: https://www.mdpi.com/2079-9292/11/10/1529.

[43] M.A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, H. Janicke, Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning, IEEE Access 10 (2022) 40281–40306.

[44] T. Vaiyapuri, S. Algamdi, R. John, Z. Sbai, M. Al-Helal, A. Alkhayyat, D. Gupta, Metaheuristics with federated learning enabled intrusion detection system in Internet of Things environment, Expert Syst. (2022) e13138.

[45] S.I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, O. Jogunola, Federated deep learning for zero-day botnet attack detection in IoT-edge devices, IEEE Internet Things J. 9 (5) (2022) 3930–3944.

[46] J. Li, L. Lyu, X. Liu, X. Zhang, X. Lyu, FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT, IEEE Trans. Ind. Inform. 18 (6) (2022) 4059–4068.

[47] M. Driss, I. Almomani, J. Ahmad, et al., A federated learning framework for cyberattack detection in vehicular sensor networks, Complex Intell. Syst. (2022) 1–15.

[48] E.M. Campos, P.F. Saura, A. González-Vidal, J.L. Hernández-Ramos, J.B. Bernabé, G. Baldini, A. Skarmeta, Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges, Comput. Netw. 203 (2022) 108661, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621005405.

[49] M.-Y. Chen, Establishing a cybersecurity home monitoring system for the elderly, IEEE Trans. Ind. Inform. 18 (7) (2022) 4838–4845.

[50] V. Ravi, T.D. Pham, M. Alazab, Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems, IEEE Trans. Comput. Soc. Syst. (2022) 1–10.

[51] M. Naseri, Y. Han, E. Mariconti, Y. Shen, G. Stringhini, E. De Cristofaro, Cerberus: Exploring federated prediction of security events, in: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 2337–2351, [Online]. Available: https://doi.org/10.1145/3548606.3560580.

[52] A. Yazdinejad, A. Dehghantanha, R. Parizi, M. Hammoudeh, H. Karimipour, G. Srivastava, Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks, IEEE Trans. Ind. Inform. 18 (11) (2022) 8356–8366, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85128634357&doi=10.11092fTII.2022.3168011&partnerID=40&md5=ca28b2631bd08f63e51f3cbb5b8fb339.

[53] M. Abdel-Basset, N. Moustafa, H. Hawash, Privacy-preserved cyberattack detection in industrial edge of things (IEoT): A blockchain-orchestrated federated learning approach, IEEE Trans. Ind. Inform. 18 (11) (2022) 7920–7934, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85128593347&doi=10.11092fTII.2022.3167663&partnerID=40&md5=09b444d67505683c910bed88495c14a4.

[54] B. Tahir, M. Tariq, Vulnerability assessment and federated intrusion detection of Air Taxi enabled smart cities, Sustain. Energy Technol. Assess. 53 (2022) [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138203540&doi=10.10162fj.seta.2022.102686&partnerID=40&md5=a0bbad9489fa3bc1e3045831591b1057.

[55] M. Sarhan, W. Lo, S. Layeghy, M. Portmann, HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection, Comput. Electr. Eng. 103 (2022) [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138091381&doi=10.1016%2fj.compeleceng.2022.108379&partnerID=40&md5=46b57f3cdd45c25f57d51b8787fc7722.

[56] H. Moayyed, A. Moradzadeh, B. Mohammadi-Ivatloo, A. Aguiar, R. Ghorbani, A Cyber-Secure generalized supermodel for wind power forecasting based on deep federated learning and image processing, Energy Convers. Manage. 267 (2022) [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85132847237&doi=10.1016%2fj.enconman.2022.115852&partnerID=40&md5=5ec72677a46078485df4963e562bd0ba.

[57] A. Qammar, J. Ding, H. Ning, Federated learning attack surface: taxonomy, cyber defences, challenges, and future directions, Artif. Intell. Rev. 55 (5) (2022) 3569–3606, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85119381222&doi=10.1007%2fs10462-021-10098w&partnerID=40&md5=21e513bcdd87fe1f2cd2447e3729ce69.

[58] Y. Liu, Y. Liu, Z. Liu, Y. Liang, C. Meng, J. Zhang, Y. Zheng, Federated forest, IEEE Trans. Big Data 8 (3) (2022) 843–854, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85089758492&doi=10.1109%2fTBDATA.2020.2992755&partnerID=40&md5=ddc3c22b7618ceb921035c9ef44706fd.

[59] Z. Guo, K. Yu, Z. Lv, K.-K. Choo, P. Shi, J. Rodrigues, Deep federated learning enhanced secure POI microservices for cyber-physical systems, IEEE Wirel. Commun. 29 (2) (2022) 22–29, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85133741136&doi=10.1109%2fMWC.002.2100272&partnerID=40&md5=2849cdb3f74c5b4e62a80ba99d51a6c1.

[60] T. Aurisch, Training of cyber defense agents in tactical inter-organizational networks by using federated learning, Procedia Comput. Sci. 205 (C) (2022) 289–299, [Online]. Available: https://doi.org/10.1016/j.procs.2022.09.030.

[61] C.J.S. Madala, G.H.K. Yadav, S. Sivakumar, R. Nithya, M.K. M, M. Deivakani, Federated learning approach for tracking malicious activities in cyber-physical systems, in: 2022 International Conference on Edge Computing and Applications, ICECAA, 2022, pp. 494–499.

[62] A. Kumar, S. Jain, K. Kaushik, R. Krishnamurthi, Patient-Centric Smart Health-Care Systems for Handling COVID-19 Variants and Future Pandemics: Technological Review, Research Challenges, and Future Directions, Institution of Engineering and Technology, 2022, pp. 181–224, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85142545514&partnerID=40&md5=23587ce079fafbc251ef321d6fc30654.

[63] Z. Anastasakis, K. Psychogyios, T. Velivassaki, S. Bourou, A.C. Voulkidis, D. Skias, A. Gonos, T.B. Zahariadis, Enhancing cyber security in IoT systems using FL-based IDS with differential privacy, in: Global Information Infrastructure and Networking Symposium, GIIS 2022, Argostoli, Greece, September 26-28, 2022, IEEE, 2022, pp. 30–34, [Online]. Available: https://doi.org/10.1109/GIIS56506.2022.9936912.

[64] H.T. Thi, N.D. Hoang Son, P.T. Duy, V.-H. Pham, Federated learning-based cyber threat hunting for APT attack detection in SDN-enabled networks, in: 2022 21st International Symposium on Communications and Information Technologies, ISCIT, 2022, pp. 1–6.

[65] I. Ridhawi, M. Aloqaily, A. Abbas, F. Karray, An intelligent blockchain-assisted cooperative framework for industry 4.0 service management, IEEE Trans. Netw. Serv. Manag. (2022) 1, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85141523294&doi=10.1109%2fTNSM.2022.3217395&partnerID=40&md5=17a408b2b24b8453fc2bab94273f4020.

[66] M. Anwer, G. Ahmed, A. Akhunzada, S. Hussain, M. Khan, Comparative analysis of soft computing approaches of zero-day-attack detection, in: 2022 International Conference on Emerging Trends in Smart Technologies, ICETST, 2022, pp. 1–5.

[67] J. Chen, Q. Guo, Z. Fu, Q. Shang, H. Ma, D. Wu, Campus network intrusion detection based on federated learning, in: 2022 International Joint Conference on Neural Networks, IJCNN, 2022, pp. 1–8.

[68] N. Moustafa, I. Khan, M. Hassanin, D. Ormrod, D. Pi, I. Razzak, J. Slay, DFSat: Deep federated learning for identifying cyber threats in IoT-based satellite networks, IEEE Trans. Ind. Inform. (2022) 1–8, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140793048&doi=10.1109%2fTII.2022.3214652&partnerID=40&md5=0d3849f6548e1e00a018e948e7fc3dca.

[69] X. Huang, J. Liu, Y. Lai, B. Mao, H. Lyu, EEFED: Personalized federated learning of Execution;Evaluation dual network for CPS intrusion detection, IEEE Trans. Inf. Forensics Secur. (2022) 1, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140792921&doi=10.1109%2fTIFS.2022.3214723&partnerID=40&md5=4066d8f1f9f8b934bc94a2593432192d.

[70] S. Datta, A. Bhattacharya, R. Rana, U. Venkanna, iDAM: A distributed MUD framework for mitigation of volumetric attacks in IoT networks, in: 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP, 2022, pp. 326–331.

[71] I. Aliyu, S. Van Engelenburg, M. Mu'azu, J. Kim, C. Lim, Statistical detection of adversarial examples in blockchain-based federated forest in-vehicle network intrusion detection systems, IEEE Access 10 (2022) 109366–109384, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139859889&doi=10.1109%2fACCESS.2022.3212412&partnerID=40&md5=f89fc639eb05cb7d2c539e845c200b6f.

[72] H. J. Alyamani, Cyber security for federated learning environment using AI technique, Expert Syst. (2022) [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138711835&doi=10.1111%2fexsy.13080&partnerID=40&md5=212dd4d1f89228207a52fdd277498e56.

[73] E. Bandara, S. Shetty, R. Mukkamala, A. Rahaman, X. Liang, LUUNU - blockchain, MISP, model cards and federated learning enabled cyber threat intelligence sharing platform, in: C.R. Martin, N. Emami, M.J. Blas, R. Rezaee (Eds.), Annual Modeling and Simulation Conference, ANNSIM 2022, San Diego, CA, USA, July 18-20, 2022, IEEE, 2022, pp. 235–245, [Online]. Available: https://doi.org/10.23919/ANNSIM55834.2022.9859355.

[74] A. De Benedictis, C. Esposito, A. Somma, Toward the adoption of secure cyber digital twins to enhance cyber-physical systems security, Commun. Comput. Inf. Sci. 1621 CCIS (2022) 307–321, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137982364&doi=10.1007%2f978-3-031-14179-9_21&partnerID=40&md5=ff68447fd8c3a251592215fb953c8766.

[75] S. Islam, S. Badsha, S. Sengupta, I. Khalil, M. Atiquzzaman, An intelligent privacy preservation scheme for EV charging infrastructure, IEEE Trans. Ind. Inform. (2022) 1–10, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137909744&doi=10.1109%2fTII.2022.3203707&partnerID=40&md5=cedc49a24cc1471759aecb0f46884941.

[76] S. Arisdakessian, O. Wahab, A. Mourad, H. Otrok, M. Guizani, A survey on IoT intrusion detection: Federated learning, game theory, social psychology and explainable AI as future directions, IEEE Internet Things J. (2022) 1, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137608785&doi=10.1109%2fJIOT.2022.3203249&partnerID=40&md5=4ad2f5be011033dd34fb63f2f88dd7f1.

[77] O. Fadi, Z. Karim, E. Abdellatif, B. Mohammed, A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments, IEEE Access 10 (2022) 93168–93186, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137588621&doi=10.1109%2fACCESS.2022.3203568&partnerID=40&md5=aa9703a758646e5ff65473440eeee194.

[78] T. Khoa, D. Hoang, N. Trung, C. Nguyen, T. Quynh, D. Nguyen, N. Ha, E. Dutkiewicz, Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks, IEEE Internet Things J. (2022) 1, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137573538&doi=10.1109%2fJIOT.2022.3202029&partnerID=40&md5=86a510f47bcf8352bb50d8fabc9af2f2.

[79] R.A. Amit, C.K. Mohan, Federated learning: Dataset management for airport object representations using remote sensing images, in: 2022 IEEE Aerospace Conference, AERO, 2022, pp. 1–14.

[80] H. Sedjelmaci, N. Kheir, A. Boudguiga, N. Kaaniche, Cooperative and smart attacks detection systems in 6G-enabled Internet of Things, in: ICC 2022 - IEEE International Conference on Communications, 2022, pp. 5238–5243.

[81] X. He, Q. Chen, L. Tang, W. Wang, T. Liu, CGAN-based collaborative intrusion detection for UAV networks: A blockchain empowered distributed federated learning approach, IEEE Internet Things J. (2022) 1, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136685290&doi=10.1109%2fJIOT.2022.3200121&partnerID=40&md5=213abaf5a6e42ebdebd6574175fdeae2.

[82] A. Pasdar, Y.C. Lee, T. Liu, S.-H. Hong, Train me to fight: Machine-learning based on-device malware detection for mobile devices, in: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing, CCGrid, 2022, pp. 239–248.

[83] T. Moulahi, R. Jabbar, A. Alabdulatif, S. Abbas, S. El Khediri, S. Zidi, M. Rizwan, Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security, Expert Syst. (2022) [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134666977&doi=10.1111%2fexsy.13103&partnerID=40&md5=63d8c17e88de28b02049e8873cf24b3b.

[84] P. Singh, G. Gaba, A. Kaur, M. Hedabou, A. Gurtov, Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT, IEEE J. Biomed. Health Inf. (2022) 1–10, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134354506&doi=10.1109%2fJBHI.2022.3186250&partnerID=40&md5=7bf83d6771f633b6fa9b62428c3c4433.

[85] T. Markovic, M. Leon, D. Buffoni, S. Punnekkat, Random forest based on federated learning for intrusion detection, IFIP Adv. Inf. Commun. Technol. 646 IFIP (2022) 132–144, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85133265989&doi=10.1007%2f978-3-031-08333-4_11&partnerID=40&md5=ee03b536bce5030a0827108e7a122ee0.

[86] W. Liu, X. Xu, L. Wu, L. Qi, A. Jolfaei, W. Ding, M. Khosravi, Intrusion detection for maritime transportation systems with batch federated aggregation, IEEE Trans. Intell. Transp. Syst. (2022) 1–12, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85132751870&doi=10.1109%2fTITS.2022.3181436&partnerID=40&md5=20bbd7301d866970f5f1a93841277d02.

[87] W. Lalouani, M. Younis, A robust distributed intrusion detection system for collusive attacks on edge of things, in: 2022 IEEE Wireless Communications and Networking Conference, WCNC, 2022, pp. 1004–1009.

[88] H. Sedjelmaci, N. Ansari, On cooperative federated defense to secure multi-access edge computing, IEEE Consum. Electron. Mag. (2022) [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85128635477&doi=10.1109%2fMCE.2022.3167527&partnerID=40&md5=b09aa4ff088c8f857bf07d4261642c6c.

[89] R. Ganjoo, M. Ganjoo, M. Patil, Mitigating poisoning attacks in federated learning, in: Lecture Notes on Data Engineering and Communications Technologies, vol. 96, Springer Science and Business Media Deutschland GmbH, 2022, pp. 687–699, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126267483&doi=10.1007%2f978-981-16-7167-8_50&partnerID=40&md5=8c3dad87d5473e0b16cdff05001fd88d.

[90] N. Hussain, P. Rani, H. Chouhan, U. Gaur, Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: Challenges, opportunities, and open issues, in: EAI/Springer Innovations in Communication and Computing, Springer Science and Business Media Deutschland GmbH, 2022, pp. 169–183, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85124387963&doi=10.1007%2f978-3-030-85559-8_11&partnerID=40&md5=e1ac5fddb4179bd78283d3f7e4ac9e45.

[91] S. Boudko., H. Abie., E. Nigussie., R. Savola., Towards federated learning-based collaborative adaptive cybersecurity for multi-microgrids, in: Proceedings of the 18th International Conference on Wireless Networks and Mobile Systems - WINSYS, INSTICC. SciTePress, 2021, pp. 83–90.

[92] M. Zago, M. Gil Pérez, G. Martínez Pérez, Early DGA-based botnet identification: pushing detection to the edges, Cluster Comput. 24 (3) (2021) 1695–1710.

[93] R.A. Mallah, G. Badu-Marfo, B. Farooq, On the initial behavior monitoring issues in federated learning, IEEE Access 9 (2021) 161046–161054.

[94] Y. Liu, W. Wu, L. Flokas, J. Wang, E. Wu, Enabling SQL-based training data debugging for federated learning, 2021, arXiv preprint arXiv:2108.11884.

[95] I. Siniosoglou, P. Sarigiannidis, V. Argyriou, T. Lagkas, S.K. Goudos, M. Poveda, Federated intrusion detection in NG-IoT healthcare systems: An adversarial approach, in: ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1–6.

[96] S. Agrawal, A. Chowdhuri, S. Sarkar, R. Selvanambi, T.R. Gadekallu, Temporal weighted averaging for asynchronous federated intrusion detection systems, Comput. Intell. Neurosci. 2021 (2021).

[97] K.S. Kumar, S.A.H. Nair, D. Guha Roy, B. Rajalingam, R.S. Kumar, Security and privacy-aware artificial intrusion detection system using federated machine learning, Comput. Electr. Eng. 96 (2021) 107440, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790621004006.

[98] D.C. Attota, V. Mothukuri, R.M. Parizi, S. Pouriyeh, An ensemble multi-view federated learning intrusion detection for IoT, IEEE Access 9 (2021) 117734–117745.

[99] A.G. Martín, M. Beltrán, A. Fernández-Isabel, I. Martín de Diego, An approach to detect user behaviour anomalies within identity federations, Comput. Secur. 108 (2021) 102356, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821001802.

[100] R. Al Mallah, G. Badu-Marfo, B. Farooq, Cybersecurity threats in connected and automated vehicles based federated learning systems, in: 2021 IEEE Intelligent Vehicles Symposium Workshops, IV Workshops, 2021, pp. 13–18.

[101] S. Piasecki, L. Urquhart, P.D. McAuley, Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards, Comput. Law Secur. Rev. 42 (2021) 105542, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364921000157.

[102] F. Farid, M. Elkhodr, F. Sabrina, F. Ahamed, E. Gide, A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services, Sensors 21 (2) (2021) [Online]. Available: https://www.mdpi.com/1424-8220/21/2/552.

[103] S. Shukla, P.D. Sai Manoj, G. Kolhe, S. Rafatirad, On-device malware detection using performance-aware and robust collaborative learning, in: 2021 58th ACM/IEEE Design Automation Conference, DAC, 2021, pp. 967–972.

[104] M. Chen, L. Zhang, T.-Y. Ma, Recommendation approach based on attentive federated distillation, Ruan Jian Xue Bao/J. Softw. 32 (12) (2021) 3852–3868, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85120857342&doi=10.13328%2fj.cnki.jos.006128&partnerID=40&md5=5785c93fa85e0b641b1805b31eb552bb.

[105] T. Zhang, C. He, T. Ma, L. Gao, M. Ma, S. Avestimehr, Federated learning for internet of things, in: Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, SenSys '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 413–419, [Online]. Available: https://doi.org/10.1145/3485730.3493444.

[106] P.T. Duy, T.V. Hung, N.H. Ha, H.D. Hoang, V.-H. Pham, Federated learning-based intrusion detection in SDN-enabled IIoT networks, in: 2021 8th NAFOSTED Conference on Information and Computer Science, NICS, 2021, pp. 424–429.

[107] O. Shahid, V. Mothukuri, S. Pouriyeh, R.M. Parizi, H. Shahriar, Detecting network attacks using federated learning for IoT devices, in: 2021 IEEE 29th International Conference on Network Protocols, ICNP, 2021, pp. 1–6.

[108] E. Bandara, S. Shetty, A. Rahman, R. Mukkamala, Let'sTrace - blockchain, federated learning and TUF/In-ToTo enabled cyber supply chain provenance platform, in: 2021 IEEE Military Communications Conference, MILCOM 2021, San Diego, CA, USA, November 29 - Dec. 2, 2021, IEEE, 2021, pp. 470–476, [Online]. Available: https://doi.org/10.1109/MILCOM52596.2021.9653024.

[109] M. Ferrag, O. Friha, L. Maglaras, H. Janicke, L. Shu, Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis, IEEE Access 9 (2021) 138509–138542, [Online]. Available:https://ieeexplore.ieee.org/document/9562531.

[110] Y. Sun, H. Esaki, H. Ochiai, Adaptive intrusion detection in the networking of large-scale LANs with segmented federated learning, IEEE Open J. Commun. Soc. 2 (2021) 102–112, [Online]. Available:https://ieeexplore.ieee.org/document/9296578.

[111] K. Demertzis, L. Iliadis, E. Pimenidis, N. Tziritas, M. Koziri, P. Kikiras, M. Tonkin, Federated blockchained supply chain management: A CyberSecurity and privacy framework, IFIP Adv. Inf. Commun. Technol. 627 (2021) 769–779, [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-79150-6_60.

[112] Y. Sun, H. Ochiai, H. Esaki, Intrusion detection with segmented federated learning for large-scale multiple lans, in: 2020 International Joint Conference on Neural Networks, IJCNN, IEEE, 2020, pp. 1–8.

[113] L.A.C. de Souza, G. Antonio F. Rebello, G.F. Camilo, L.C.B. Guimarães, O.C.M.B. Duarte, DFedForest: Decentralized federated forest, in: 2020 IEEE International Conference on Blockchain, Blockchain, 2020, pp. 90–97.

[114] R. Zhao, Y. Yin, Y. Shi, Z. Xue, Intelligent intrusion detection based on federated learning aided long short-term memory, Phys. Commun. 42 (2020) 101157, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874490720302342.

[115] T.V. Khoa, Y.M. Saputra, D.T. Hoang, N.L. Trung, D. Nguyen, N.V. Ha, E. Dutkiewicz, Collaborative learning model for cyberattack detection systems in iot industry 4.0, in: 2020 IEEE Wireless Communications and Networking Conference, WCNC, IEEE, 2020, pp. 1–6.

[116] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, E. Ilie-Zudor, Chained anomaly detection models for federated learning: An intrusion detection case study, Appl. Sci. 8 (12) (2018) [Online]. Available: https://www.mdpi.com/2076-3417/8/12/2663.

[117] E. Alpaydin, Introduction to Machine Learning, MIT Press, 2020.

[118] L. Zhang, Y. Shi, Y.-C. Chang, C.-T. Lin, Federated fuzzy neural network with evolutionary rule learning, IEEE Trans. Fuzzy Syst. 31 (5) (2023) 1653–1664.

[119] N. Kshetri, C.S. Bhushal, P.S. Pandey, et al., BCT-CS: Blockchain technology applications for cyber defense and cybersecurity: A survey and solutions, Int. J. Adv. Comput. Sci. Appl. 13 (11) (2022).

[120] M.S. Ferdous, M.J.M. Chowdhury, M.A. Hoque, A survey of consensus algorithms in public blockchain systems for crypto-currencies, J. Netw. Comput. Appl. 182 (2021) 103035, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521000618.

[121] P. Paul, P. Aithal, R. Saavedra, S. Ghosh, Blockchain technology and its types—A short review, Int. J. Appl. Sci. Eng. (IJASE) 9 (2) (2021) 189–200.

[122] Z. Cui, F. XUE, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A hybrid blockchain-based identity authentication scheme for multi-WSN, IEEE Trans. Serv. Comput. 13 (2) (2020) 241–251.

[123] D. Zhang, S. Wang, Y. Zhang, Q. Zhang, Y. Zhang, et al., A secure and privacy-preserving medical data sharing via consortium blockchain, Secur. Commun. Netw. 2022 (2022).

[124] R. Prakash, V. Anoop, S. Asharaf, Blockchain technology for cybersecurity: A text mining literature analysis, Int. J. Inf. Manag. Data Insights 2 (2) (2022) 100112, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667096822000556.

[125] S.K. Yadav, K. Sharma, C. Kumar, A. Arora, Blockchain-based synergistic solution to current cybersecurity frameworks, Multimedia Tools Appl. 81 (25) (2022) 36623–36644, [Online]. Available: https://doi.org/10.1007/s11042-021-11465-z.

[126] Y.I.L. Lucio, K. Márceles Villalba, S.A. Donado, Adaptive blockchain technology for a cybersecurity framework in IIoT, IEEE Rev. Iberoam. Tecnol. Aprendiz. 17 (2) (2022) 178–184.

[127] N. Tamani, S. El-Jaouhari, Blockchain meets formal logic: Semantics level cybersecurity challenges, in: 2022 6th Cyber Security in Networking Conference, CSNet, 2022, pp. 1–6.

[128] A. Lakhan, M.A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, N. Kumar, Blockchain-enabled cybersecurity efficient IIOHT cyber-physical system for medical applications, IEEE Trans. Netw. Sci. Eng. (2022) 1–14.

[129] M. Ragab, A. Altalbe, A Blockchain-based architecture for enabling cybersecurity in the internet-of-critical infrastructures, CMC-Comput. Mater. Contin. 72 (1) (2022) 1579–1592.

[130] A. Hazra, A. Alkhayyat, M. Adhikari, Blockchain-aided integrated edge framework of cybersecurity for internet of things, IEEE Consum. Electron. Mag. (2022) 1.

[131] S. Mahmood, M. Chadhar, S. Firmin, Cybersecurity challenges in blockchain technology: A scoping review, Hum. Behav. Emerg. Technol. 2022 (2022).

[132] M. Gimenez-Aguilar, J.M. de Fuentes, L. Gonzalez-Manzano, D. Arroyo, Achieving cybersecurity in blockchain-based systems: A survey, Future Gener. Comput. Syst. 124 (2021) 91–118, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21001576.

[133] A. Razaque, A. Al Ajlan, N. Melaoune, M. Alotaibi, B. Alotaibi, I. Dias, A. Oad, S. Hariri, C. Zhao, Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system, Appl. Sci. 11 (17) (2021) [Online]. Available: https://www.mdpi.com/2076-3417/11/17/7880.

[134] L. Shi, X. Li, Z. Gao, P. Duan, N. Liu, H. Chen, Worm computing: A blockchain-based resource sharing and cybersecurity framework, J. Netw. Comput. Appl. 185 (2021) 103081, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S108480452100103X.

[135] A.A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S.E. Venegas-Andraca, J. Peng, Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-based smart cities, Inf. Process. Manage. 58 (4) (2021) 102549, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306457321000546.

[136] O. Lage, M. Saiz-Santos, Blockchain and the decentralisation of the cybersecurity Industry, DYNA 96 (3) (2021) 239.

[137] N. Etemadi, P. Van Gelder, F. Strozzi, An ISM modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity, Sustainability 13 (9) (2021) [Online]. Available: https://www.mdpi.com/2071-1050/13/9/4672.

[138] A. Mittal, M. Gupta, M. Chaturvedi, S.R. Chansarkar, S. Gupta, Cybersecurity Enhancement through Blockchain Training (CEBT) – A serious game approach, Int. J. Inf. Manag. Data Insights 1 (1) (2021) 100001, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266709682030001X.

[139] N. Mengidis, T. Tsikrika, S. Vrochidis, I. Kompatsiaris, Cybersecurity in next generation energy grids: Challenges and opportunities for blockchain and AI technologies, in: T. Tagarev, K.T. Atanassov, V. Kharchenko, J. Kacprzyk (Eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, Springer International Publishing, Cham, 2021, pp. 299–314, [Online]. Available: https://doi.org/10.1007/978-3-030-65722-2_18.

[140] N.D. Trung, D.T.N. Huy, T. Van Thanh, N.T.P. Thanh, N.T. Dung, L. Thanh Huong, Digital transformation, AI applications and IoTs in Blockchain managing commerce secrets: and cybersecurity risk solutions in the era of industry 4.0 and further, Management 18 (2021) 10–14704.

[141] I. Ahmed, M. Darda, S. Nath, Blockchain: A new safeguard to cybersecurity, in: S.K. Panda, A.K. Jena, S.K. Swain, S.C. Satapathy (Eds.), Blockchain Technology: Applications and Challenges, Springer International Publishing, Cham, 2021, pp. 271–284, [Online]. Available: https://doi.org/10.1007/978-3-030-69395-4_15.

[142] P. Zhuang, T. Zamir, H. Liang, Blockchain for cybersecurity in smart grid: A comprehensive survey, IEEE Trans. Ind. Inform. 17 (1) (2021) 3–19.

[143] T. Daim, K.K. Lai, H. Yalcin, F. Alsoubie, V. Kumar, Forecasting technological positioning through technology knowledge redundancy: Patent citation analysis of IoT, cybersecurity, and Blockchain, Technol. Forecast. Soc. Change 161 (2020) 120329, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162520311550.

[144] K.M. Giannoutakis, G. Spathoulas, C.K. Filelis-Papadopoulos, A. Collen, M. Anagnostopoulos, K. Votis, N.A. Nijdam, A blockchain solution for enhancing cybersecurity defence of IoT, in: 2020 IEEE International Conference on Blockchain, Blockchain, 2020, pp. 490–495.

[145] K.J. Smith, G. Dhillon, Assessing blockchain potential for improving the cybersecurity of financial transactions, Manag. Finance 46 (6) (2020) 833–848.

[146] J. Kim, N. Park, Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments, Appl. Sci. 10 (14) (2020) [Online]. Available: https://www.mdpi.com/2076-3417/10/14/4718.

[147] A. Ossamah, Blockchain as a solution to drone cybersecurity, in: 2020 IEEE 6th World Forum on Internet of Things, WF-IoT, 2020, pp. 1–9.

[148] X. Wang, C. Xu, Z. Zhou, S. Yang, L. Sun, A survey of blockchain-based cybersecurity for vehicular networks, in: 2020 International Wireless Communications and Mobile Computing, IWCMC, 2020, pp. 740–745.

[149] R. Neisse, J.L. Hernández-Ramos, S.N. Matheu-García, G. Baldini, A. Skarmeta, V. Siris, D. Lagutin, P. Nikander, An interledger blockchain platform for cross-border management of cybersecurity information, IEEE Internet Comput. 24 (3) (2020) 19–29.

[150] P. Bansal, R. Panchal, S. Bassi, A. Kumar, Blockchain for cybersecurity: A comprehensive survey, in: 2020 IEEE 9th International Conference on Communication Systems and Network Technologies, CSNT, 2020, pp. 260–265.

[151] R. Riesco, X. Larriva-Novo, V.A. Villagrá, Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information, Telecommun. Syst. 73 (2) (2020) 259–288.

[152] P. Asuquo, C. Ogah, W. Hathal, S. Bao, Blockchain meets cybersecurity: Security, privacy, challenges, and opportunity, in: S. Kim, G.C. Deka (Eds.), Advanced Applications of Blockchain Technology, Springer Singapore, Singapore, 2020, pp. 115–127, [Online]. Available: https://doi.org/10.1007/978-981-13-8775-3_5.

[153] N. Etemadi, Y. Borbon, F. Strozzi, Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review, in: Proceedings of the XXIV Summer School "Francesco Turco"—Industrial Systems Engineering, Bergamo, Italy, 2020, pp. 9–11.

[154] P. Moriggl, P.M. Asprion, F. Kramer, Blockchain as an enabler for cybersecurity use case: Electronic health records in Switzerland, in: P.M. Asprion, S. Balina, P. Forbrig, J. Kampars, M. Kirikova, C. Møller, A. Morichetta, B. Roelens, K. Sandkuhl (Eds.), Proceedings of the Workshops Co-Organized with the 13th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modelling (PoEM 2020), On-Line (Originally Located in Riga, Latvia), November 26, 2020, in: CEUR Workshop Proceedings, vol. 2749, CEUR-WS.org, 2020, pp. 80–91, [Online]. Available: http://ceur-ws.org/Vol-2749/paper7.pdf.

[155] L.-h. ParkDea-woo, Hyperledger blockchain design for sharing, spreading, and protecting national cybersecurity information, J. Inf. Commun. Converg. Eng. 18 (2) (2020) 94–99.

[156] S. Badsha, I. Vakilinia, S. Sengupta, BloCyNfo-share: Blockchain based cybersecurity information sharing with fine grained access control, in: 2020 10th Annual Computing and Communication Workshop and Conference, CCWC, 2020, pp. 0317–0323.

[157] W. Serrano, 5G cybersecurity based on the blockchain random neural network in intelligent buildings, in: Z. Ju, L. Yang, C. Yang, A. Gegov, D. Zhou (Eds.), Advances in Computational Intelligence Systems, Springer International Publishing, Cham, 2020, pp. 409–422.

[158] A.U. Mentsiev, V.S. Magomadov, M.Z. Ashakhanova, A.U. Mentsiev, M.T. Alams, How the development of Blockchain affected cybersecurity, J. Phys. Conf. Ser. 1399 (3) (2019) 033048, [Online]. Available: http://dx.doi.org/10.1088/1742-6596/1399/3/033048.

[159] A. Alkhalifah, A. Ng, M.J.M. Chowdhury, A.S.M. Kayes, P.A. Watters, An empirical analysis of blockchain cybersecurity incidents, in: 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE, 2019, pp. 1–8.

[160] F. Zola, J.L. Bruse, M. Eguimendia, M. Galar, R. Orduna Urrutia, Bitcoin and cybersecurity: Temporal dissection of blockchain data to unveil changes in entity behavioral patterns, Appl. Sci. 9 (23) (2019) [Online]. Available: https://www.mdpi.com/2076-3417/9/23/5003.

[161] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, S. Mehraeen, Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach, IEEE Trans. Ind. Appl. 55 (6) (2019) 7300–7309.

[162] T.R. Vance, A. Vance, Cybersecurity in the blockchain era : A survey on examining critical infrastructure protection with blockchain-based technology, in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology, PIC S&T, 2019, pp. 107–112.

[163] K. Cremona, D. Tabone, C. De Raffaele, Cybersecurity and the blockchain: Preventing the insertion of child pornography images, in: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, pp. 197–204.

[164] R. Neisse, J.L. Hernández-Ramos, S.N. Matheu, G. Baldini, A. Skarmeta, Toward a blockchain-based platform to manage cybersecurity certification of IoT devices, in: 2019 IEEE Conference on Standards for Communications and Networking, CSCN, 2019, pp. 1–6.

[165] M. Sharma, Blockchain for cybersecurity: Working mechanism, application areas and security challenges, in: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT, Vol. 1, 2019, pp. 1182–1187.

[166] J. Moradi, H. Shahinzadeh, H. Nafisi, G.B. Gharehpetian, M. Shaneh, Blockchain, a sustainable solution for cybersecurity using cryptocurrency for financial transactions in smart grids, in: 2019 24th Electrical Power Distribution Conference, EPDC, 2019, pp. 47–53.

[167] O. Abdulkader, A.M. Bamhdi, V. Thayananthan, F. Elbouraey, B. Al-Ghamdi, A lightweight blockchain based cybersecurity for IoT environments, in: 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2019, pp. 139–144.

[168] J. White, C. Daniels, Continuous cybersecurity management through blockchain technology, in: 2019 IEEE Technology & Engineering Management Conference, TEMSCON, 2019, pp. 1–5.

[169] A. Rot, B. Blaicke, Blockchain's future role in cybersecurity. Analysis of defensive and offensive potential leveraging blockchain-based platforms, in: 2019 9th International Conference on Advanced Computer Information Technologies, ACIT, 2019, pp. 447–451.

[170] D. Akarca, P.Y. Xiu, D. Ebbitt, B. Mustafa, H. Al-Ramadhani, A. Albeyatti, Blockchain secured electronic health records: Patient rights, privacy and cybersecurity, in: 2019 10th International Conference on Dependable Systems, Services and Technologies, DESSERT, 2019, pp. 108–111.

[171] C.A. Alexander, L. Wang, Cybersecurity, information assurance, and big data based on blockchain, in: 2019 SoutheastCon, 2019, pp. 1–7.

[172] N. Gupta Gourisetti, M. Mylrea, H. Patangia, Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC, 2019, pp. 0206–0213.

[173] H. Hasanova, U. Baek, M. Shin, K. Cho, M. Kim, A survey on blockchain cybersecurity vulnerabilities and possible countermeasures, Int. J. Netw. Manag. 29 (2) (2019) [Online]. Available: https://doi.org/10.1002/nem.2060.

[174] O.B. Mora, R. Rivera, V.M. Larios, J.R. Beltrán-Ramírez, R. Maciel, A. Ochoa, A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures, in: 2018 IEEE International Smart Cities Conference, ISC2, 2018, pp. 1–4.

[175] J. Canelón, E. Huerta, J. Incera, T. Ryan, A cybersecurity control framework for blockchain ecosystems, Int. J. Digit. Account. Res. 19 (25) (2019) 103–144.

[176] W. Serrano, The blockchain random neural network in cybersecurity and the internet of things, in: J. MacIntyre, I. Maglogiannis, L. Iliadis, E. Pimenidis (Eds.), Artificial Intelligence Applications and Innovations, Springer International Publishing, Cham, 2019, pp. 50–63.

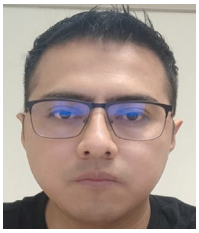
[177] O. Malomo, D.B. Rawat, M. Garuba, Next-generation cybersecurity through a blockchain-enabled federated cloud framework, J. Supercomput. 74 (10) (2018) 5099–5126, [Online]. Available: https://doi.org/10.1007/s11227-018-2385-7.

[178] M. Mylrea, S.N.G. Gourisetti, Blockchain for supply chain cybersecurity, optimization and compliance, in: 2018 Resilience Week, RWS, 2018, pp. 70–76.

[179] C. Gorog, T.E. Boult, Solving global cybersecurity problems by connecting trust using blockchain, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1425–1432.

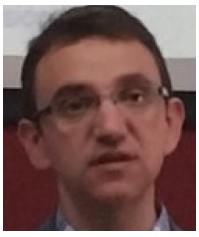
[180] M. Kiš, B. Singh, A cybersecurity case for the adoption of blockchain in the financial industry, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1491–1498.
[181] D.B. Rawat, L. Njilla, K. Kwiat, C. Kamhoua, iShare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity, in: 2018 International Conference on Computing, Networking and Communications, ICNC, 2018, pp. 425–431.
[182] L. Axon, M. Goldsmith, S. Creese, Chapter eight - privacy requirements in cybersecurity applications of blockchain, in: P. Raj, G.C. Deka (Eds.), Blockchain Technology: Platforms, Tools and Use Cases, in: Advances in Computers, vol. 111, Elsevier, 2018, pp. 229–278, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0065245818300172.
[183] M.H. Nasir, S.A. Khan, M.M. Khan, M. Fatima, Swarm intelligence inspired intrusion detection systems — A systematic literature review, Comput. Netw. 205 (2022) 108708, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621005673.
[184] C. Thanh, I. Zelinka, A survey on artificial intelligence in malware as next-generation threats, MENDEL 25 (2) (2019) 27–34, [Online]. Available: https://mendel-journal.org/index.php/mendel/article/view/105.
[185] R.G.C. Upeksha, W.P.J. Pemarathne, Ant colony optimization algorithms for routing in wireless sensor networks: A review, in: Z. Zakaria, S.S. Emamian (Eds.), Recent Advances in Electrical and Electronic Engineering and Computer Science, Springer Singapore, Singapore, 2022, pp. 47–57.
[186] T.M. Shami, A.A. El-Saleh, M. Alswaitti, Q. Al-Tashi, M.A. Summakieh, S. Mirjalili, Particle swarm optimization: A comprehensive survey, IEEE Access 10 (2022) 10031–10061.
[187] D. Pula, R. Puviarasi, Particle Swarm Bacterial Foraging Optimization method for Enhanced digital image watermarking system for data security comparison with Genetic algorithm, in: 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering, ICECONF, 2023, pp. 1–5.
[188] D. Karaboga, et al., An Idea Based on Honey Bee Swarm for Numerical Optimization, Technical report-tr06, Tech. Rep., Erciyes university, engineering faculty, computer . . . , 2005.
[189] D. Chopra, P. Arora, Swarm intelligence in data science: Challenges, opportunities and applications, Procedia Comput. Sci. 215 (2022) 104–111, 4th International Conference on Innovative Data Communication Technology and Application. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705092202083X.
[190] Q.-V. Pham, D.C. Nguyen, S. Mirjalili, D.T. Hoang, D.N. Nguyen, P.N. Pathirana, W.-J. Hwang, Swarm intelligence for next-generation networks: Recent advances and applications, J. Netw. Comput. Appl. 191 (2021) 103141.
[191] C. Census, H. Wang, J. Zhang, P. Deng, T. Li, Particle subswarms collaborative clustering, IEEE Trans. Comput. Soc. Syst. 6 (6) (2019) 1165–1179.
[192] J. Andreu-Perez, Fuzzy learning and its applications in neural-engineering, Neurocomputing 389 (2020) 196–197.
[193] Á. Labella, Y. Liu, R. Rodríguez, L. Martínez, Analyzing the performance of classical consensus models in large scale group decision making: A comparative study, Appl. Soft Comput. 67 (2018) 677–690.
[194] M. Rizwanullah, H.A. Mengash, M. Alamgeer, K. Tarmissi, A.S.A. Aziz, A.A. Abdelmageed, M.I. Alsaid, M.I. Eldesouki, Modelling of metaheuristics with machine learning-enabled cybersecurity in unmanned aerial vehicles, Sustainability 14 (24) (2022) [Online]. Available: https://www.mdpi.com/2071-1050/14/24/16741.
[195] S.-K.A. Kim, Advanced drone swarm security by using blockchain governance game, Mathematics 10 (18) (2022).
[196] M.A. Alohali, F.N. Al-Wesabi, A.M. Hilal, S. Goel, D. Gupta, A. Khanna, Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment, Cogn. Neurodyn. 16 (5) (2022) 1045–1057.
[197] A. Fatani, A. Dahou, M.A.A. Al-qaness, S. Lu, M. Abd Elaziz, Advanced feature extraction and selection approach using deep learning and aquila optimizer for IoT intrusion detection system, Sensors 22 (1) (2022) [Online]. Available: https://www.mdpi.com/1424-8220/22/1/140.
[198] D. Dai, S. Boroomand, A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges, Arch. Comput. Methods Eng. (2021) 1–19.
[199] Y.E. Yao, P. Dash, K. Pattabiraman, Poster: May the swarm be with you: Sensor spoofing attacks against drone swarms, in: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 3511–3513, [Online]. Available: https://doi.org/10.1145/3548606.3563535.
[200] N.S. Chahal, P. Bali, P.K. Khosla, A Proactive Approach to assess web application security through the integration of security tools in a Security Orchestration Platform, Comput. Secur. 122 (2022) 102886, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822002802.
[201] H.A. Alterazi, P.R. Kshirsagar, H. Manoharan, S. Selvarajan, N. Alhebaishi, G. Srivastava, J.C.-W. Lin, Prevention of cyber security with the internet of things using particle swarm optimization, Sensors 22 (16) (2022) 6117.
[202] P. Sajith, G. Nagarajan, Intrusion detection system using deep belief network & particle swarm optimization, Wirel. Pers. Commun. 125 (2) (2022) 1385–1403.
[203] P. Sreedevi, S. Venkateswarlu, An Efficient Intra-Cluster Data Aggregation and finding the Best Sink location in WSN using EEC-MA-PSOGA approach, Int. J. Commun. Syst. 35 (8) (2022) e5110, [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.5110.
[204] T.C. Truong, J. Plucar, B.Q. Diep, I. Zelinka, X-ware: a proof of concept malware utilizing artificial intelligence, Int. J. Electr. Comput. Eng. (IJECE) 12 (2) (2022) 1937–1944.
[205] A. Al Mamun, H. Al-Sahaf, I. Welch, S. Camtepe, Advanced persistent threat detection: A particle swarm optimization approach, in: 2022 32nd International Telecommunication Networks and Applications Conference, ITNAC, 2022, pp. 1–8.
[206] S. Vijayalakshmi, T.D. Subha, M. L, E.S. Reddy, D. Yaswanth, S. Gopinath., A novel approach for IoT intrusion detection system using modified optimizer and convolutional neural network, in: 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2022, pp. 180–186.
[207] A.A. Yilmaz, Intrusion detection in computer networks using optimized machine learning algorithms, in: 2022 3rd International Informatics and Software Engineering Conference, IISEC, 2022, pp. 1–5.
[208] P. Ribino, M. Ciampi, S. Islam, S. Papastergiou, Swarm intelligence model for securing healthcare ecosystem, Procedia Comput. Sci. 210 (2022) 149–156, The 13th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN) / The 12th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2022) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050922015885.
[209] L. Yang, A. Shami, A transfer learning and optimized CNN based intrusion detection system for internet of vehicles, in: ICC 2022 - IEEE International Conference on Communications, 2022, pp. 2774–2779.
[210] D. Rosch-Grace, J. Straub, From quantum fuzzing to the multiverse: Possible effective uses of quantum noise, in: Advances in Information and Communication: Proceedings of the 2022 Future of Information and Communication Conference (FICC), Volume 1, Springer, 2022, pp. 399–410.
[211] H. Alibrahim, S.A. Ludwig, Investigation of domain name system attack clustering using semi-supervised learning with swarm intelligence algorithms, in: 2021 IEEE Symposium Series on Computational Intelligence, SSCI, 2021, pp. 01–09.
[212] R.O. Ogundokun, J.B. Awotunde, P. Sadiku, E.A. Adeniyi, M. Abiodun, O.I. Dauda, An enhanced intrusion detection system using particle swarm optimization feature extraction technique, Procedia Comput. Sci. 193 (2021) 504–512, 10th International Young Scientists Conference in Computational Science, YSC2021, 28 June – 2 July, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921020937.
[213] S. Anupam, A.K. Kar, Phishing website detection using support vector machines and nature-inspired optimization algorithms, Telecommun. Syst. 76 (1) (2021) 17–32, [Online]. Available: https://doi.org/10.1007/s11235-020-00739-w.
[214] S. Islam, S. Papastergiou, H. Mouratidis, A dynamic cyber security situational awareness framework for healthcare ICT infrastructures, in: 25th Pan-Hellenic Conference on Informatics, in: PCI 2021, Association for Computing Machinery, New York, NY, USA, 2022, pp. 334–339, [Online]. Available: https://doi.org/10.1145/3503823.3503885.
[215] M.M. Ahsan, K.D. Gupta, A.K. Nag, S. Poudyal, A.Z. Kouzani, M.A.P. Mahmud, Applications and evaluations of bio-inspired approaches in cloud security: A review, IEEE Access 8 (2020) 180799–180814.
[216] T.C. Truong, T.-P. Huynh, I. Zelinka, Applications of swarm intelligence algorithms countering the cyber threats, in: Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion, GECCO '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 1476–1485, [Online]. Available: https://doi.org/10.1145/3377929.3398119.
[217] A.-U.-H. Qureshi, H. Larijani, N. Mtetwa, A. Javed, J. Ahmad, RNN-ABC: A new swarm optimization based technique for anomaly detection, Computers 8 (3) (2019) [Online]. Available: https://www.mdpi.com/2073-431X/8/3/59.
[218] J. Kusyk, M.U. Uyar, K. Ma, J. Plishka, G. Bertoli, J. Boksiner, AI and game theory based autonomous UAV swarm for cybersecurity, in: MILCOM 2019 - 2019 IEEE Military Communications Conference, MILCOM, 2019, pp. 1–6.
[219] J. Kusyk, M.Ü. Uyar, C.S. Sahin, Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks, Evol. Intell. 10 (3–4) (2018) 95–117, [Online]. Available: https://doi.org/10.1007/s12065-018-0154-4.
[220] A. Hernández-Herrera, E.R. Espino, P.J. Escamilla Ambrosio, A bio-inspired cybersecurity schemeto protect a swarm of robots, in: Advances in Computational Intelligence: 17th Mexican International Conference on Artificial Intelligence, MICAI 2018, Guadalajara, Mexico, October 22–27, 2018, Proceedings, Part II 17, Springer, 2018, pp. 318–331.
[221] S.-K.A. Kim, Advanced drone swarm security by using blockchain governance game, Mathematics 10 (18) (2022) [Online]. Available: https://www.mdpi.com/2227-7390/10/18/3338.
[222] T. Truong, Q. Diep, I. Zelinka, T. Dao, X-Swarm: The upcoming swarm worm, Mendel 26 (1) (2020) 7–14, [Online]. Available: https://mendel-journal.org/index.php/mendel/article/view/112.

[223] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, Y. Jararweh, Federated learning review: Fundamentals, enabling technologies, and future applications, Inf. Process. Manage. 59 (6) (2022) 103061, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306457322001649.
[224] M. Ekmefjord, A. Ait-Mlouk, S. Alawadi, M. Åkesson, P. Singh, O. Spjuth, S. Toor, A. Hellander, Scalable federated machine learning with FEDn, in: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing, CCGrid, 2022, pp. 555–564.
[225] M. Iqbal, R. Matulevičius, Exploring sybil and double-spending risks in blockchain systems, IEEE Access 9 (2021) 76153–76177.
[226] G. Dorfleitner, F. Muck, I. Scheckenbach, Blockchain applications for climate protection: A global empirical investigation, Renew. Sustain. Energy Rev. 149 (2021) 111378, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032121006638.
[227] D. Khan, L.T. Jung, M.A. Hashmani, Systematic literature review of challenges in blockchain scalability, Appl. Sci. 11 (20) (2021) [Online]. Available: https://www.mdpi.com/2076-3417/11/20/9372.
[228] M. Raikwar, D. Gligoroski, DoS attacks on blockchain ecosystem, in: R. Chaves, D. B. Heras, A. Ilic, D. Unat, R.M. Badia, A. Bracciali, P. Diehl, A. Dubey, O. Sangyoon, S. L. Scott, L. Ricci (Eds.), Euro-Par 2021: Parallel Processing Workshops, Springer International Publishing, Cham, 2022, pp. 230–242.
[229] P. Shen, S. Li, M. Huang, H. Gao, L. Li, J. Li, H. Lei, A survey on safety regulation technology of blockchain application and blockchain ecology, in: 2022 IEEE International Conference on Blockchain, Blockchain, 2022, pp. 494–499.
[230] X.-S. Yang, S. Deb, Y.-X. Zhao, S. Fong, X. He, Swarm intelligence: past, present and future, Soft Comput. 22 (2018) 5923–5933.
[231] M. Schranz, G.A. Di Caro, T. Schmickl, W. Elmenreich, F. Arvin, A. Şekercioğlu, M. Sende, Swarm Intelligence and cyber-physical systems: Concepts, challenges and future trends, Swarm Evol. Comput. 60 (2021) 100762, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210650220304156.
[232] J. Tang, H. Duan, S. Lao, Swarm intelligence algorithms for multiple unmanned aerial vehicles collaboration: A comprehensive review, Artif. Intell. Rev. 56 (5) (2023) 4295–4327.
[233] M.M. Abdelhamid, L. Sliman, R. Ben Djemaa, B. Ait Salem, ABISchain: Towards a secure and scalable blockchain using swarm-based pruning, in: Proceedings of the 2023 Australasian Computer Science Week, ACSW '23, Association for Computing Machinery, New York, NY, USA, 2023, pp. 28–35, [Online]. Available: https://doi.org/10.1145/3579375.3579420.
[234] Y. Luo, X. Ouyang, J. Liu, L. Cao, Y. Zou, An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system, Soft Comput. (2022) 1–27.
[235] J. Li, X. Tong, J. Liu, L. Cheng, An efficient federated learning system for network intrusion detection, IEEE Syst. J. 17 (2) (2023) 2455–2464.
[236] M. Venkatasubramanian, A.H. Lashkari, S. Hakak, IoT malware analysis using federated learning: A comprehensive survey, IEEE Access 11 (2023) 5004–5018.
[237] P.M. Yawalkar, D.N. Paithankar, A.R. Pabale, R.V. Kolhe, P. William, Integrated identity and auditing management using blockchain mechanism, Meas.: Sens. 27 (2023) 100732, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2665917423000685.
[238] P. Sharma, R. Jindal, M.D. Borah, A review of smart contract-based platforms, applications, and challenges, Clust. Comput. 26 (1) (2023) 395–421, [Online]. Available: https://doi.org/10.1007/s10586-021-03491-1.
[239] M.A. Alohali, M. Elsadig, F.N. Al-Wesabi, M.A. Duhayyim, A.M. Hilal, A. Motwakel, Swarm intelligence for IoT attack detection in fog-enabled cyber-physical system, Comput. Electr. Eng. 108 (2023) 108676, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790623001003.
[240] Y. Liu, L. Huo, J. Wu, A.K. Bashir, Swarm learning-based dynamic optimal management for traffic congestion in 6G-driven intelligent transportation system, IEEE Trans. Intell. Transp. Syst. 24 (7) (2023) 7831–7846.
[241] M.J. Baucas, P. Spachos, K.N. Plataniotis, Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare, IEEE Trans. Comput. Soc. Syst. 10 (4) (2023) 1732–1741.
[242] A.Y.A.B. Ahmad, S.S. Kumari, M. S, S.K. Guha, A. Gehlot, B. Pant, Blockchain implementation in financial sector and cyber security system, in: 2023 International Conference on Artificial Intelligence and Smart Communication, AISC, 2023, pp. 586–590.
[243] S.K. Nanda, S.K. Panda, M. Dash, Medical supply chain integrated with blockchain and IoT to track the logistics of medical products, Multimedia Tools Appl. 82 (21) (2023) 32917–32939, [Online]. Available: https://doi.org/10.1007/s11042-023-14846-8.
[244] J. Ahn, Y. Lee, N. Kim, C. Park, J. Jeong, Federated learning for predictive maintenance and anomaly detection using time series data distribution shifts in manufacturing processes, Sensors 23 (17) (2023) [Online]. Available: https://www.mdpi.com/1424-8220/23/17/7331.
[245] T. Yu, F. Luo, Q. Wu, G. Ranzi, Blockchain in smart grids: A review of recent developments, in: Emerging Smart Technologies for Critical Infrastructure, Springer, 2023, pp. 23–59.
[246] DevTeam.space, How to build a cybersecurity mesh? 2023, [Online], Last accessed 2024-01-10, https:https://www.devteam.space/blog/cybersecurity-mesh/.
[247] D.S. Battina, Artificial intelligence in software test automation: A systematic literature review, Int. J. Emerg. Technol. Innov. Res. (2019) 2349–5162, (www.jetir.org|UGCandissnApproved), ISSN.
[248] R. Bitton, N. Maman, I. Singh, S. Momiyama, Y. Elovici, A. Shabtai, Evaluating the cybersecurity risk of real-world, machine learning production systems, ACM Comput. Surv. 55 (9) (2023) 1–36.
[249] P. Radanliev, D. De Roure, R. Walton, M. Van Kleek, R.M. Montalvo, L. Maddox, O. Santos, P. Burnap, E. Anthi, Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge, SN Appl. Sci. 2 (2020) 1–8.



Bruno Ramos-Cruz (PhD candidate) is currently pursuing his doctorate at the University of Jaén (Spain). He studied the master's degree in Computer Science at the National Institute of Astrophysics, Optics, and Electronics (Mexico) and the bachelor's degree in mathematics at Autonomous University of Puebla (Mexico). His research is related to security in outsourced databases in cloud computing, authenticated data structure, cryptography, blockchain, and cybersecurity.

Javier Andreu-Perez (Senior Member, IEEE) received the Ph.D. degree, in 2012. He is a Senior Lecturer (Associate Professor, tenured) in the School of Computer Science and Electronic Engineering (CSEE) and group chair of the Smart Health Technologies Group at the University of Essex, United Kingdom. He was awarded his PhD in Intelligent Systems from Lancaster University (UK) and MSc from the University of Granada (Spain). His expertise focuses on artificial intelligence, and fuzzy methodologies & computing-with-words approach for uncertainty modelling in highly noisy, non-stationary, high-dimensional data. Javier has published in journals edited by Elsevier, Springer-Nature, IEEE (TFS, TSMC, TBMI, JBHI, TDCS, etc.), and other venues in artificial intelligence and cognitive neuroscience. Javier's work in artificial intelligence, human informatics and biomedical engineering has attracted 4000+ citations. Javier was chair of the IEEE Computational Intelligence Society (CIS) task force on Extensions of Type-1 fuzzy sets (2018-2022). Javier acts as associate Editor-in-chief of the journal Neurocomputing (Elsevier), the EUSFLAT-sponsored International Journal of Computational Intelligence Systems, and other newer journals on emerging technologies. He's been invited as an expert reviewer for significant publishers such as Science, The Lancet, and BMC. He has served on the technical committee for IEEE WCCI on several occasions and as the workshop chair for FUZZ-IEEE. He has regularly led tutorials and a special session at this event. He was also the general chair for fNIRS-UK 2023. Javier's research has been founded by UK research councils, other funding schemes supported by the Welcome Trust, NIHR, and big-IT corporations such as Nvidia, Amazon, and Oracle. Javier has an extensive portfolio of completed successful knowledge transfer and collaboration with the industry. Dr Andreu-Perez has been awarded prestigious fellowships for his research career from the Japan Society for the Promotion of Science (2022) and a Talentia Senior Fellowship from the Andalusia Scientific Council (2020). His research interests focus on human informatics, symbiotic artificial intelligence, human-machine interaction, robotics, sensor engineering, bio/neuro-engineering, and life science research.



Luis Martínez (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer sciences from the University of Granada, Granada, Spain, in 1993 and 1999, respectively. He is currently a Full Professor with the Computer Science Department, University of Jaén, Jaén, Spain. He is also Visiting Professor with the University of Technology Sydney, Ultmo, NSW, Australia, University of Portsmouth, Portsmouth, U.K., (Isambard Kingdom Brunel Fellowship Scheme), and with the Wuhan University of Technology,

Wuhan, China, (Chutan Scholar), Guest Professor with the Southwest Jiaotong University, Chengdu, China, and Honourable Professor with Xihua University, Chengdu. He has coedited eleven journal special issues on fuzzy preference modelling, soft computing, linguistic decision making, and fuzzy sets theory and has been the Main Researcher in 14 R&D projects. He has also authored or coauthored more than 100 papers in journals indexed by the SCI and more than 150 contributions in International Conferences in his areas of interest. His research interests include decision making, fuzzy logic-based systems, computing with words, and recommender systems. Dr. Martínez was the recipient of IEEE Transactions on Fuzzy Systems Outstanding Paper Award 2008 and 2012 (bestowed in 2011 and 2015, respectively). He is a Co-Editor-in-Chief for International Journal of Computational Intelligence Systems and an Associate Editor for the journals including IEEE Transactions on Fuzzy Systems, Information Fusion, Knowledge-Based Systems, International Journal of Fuzzy Systems, Journal of Intelligent and Fuzzy Systems, etc.