IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 3, 2021, accepted March 17, 2021, date of publication March 30, 2021, date of current version April 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3069737

Privacy-Preserving Schemes for Safeguarding Heterogeneous Data Sources in Cyber-Physical Systems

MARWA KESHK[1], BENJAMIN TURNBULL[1], ELENA SITNIKOVA[1], DINUSHA VATSALAN[2], AND NOUR MOUSTAFA[1], (Senior Member, IEEE)

[1]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2612, Australia
[2]Information Security and Privacy Group, Data61-CSIRO, Eveleigh, NSW 2015, Australia

Corresponding author: Nour Moustafa (nour.moustafa@unsw.edu.au)

ABSTRACT Cyber-Physical Systems (CPS) underpin global critical infrastructure, including power, water, gas systems and smart grids. CPS, as a technology platform, is unique as a target for Advanced Persistent Threats (APTs), given the potentially high impact of a successful breach. Additionally, CPSs are targets as they produce significant amounts of heterogeneous data from the multitude of devices and networks included in their architecture. It is, therefore, essential to develop efficient privacy-preserving techniques for safeguarding system data from cyber attacks. This paper introduces a comprehensive review of the current privacy-preserving techniques for protecting CPS systems and their data from cyber attacks. Concepts of Privacy preservation and CPSs are discussed, demonstrating CPSs' components and the way these systems could be exploited by either cyber and physical hacking scenarios. Then, classification of privacy preservation according to the way they would be protected, including perturbation, authentication, machine learning (ML), cryptography and blockchain, are explained to illustrate how they would be employed for data privacy preservation. Finally, we show existing challenges, solutions and future research directions of privacy preservation in CPSs.

INDEX TERMS Privacy preservation, cyber-physical systems, perturbation, authentication, machine learning, cryptography, blockchain.

I. INTRODUCTION

A Cyber-Physical Systems (CPSs) are the underpinning fabric controlling the world's critical infrastructure. CPS is the integration between the cyber and physical spaces, and are the bridge between the purely cyber and the kinetic, such as power generation and distribution, water treatment, manufacturing and mining. Such systems are tightly integrated and customised to the specific domain [1]. Each CPS installation can be comprised of hundreds or thousands of singular sensors and actuators. This scale and integration generates significant heterogeneous data [2]–[4], including sensor observations, network flow, and user data. This combination of unique factors creates challenges in the performance of efficient big data analytics. Specifically, there are issues in system control and data analytics for the observation of and management of activities within these environments [2], [5]. A CPS environment, such as a power system, will be comprised of multiple cyber-physical components, each with its own industry-specific communication protocol [6]. Such interconnectivity significantly increases the complexity of such environments [2], [6], [7], generating a large volume of data to be protected from cyber attacks.

One of the more common CPS control systems architectures is SCADA. More particularly, SCADA acts as interface, which is responsible for monitoring, configuring and controlling the physical components of the CPS, such as its power systems [3], [7]. Its main function is to anatomise and deduce valuable information to improve a system's operational functions for which various computerised models use a Human-machine Interface (HMI) [7]; for instance, SCADA in a power system acts as industrial technology which manipulates big data measurements gathered from the input through current and voltage transformers and then forwards certain

The associate editor coordinating the review of this manuscript and approving it for publication was Md Zakirul Alam Bhuiyan.

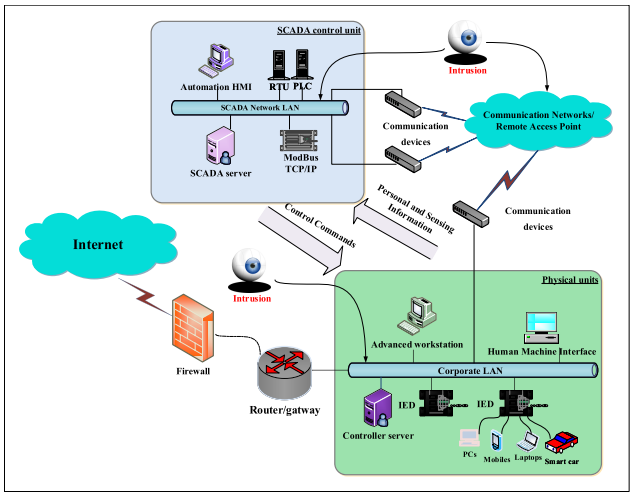

FIGURE 1. Simplified architecture of SCADA in CPS.

commands to control other system devices [4]. Its key components are Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) that operate as ports for handling data sent to terminals using some protocols, such as IEC 60870-5-101/104, IEC 61850 and DNP3 that interact with the Modbus TCP/IP model [7], [8].

To identify and recognise potential cyber attacks against CPSs, it is essential to characterise the standard components of a CPS that could be vulnerable and be exploited using advanced persistent attacks. As shown in Figure 1, a CPS has a large scale of devices and systems, as sensors, actuators, PLCs, RTUs and HMIs [9], which run systems and interact with the Internet for engaging CPSs operations, like use sensors to measure the power meters' data and sending them for further processing, analysis and visualisation. CPSs include different layers of operations and communications, physical, control, supervisory control and corporate layers [10]. Each of these layers is discussed separately. First, the physical layer is comprised of components involving sensors and actuators, which send directly to the control system for processing. The control layer is comprised of Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). These units receive data from physical devices and send back the control commands to be executed. Based on the data received from physical sensing devices and actuators, the control unit pushes commands to perform specific tasks. Lastly, the corporate layer is responsible for communicating between the physical, computing and network devices and systems is potentially vulnerable to the security and privacy issues found in any corporate network [6], [10], [11]. Cyberthreats are exploitable by attackers who often use advanced and sophisticated attacking methods and tools to breach the security principles of the Confidentiality, Integrity and Availability (CIA) triad [12].

This paper provides the core concepts and a critical review of the previous research of Cyber-Physical Systems from a cybersecurity perspective. As CPSs, such as power networks, produce significant volumes of heterogeneous data from multiple sources, it is necessary to also understand mechanisms that can be applied to maintain customer and system privacy. This work therefore also seeks to also focus on processes and research in the area of privacy preservation, as applied to the cybersecurity of this domains. The key aim of this paper is to review the current state of privacy-preserving techniques for protecting CPSs and their networks against cyber threats, with their effectiveness for enabling intrusion detection examined to determine their capability to discover cyber attacks while implementing privacy preservation. One key outcome is to outline the need to develop efficient methods for intrusion detection in a privacy-preserving manner, for protecting data and system components against unauthorised access and identifying cyber attacks, respectively.

The concept and architecture of CPSs and how their components can be compromised using cyber and physical hacking scenarios is discussed in Section II. Privacy preservation and its types, including perturbation, authentication, Machine Learning (ML), cryptography and blockchain, are discussed in section III to demonstrate how they could be applied to protect the original data in CPSs and their networks. Approaches for intrusion detection and their methodologies are explained to indicate how they can be used to discover cyber attacks on CPSs and their networks. Also, the heterogeneous data sources of CPSs and their characteristics are examined to show how methods for privacy preservation and intrusion detection can be evaluated. The Challenges and research contributions of this work are elaborated in Section IV. Finally, The conclusion of this research study is discussed in section V.

II. CPSs AND CYBER THREATS

A CPS incorporates physical and communication technologies and their elements which can be classified as cyber, physical and cyber-physical. A cyber element includes computing and network parts which have no direct contact with the physical world, the physical one the hardware and industrial parts which have no direct contact with the cyber parts and the cyber-physical one devices and systems that link the cyber and physical parts, such as sensors and actuators [1]. A CPS involves the heterogeneous data sources of its physical devices as well as its computing and network systems that generate big data [3], [4]. Due to the complex nature of big data, they are challenging on several levels; specifically, system control and data analytics for monitoring and managing their activities [2], [5]. In a CPS, such as a power system, the role of Supervisory Control and Data Acquisition (SCADA) is to act as an interface for monitoring and managing its operations using standard communication and industrial protocols [6]. However, the CPS's inter-connectivity of sensors, actuators and network devices at different power nodes increases the complexity of the platform ecosystem (such as a power grid) [7], and produces a large amount of data that must be protected against cyber attacks.

A SCADA system is responsible for the remote control, configuration and monitoring of the physical components of any CPS, such as its power systems [3]. Its main role is to synthesize and infer valuable information to improve a system's operational functions for which various computerised models use a Human-Machine Interface (HMI) [7]; for instance, in a power system, SCADA acts as industrial technology which manipulates big data measurements gathered from the input through current and voltage transformers and then forwards certain commands to control other system devices [4]. Its key components are Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) that operate as ports for handling data sent to terminals using some protocols, such as IEC 60870-5-101/104, IEC 61850 and DNP3 that interact with the Modbus TCP/IP model [8].

Apart from SCADA systems, there are other control mechanisms used in power sub-stations, such as interlocking and defence utilities [8]. The intercommunication between physical automation systems and Information Technology (IT) platforms through network connections greatly effects the complexity of these systems and their big data. This complexity is highlighted in Figure 1. As SCADA is more vulnerable to exposure by cyber attackers than other modules because one of its primary functions is to remotely monitor the physical processes in a power system, securing such systems is a complicated and unstable target as new vulnerabilities appear every day, especially given the high sensitivity of control data.

In order to identify potential cyber threats against CPS systems, it is necessary to first understand the basic components of a CPS, including which aspects are vulnerable and can be exploited from advanced and motivated attackers. As shown in Figure 1, a CPS is comprised of a wide range of sensors, actuators and components [9] which manage systems and interact with additional networks (including corporate networks and potentially Internet connections) to undertake CPS operations. CPSs are comprised of physical, control, supervisory control and corporate layers [10]. Cyber-threats have been developed by Cyber attackers who often use advanced and sophisticated attacking methods and tools to breach the security principles of the Confidentiality, Integrity and Availability (CIA) triad [12]. Malicious activities affecting confidentiality include Man-In-The-Middle (MITM) attacks and data exfiltration [13]. There are also integrity attacks that are specific to CPS ecosystems; these include the alteration of CPS components or registers [14], the exposure of the system data by false data injection, data poising, and illegal alteration of data or configuration. This can include data sources including sensor or devices measurements and control commands, and therefore, the normal events of the physical and network devices are modified. While attacks on availability, including Denial of Service (DoS) and Distributed DoS (DDoS). There are also cases specific to CPS in this area, such as the ability to impact the operation of RTUs and PLCs by sending them malformed data. This is a particular issue on older systems that do not have the computational power for rigorous error checking. Such attacks can temporarily or permanently offline or physically damage network elements. This can distort the normal operations of CPSs [15].

To protect CPS devices and data against cyberattacks, there are several areas of research that are being actively explored. These include methods for privacy preservation to keep the system original data to be secure from illegal access, and intrusion detection that can identify cyber attacks that can exploit CPSs and their networks. These are introduced below.

III. PRIVACY PRESERVATION IN CPS ENVIRONMENTS

Privacy preservation is the procedure of safeguarding sensitive information from exploitation by adversaries while still allowing it to be effectively processed on the network [6], [16]. Privacy preservation in CPS first appeared in 2008 in work by Aggarwal and Srikan [17], and was designed to both provide data utility whilst eliminating the ability for adversaries in the network to gain access to the CPS sensitive data storage. As previously outlined, CPS systems generate large amounts of heterogeneous data from multiple sources, and there is therefore a need for developing privacy preservation methods across this data, whilst still allowing existing network security measures, such as anomaly detection, to operate effectively [18], [19]. Given that CPS systems attract motivated, skilled attackers over a significant time period, one goal is the potential access and exfiltration of control system data such as power information, user credentials for further system access, and an understanding of key nodes to cause significant kinetic impact.

There are extensive research studies that have been proposed to maintain the data privacy and security of CPS environments against cyber-threats, specifically for ensuring their confidentiality and integrity [3], [7], [18], [20], [21]. There are multiple ways of classify methods for privacy-preservation, but the most effective and intuitive is to classify according to the purpose of data transformation [7], [16]. This classification has three categories: data generalisation; data transformation; and data aggregation. Generalisation techniques [20] maintain data confidentiality by converting sensitive features into general values. By contrast, transformation techniques [21] modify the original data with new values and use some projection techniques to reduce the data's dimensionality. Aggregation techniques work by [18] splitting the original data into small parts and altering each part's private values with the average of that part. Other studies introduced in [22] focused on data aggregation for maintaining system security and privacy. These techniques are effective to preserve sensitive data from illegitimate access. However data heterogeneity techniques are still nascent in CPS research given the difficulty in effectively managing different data types [17]. Given the large variety of data in CPS ecosystems, this is a non-trivial issue in the field.

An alternate method for categorising privacy preservation techniques is based on their characteristics. The categories in this form are; heuristic- [23], reconstruction- [24],

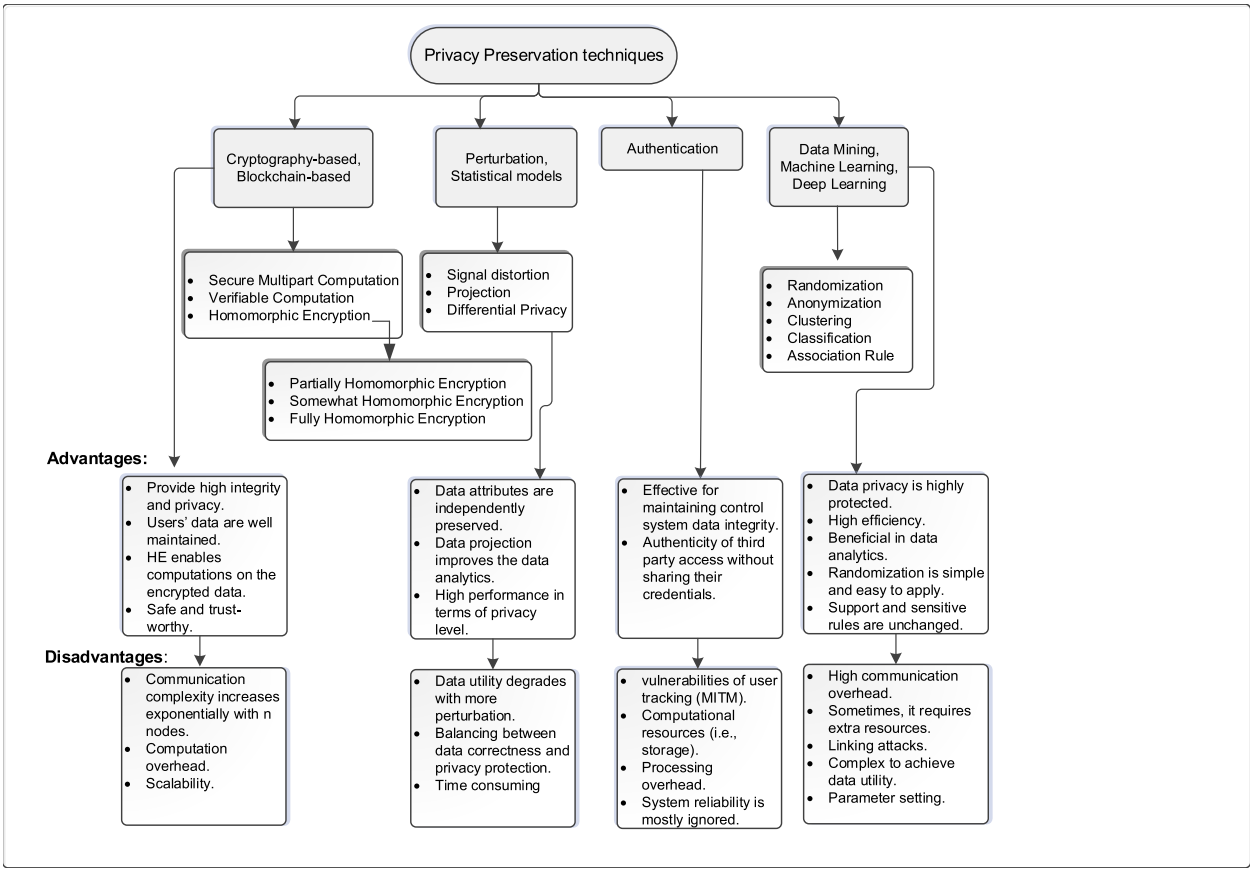

FIGURE 2. Classification of privacy preservation in control systems.

cryptographic- [25] and blockchain-based [26]. These techniques are considered to be effective in data protection, but they still have problems of providing few cryptographic details, incur high computational costs, lack describing data norms if it is raw or aggregated and can't scale well [16], [25]. Several methods based on Data Mining (DM) and Machine Learning (ML) [27], perturbation (i.e., Differential Privacy (DP)) [1] and encryption [28] were deployed to transform, alter, distribute and conceal system information from exposure during processing or transmitting them though networks [3], [29]. In control systems, such as power grids, there are security, privacy and commercial limitations on data, and as such it is not available within the public domain or for research purposes [3], [7], therefore, it is hard to obtain relevant data from different sources.

Therefore, mitigating the cyber and privacy threats attacking CPS ecosystems is still an active area of research, and several research studies have been conducted with the express aim of protecting CPS physical and network confidential data [16], [18], [27], [30], [31]. Encryption techniques are traditionally used to safeguard sensitive data but still they have issue in further analysis and data management while lately Machine learning, data mining and statistical approaches are extensively applied [16], [17], [18], [24].

Figure 2 depicts privacy preservation techniques types, methodologies, advantages and drawbacks to elaborate their contributions and aspects for improvement. The overview of existing privacy-preserving techniques provided below highlights their benefits and limitations based on the ways they protect the data.

A. PERTURBATION-BASED PRIVACY PRESERVATION

The basic concept behind perturbation is to find an appropriate way of transforming the original information in order to hide the sensitive data using different types of transformations, such as projection and geometric perturbations, statistical measures, such as noise, and Gaussian and Markov processes. Preserving data privacy is critical but difficult to achieve in terms of the level of protection (i.e., the amount of sensitive information altered) while maintaining data utility which is the capability to derive useful information from the shape of data, especially good performances of intrusion detection [7]. The more perturbation applied, the greater the difficulty of obtaining useful information from altered data. Achieving a trade-off between the privacy protection level and data utility is a controversial issue that requires more investigation [32]. There are many approaches for

transforming the original data to a new form, as described in the following sub-sections.

1) SIGNAL DISTORTION

Distorting the data of CPSs is an important perturbation technique for providing privacy preservation in different applications, such as power consumption and intrusion detection systems (IDSs), which is achieved by adding or removing some noise matrices from the original data. However as, like any perturbation approach, such changes could affect some important information (i.e., lose data utility), obtaining a balance between data protection and utility is still a significant challenge [7], [32]. Various studies for maintaining the privacy of data-driven devices in different applications, such as that of Kabir *et al.* [33], use the Non-negative Matrix Factorisation (NMF) and sparseness constraint to hide sensitive information. This constraint provides a sparse data representation in which a predefined threshold is set to control the level of data distortion. The authors mention the effectiveness of this approach for preserving and cancelling sensitive information as well as the usefulness of this information when applying DM techniques. However, as using a sparseness constraint with NMF is considered a side-effect of controlling the degree of data sparseness, the parameters used should be carefully specified before data distortion, especially the truncation threshold for completing the distortion process.

In [34], a distortion method that aims to remove some sensitive itemsets is proposed. This method works through the generation of association rule mining from the original data, which leads to sensitive rules being hidden and their support or confidence reduced. In this method, the rules for modification preferably contain fewer non-negative itemsets which could decrease the side-effects of information while mining. Although the experimental results show that this proposed approach can efficiently hide the sensitive rules and reduce their side-effects, thereby achieving the ideal of hiding all the sensitive rules while retaining the non-sensitive ones for mining purposes with no side effects, is difficult. It depends greatly on the user's definition of sensitive and non-sensitive rules and the data context. The more itemsets and sensitive rules, the more processing time is required. Jia *et al.* [35] proposed two protocol schemes for privacy preservation and data aggregation in a smart grid in the face of a Human-factor-aware Differential (HAD) aggregation attack which is responsible for inferring a person's information and exploiting their readings while measuring data aggregation/data metering aggregation. To resist this attack, noise was added to each reading value with no avoiding aggregator to deduce any information about users. However, these methods consume additional time and resources when compared to other methods. This potentially affected the accuracy of meter readings, which is not preferred for billing operations. A new algorithm for protecting data privacy based on NMF and singular value decomposition as a type of matrix decomposition was proposed in [36]. Although it improves the privacy level over that of a single decomposition, its data utility measures are not sufficiently enhanced and the parameter adjustments required increase its computational time.

2) PROJECTION-BASED TRANSFORMATION

The balance of privacy-preservation techniques is in both protecting sensitive information from advanced persistent threats and other adversaries at the same time as ensuring a significant level of information utility. Transformation-based privacy-preserving techniques are one form of process designed to create this balance. The Geometrical Data Transformation (GDT) is extensively used to preserve privacy to an extent, but it does not achieve high levels of privacy [3], [37]. Other transformation-based projection techniques, such as Principal Component Analysis (PCA) and Independent Component Analysis (ICA), decrease data dimensions using the highest variations in the original data [37]. Feature Reduction (FR), which is an approach that removes unimportant or irrelevant and noisy features from a dataset [38], has two stages: Feature Selection (FS); and Feature Extraction (FE) [7], [38]. The former aims to eradicate redundant and uncorrelated features from CPSs big data collections and the latter changes the high dimensions of data to smaller ones. The purpose of both stages is to reduce the computational cost and enhance the process of big data analytics and data privacy by removing unnecessary information [11], [38].

Various studies use projection techniques to protect the privacy of sensitive data [7], [39]; for example, Keshk *et al.* [7] designed a method called Privacy Preservation Intrusion Detection (PPID) for protecting and defending SCADA systems against attackers. In it, the correlation coefficient approach is employed to reduce the number of SCADA features by selecting important information with no data exposure. Then, the EM clustering algorithm is applied to detect malicious behaviours in the SCADA data. An experiment conducted on a power system dataset shows that the PPID is more effective and efficient than the ML techniques with which it is compared but it needs advanced clustering approaches to obtain better detection accuracy. Another projection technique introduced in 2018 [39] for feature learning of big data is the Double-projection Deep-computation Model (DPDCM). In it, the raw data input is projected into two non-linear sub-spaces by exchanging the DCM layer with a double-projection one and then using these two sub-spaces as output to model the features. As this method's parameters require adjustment, a learning algorithm is applied, with cloud computing used to enhance the computational overhead (i.e., for storage and power computations). However, as the cloud suffers from privacy concerns, a fully Homomorphic Encryption (HE) technique used to encrypt the private training objects leads to the PPDPDCM. The results of experiments conducted on two classification datasets and compared with those of the traditional DCM and proposed PPDPDCM show that the latter is more effective and accurate. Although the cloud is used, the model's complexity is still high in terms of computational time and model training. In the study of dimension reduction with privacy preservation in

[40], mechanisms for dimension reduction are theoretically evaluated and then a non-linear reduction based on neural networks (NNs) is used to ensure the protection of data images. This method performs effectively compared with other similar ones but has a learning process that incurs a large computational overhead and has an issue regarding parameter settings.

3) DIFFERENTIAL PRIVACY (DP)

DP is an efficient statistical approach that guarantees unconditional privacy as no assumption is made about an attacking adversary's knowledge. This ensures that certain perturbed data computations do not change greatly when the original data are updated while data privacy is retained even after other parties are accessed [1], with the results of any computations indistinguishable regardless of the original records in the dataset. Its concept is first introduced by Dwork in [41] for privacy preservation in different domains. Many of the mechanisms used to preserve DP at a certain level are explained in the following.

- **Laplace mechanism (-DP)** - achieves an intrinsic trade-off between the privacy and accuracy of outcomes by adding additive noise from a Laplace distribution [42], [43] that is inversely proportional to that of the database's users. In other words, achieving the same privacy protection for more users requires less noise because of the smaller value but greater privacy protection leads to less accurate outcomes.
- **Gaussian mechanism ((,d)-DP)** adds additive noise to numeric queries and Independent and Identically Distributed (i.i.d) entries. It could be better to apply it than the -DP although it achieves less privacy. Nevertheless, an analysis of its performance is simple because any linear transformation of a Gaussian random vector remains Gaussian, such as in linear systems [42].
- **Exponential mechanism**– is a more general mechanism with a scoring function that is selected randomly. It is often chosen based on corresponding queries as it accomplishes the -DP by reporting a query in a Probability Density Function (PDF) [43]. Although it is not limited to numeric queries, it is not easy to find aPDFs in a closed form to a multivariate distribution.
- **Hybrid mechanism**– while the previous mechanisms are relatively straightforward as they have to calculate only one value (i.e., sensitivity) in simple queries, more complicated ones need to be decomposed into multiple simpler ones for easy calculations.

Due to the purely mathematical computations in DP, it has been widely applied as one of the major privacy approaches for CPSs in recent years. In [44], Uhlerop *et al.* apply the -DP to publish a genome's aggregate data and secure them from attackers to identify a person using the DNA mixture. Additive noise is added to the confidential data to be released, with a -DP and utility level achieved in a promising way. However, the increase in the amount of data and sparsity of the released data create an issue for securely publishing genome data in terms of data privacy and utility. In 2015, Chen *et al.* [45] proposed a Multifunctional Data Aggregation (MuDA) approach for preserving an individual's data while managing the consumption of electricity in a smart grid. In it, several statistical functions are computed based on user data to achieve a variety of services, such as system initialisation, with the aggregation reported. Also, it can withstand differential attacks, with simulations of it demonstrating its efficiency in terms of computational complexity and communication overhead. However, it requires some assumptions for better understanding and implementation, and its results are compared with only those of one popular method.

A similar secure data-aggregation scheme called Differentially Private Aggregation with Fault Tolerance (DPAFT) in [46] applies both DP and fault tolerance. In it, a constraint relationship based on a key-exchange protocol is used for aggregation to support the fault tolerance that DPAFT can maintain against strong attacks. The different phases implemented are system initialisation, data aggregation request, data aggregation request relay, user report generation, privacy-preserving report aggregation and secure report reading. Although the extensive experiments conducted reveal that it is efficient in terms of storage and computational costs and is capable of achieving both privacy and data utility, its communication overhead and data confidentiality and integrity are not considered. Very recently, Guan *et al.* [47] introduced a data-aggregation scheme for privacy protection based on fault tolerance and aggregation in which the data privacy of a smart grid can be preserved by using secret sharing and setting a threshold to resist a differential attack. It demonstrates reasonable efficiency and a low error rate but has an issue regarding the parameter setting (i.e., threshold) and its computational complexity is considered high as it increases exponentially with more smart meters.

The schemes in [45] and [46] are similar, with the main difference between them their cryptographic methods. Lin *et al.* [48] designed a scheme for tackling privacy preservation for a Body Area Network (BAN) using DP, where the noise is added to the BAN's big data to provide adequate interferences. The feasibility of this processing system for big data is ensured by dynamic noise thresholds rather than ordinary noises. Their results demonstrate the capability of this scheme to generate sufficient interferences to resist an attacker targeting a specific user's sensitive data. However, the threshold values need to be carefully quantified for better privacy protection and using such noises can affect data utility.

A systematic approach aimed at identifying the data utility level in an attempt to characterise the sensitive critical data needing to be protected and releasing the unimportant data without sacrificing control by analysing the 'no free lunch privacy principle' is proposed in [84]. In it, the original data are filtered to comprise the least confidential data and then an adaptive local DP is applied to study optimal control

versus privacy protection. In [49], Zhang *et al.* present a battery-based DP-preserving scheme and then extend it to two cost-friendly techniques for preventing meter readings from exposing a customer's electricity consumption. Although the experiments show DP and cost savings under static and dynamic pricing policies, changes in the DP's parameters can cause a loss of privacy. Ni *et al.* [50] proposed a new privacy-preserving clustering technique using DP to tackle the problem of balancing between data privacy and the availability of clustering results. In it, the multi-core point method is used at the most remote location from the clustering results. While this technique shows that the clustering is accurately affected by scaled data, the parameters used affect its accuracy and privacy budget.

B. AUTHENTICATION-BASED PRIVACY PRESERVATION

Advances in the capabilities of communication and Internet technologies have introduced additional security and privacy challenges, such as (i) the confidentiality and integrity of control system data and (ii) system and user authentications. One popular authentication approach (i.e., single sign-on) called OAuth [51] can provide ways of checking the authenticity of a third-party's access without sharing its credentials. Other methods used extensively over web services are the OpenID [38] and Secure Assertion Markup Language (SAML) [52], where the former allows web users to sign on to various web services using one digital identity while the latter provides the necessary identity credentials in XML. Despite the above approaches being extensively used, they raise many security concerns, such as potential vulnerabilities to attacks that track users (e.g., MITM ones) [49] and the resources required to store these data. Several researchers have tried to address these challenges; for example, Das *et al.* [53] proposed a unified key management theoretical framework for protecting a smart grid user's data by working through multiple communication layers. In it, the Extensible Authentication Protocol (EAP) is employed assuming that smart meters have low-cost wireless devices. However, it could increase a system's overhead by repeating attempts to obtain peer authentications for different protocols.

In another authentication technique introduced in [54], a key management framework is applied to meter infrastructures at three different transmission modes, unicast, broadcast and multicast, based on a key graph. Since it was designed for different modes, key generation, refreshment and distribution policies are needed in each mode for message authentication and encryption purposes. However, its storage and time costs are considered high due to the requirement to store related data, such as keys and data values, and process key management at different modes. Also, in [55], an integrated authentication and confidentiality protocol that offers privacy and integrity for a metering system in a smart grid through a mutual authentication of messages among smart meters and gateways is proposed. For each smart meter, the reading message is encrypted and aggregated with the current message after its validation. Finally, the resultant message is forwarded to the next level/node until it reaches the collector end for further use by a control system. However, messages could be delayed or clash with an increase in the number of hops/nodes and many of the device's computations are consumed. Xu *et al.* [56] proposed a technique based on virtual-reality methods to avoid the need for an actual face to be authenticated which could breach user privacy. Despite its effectiveness for domain-specific data privacy, its utility for social networking is ignored.

Several studies introduced in [22] maintain security and prevent privacy leaks by focusing on data aggregation. In [57], Chim *et al.* suggest an approach for keeping a user's daily electricity usage safely away from third-party invaders by applying the concept of the customer blindly signing his credentials for use later when acquiring more power. Although its performance shows that it is feasible in terms of time and the likelihood of a lack of collisions, it requires a prior signing operation and memory resources as additional storage for customers signatures. Chim *et al.* [8] attempted to solve issues of the authentication and privacy of a user's power information by aggregating the messages sent to a control centre to decrease the capacities of traffic packets. Also, the encryption methods that keep users identities secure while requesting more or less power perform reasonably well. However, this is not sufficient as the assumption that the encryption keys are difficult to hack requires more investigation.

In [58], a proposed cloud-based authentication scheme using a modular exponential technique firstly encrypts a tag's information regarding communications between IoV and radar. Then, the anonymity of the tag is developed as an efficient way of ensuring data privacy by protecting itse information from malicious actions. Compared with other protocols, it shows that it is effective and reliable in terms of having a lower computational overhead and fewer communication interactions. Some authentication work is based on access control, such as in [59] where a self-adaptive access control method for securely viewing patients records in both normal and emergency cases is proposed, with a de-duplication method used to save the storage of identical medical files. Firstly, the medical data are encrypted according to an access policy and then the method applied based on a break-glass control one. The experimental results show that this methodology is efficient and practical but that the time it consumes increases with the sizes of the attributes.

C. DATA MINING AND MACHINE LEARNING BASED PRIVACY PRESERVATION

DM and ML are usually used to deduce and conclude patterns and inferences from a collection of data which could compromise CIA [60]. As exchanging sensitive and confidential information for data analysis and publishing purposes requires protecting the data from disclosure, Privacy-preserving DM (PPDM) and Privacy-preserving ML (PPML) methods for guaranteeing a high level of privacy while maximising data utility for analytical and mining purposes are

essential. In other words, using PPDM or PPML for data analysis and inference goals without losing the privacy of sensitive and personal data is very important [27]. Currently, there are many PPDM and PPML methods, such as randomisation, anonymisation, clustering, classification and association rule mining, as discussed in the following sub-sections.

1) RANDOMISATION-BASED PPDM/PPML

Randomisation approaches are applied mainly in the collection phase as the collector is assumed to be untrusted, with the original data distorted by noise to build new representations of the authentic them. Therefore, although the original data cannot be recovered, the aggregate distributions can be used for mining and inferring operations [61]. They could be randomised using additive [21] or multiplicative alterations [62], where the former adds randomised noise-generating data distributions for DM and the latter uses random projections or rotations of noises with a known distribution. While these approaches are effective in the data collection stages and do not need further resources, their data utility is degraded/limited and requires a large amount of noise-masking original data values. Randomised responses and noise perturbations assist in achieving privacy preservation with knowledge inference [16].

2) ANONYMISATION-BASED PPDM/PPML

In the publishing phase, protecting individuals information (i.e., personalised privacy) requires data holders and publishers to clear the identification data because they could compromise individuals sensitive and personal data [41]. Two general types of disclosure are identity and attribute. The first relates to hacking the unique identifiers of individuals while the attribute one can be inferred through the available data. Several techniques are used to preserve identity privacy, such as k-anonymity, l-diversity and t-closeness. One or more data-sanitising operations, such as generalisation, suppression, anatomisation and perturbation, can be applied in privacy models. K-anonymity is a simple and efficient approach for identity protection as it can prevent any association between individuals and related sensitive values by modifying the original data (D) so that the identifiable attributes of a dataset are not considered different from at least k-1 records. Data generalisation and suppression are used in k-anonymity to replace the sensitive values by a general one for privacy purposes. In [63], an anonymisation technique for minimising information loss (IL) during the process of data publishing is proposed.

To satisfy the requirements of data experts, two algorithms that provide accurate measurements of the IL and effective data anonymisation explore the largest portion of a problem. The experimental evaluations using click-stream and medical data show more reliable answers to queries than some other methods. In another effective approach for the privacy preservation of personal data proposed in [64], the data are transformed into a k-anonymous shape with their utility using a reference to differentiate among their analytical characteristics. The experimental results reveal that this technique can protect the data patterns extracted from mining algorithms. Although anonymisation methods are simple, they do not consider that each record represents one individual and, occasionally, ignore the sensitive attributes while anonymising the available data which might disclose private information during the de-anonymisation process.

Wang *et al.* [65] introduced a novel notion of Differentially Private K-anonymity (DPKA) based on the DP and k-anonymity perceptions to support the privacy of queries in location services such as mobile devices. A pool of k-query interests is defined, including $k - 1$ dummy ones, with the selected and dummy ones submitted together to the location provider which cannot differentiate between them. Therefore, DP is employed using a probabilistic inference, where the protection level is achieved if the posterior probability of any two queries is sufficiently close and controlled by an privacy budget. For two cases in this work, the necessary 0-DPKA and more general -DPKA, if the first one is not achieved, it is proven that the -DPKA is equivalent to the transformed 0-DPKA. Four real datasets and synthetic Zipf distributions are used for simulation tests which demonstrate this method's effectiveness in guaranteeing the privacy of queries. However, a careful setting of the parameters which can affect the privacy budget and data utility is required while the integration of DP would increase the time costs.

The l-diversity approach is used to maintain the diversity of sensitive attributes, the inferences of which k-anonymity fails to hide [27]. In it, a set of entities in which there is at least a l value for each sensitive attribute, a more solid notion is entropy l-diversity as it could be extended to numerous sensitive attributes through more anonymisation [66]. L is a privacy measure like k, with a higher l leading to greater privacy but possibly decreasing the data utility. However, it does not include the data distribution for each value which can result in privacy leakage if the sensitive values have a skewed distribution. To solve this problem, in another approach called t-closeness in [67], a threshold (t) is preset as the upper bound for checking the closeness of the distributions of the sensitive values in the original and anonymised data. Privacy preservation in the data-publishing phase using the above mentioned techniques, that alter the original data to keep the identities of the data and user secure, provides great privacy control and data utility as the publisher can access all the data. However, these techniques perform many processes which increase the overhead and the data holder (third party) must be online and available most of the time.

The authors in [68] improved on their previous work in [69] by proposing a privacy-preserving data-publishing framework using k-anonymity which has better data utility than comparative methods as it customises k-anonymisation to the interest of data users. Instead of linear features, non-linear ones are used in the evaluation to assess this extended framework. Although, experimentally, it demonstrates enhanced data protection and utility, the IL in the pre-sanitised data increases when the level of k-anonymity is higher. Also,

the computational overhead increases with increases in the labelled data and features of data records. A novel Restricted Sensitive Attributes-based Sequential Anonymisation (RSA-SA) approach for preserving data-stream publishing and achieving the diversity of both semantics and sensitivity is introduced in [70]. Unlike the previous approaches mentioned, it is a simple anonymisation process with tuple-by-tuple noise addition. It can minimise the delay time and IL as well as maintain data usage as the exact value (QID) of each tuple is released. However, its average processing time increases with large data streams and some sensitive attributes.

3) ASSOCIATION RULE-BASED PPDM/PPML

An association rule-mining method aims to find the relevant relationships among a dataset's elements which are expressed as rules associated with their probability of occurrence [16], [71]. Any rule is a strong one if it satisfies the thresholds of minimum support and confidence [27]. As some rules could release confidential information about the original data, privacy preservation based on hiding these rules is essential, with its main target to mine all non-sensitive rules and not reveal sensitive ones [16]. Some techniques [16], [71], [72] propose certain solutions for guaranteeing the hiding of sensitive rules while maintaining non-sensitive ones ready for processing; for example, Lai *et al.* [72] developed a semantic solution for outsourcing rule mining and data integrity as attackers could breach data servers to obtain sensitive data and inject false data into the results to semantically expose the data. Assuming that the data are categorical, this solution is capable of sounding an alarm regarding any false injection into the mining results.

Iqbal *et al.* [73] used a Bayesian network-based centre tendency and a priori algorithms to differentiate between sensitive and non-sensitive rules to protect the former, with the K2 algorithm applied to create the Bayesian network's nodes and improve the accuracy of preserving the privacy of the XML rules. A heuristic-based algorithm for enclosing certain sensitive association rules called the Modified Decrease in Support for the Right-hand Side (RHS) items in Rule Clusters (MDSRRC) is proposed in [71]. Multiple items are used in the consequent (RHS) and antecedent (LHS) items of rule clusters by which the drawbacks of the DSRRC rule-hiding algorithm [74] are overcome as sensitive transactions are chosen according to defined criteria and then modified. The experimental results demonstrate its better efficiency and capability in managing the database than the DSRRC algorithm.

The intensive research conducted over decades reveals that existing privacy-preserving techniques facilitate good data protection. However, they still suffer from major incompleteness because of their high computational and communication overheads, scalability issue when the volume of data increases, lack of resilience against, and capabilities to detect, some attacks, and poor levels of integrity and data utility, with some, such as authentication and encryption techniques, requiring unique identities to create keys or having complicated key management. The connection between personal data and personal identification should be eliminated to prevent any hacker inferring confidential information about users from their identifications.

4) CLASSIFICATION-BASED PPDM/PPML

Classification is a form of supervised learning by a classifier that is first built in the learning phase based on an amount of data called a training set, with the class labels of undefined data then identified and called a testing set [16]. In other words, classification is a mapping function that transforms a record of some attributes into a corresponding class label which can be a mathematical equation, decision tree or rules [27]. Evaluating such a classifier depends on the accuracy of correctly classified records using a dataset divided into training and testing sets. During the data-release stage, it is essential to preserve and hide confidential information while classification mining is performed, as illustrated in the literature [16], [75], [76]; for example, Bi and Zhang [76] proposed a privacy-preserving classification algorithm based on a perturbation scheme in which a random perturbation matrix is applied to different data types such as character, Boolean, numeric and classified. The experimental outcomes show the effectiveness of this method in terms of its privacy level and mining accuracy but its computational cost is greatly impacted. In a proposed outsourced privacy-protecting framework for classification, the classifier can be securely trained using the data available on cloud servers encrypted with different keys using a semi-honest model based on HE without a clear interaction between data providers and evaluators. However, it incurs a high computational cost and complex communication.

5) CLUSTERING-BASED PPDM/PPML

Clustering is the process of apportioning a collection of data into groups based on some measures (i.e., similarity ones) in which data in the same cluster are more similar than those in others. Several research studies carried out to apply clustering algorithms for privacy preservation include vertically and horizontally partitioned data models. In the latter, the data collected from different organisations with the same set of features/attributes are divided into non-overlapped horizontal portions while the former divides the data into different sets of attributes which have the same number of transactions.

Many studies apply clustering as pre-processing for privacy protection, for example, He *et al.* [77] proposed a clustering-based anonymity approach in which all the data records are clustered into correlated portions using a k-means algorithm, and then expanded it to the l-diversity technique. The experimental results show that data utility is improved in terms of IL but increasing the data dimensionality negatively affects both it and the computational cost. The authors in [78] used a single-pass k-means clustering algorithm before the data are anonymised which protects an individual's personal data from disclosure by unauthorised parties. To maintain

data confidentiality, generalisation and suppression processes are implemented. In [3], Fahad *et al.* firstly apportion the data according to their types, then cluster them based on similarity measures (distance) and, finally, replace the assigned values of the clusters to achieve data perturbation. This framework shows experimentally that it is effective for simultaneously dealing with different data types and changing the original data and data utility. However, the significance of the given attributes is not sufficiently considered.

D. CRYPTOGRAPHY-BASED PRIVACY PRESERVATION

Securing computations in several applications could pose privacy concerns as they allow one or multiple parties to share and execute certain functions and analyse data inputs [79], [80]. A public key is shared among users/peers who exchange an encrypted message which, as well as accessing the message content, discloses the system's privacy and integrity. Various researchers use cryptographic mechanisms as a conventional way of guaranteeing system security and information privacy [80]; for instance, Kalogridis *et al.* [81] introduced a unified approach that aims to address the security and privacy issues of smart meters by analysing different security solutions and fusing them to be associated with the tightly correlated system components. In particular, the analysed solutions are categorised as three main components (i.e., communication, computing and system control) and then security solutions are mapped, with the most appropriate defense mechanism selected.

Encryption schemes can be symmetric or asymmetric and both try to transform readable data into an unreadable form (plain text into ciphertext). Symmetric encryption uses the same key for two parties and the asymmetric one a public key for encrypting the text and a private one for decryption. Although these schemes seem to be efficient, their biggest problem is how to trust the keys through the encryption process. A common attack that can compromise keys is a MITM one that can render encryption useless. In [82], a Public Key Infrastructure (PKI) scheme for securing devices while exchanging messages between users on two edges is proposed. It binds public keys with user identities while the registration authority processes and applies attestation protocols, firewalls and common authentication to restrict the impacts on disclosed devices.

There are many cryptographic techniques for securing and protecting a large amount of data on the cloud or control systems. The three major approaches that can achieve data privacy through computations in a scalable and lightweight manner [83] are: Secure Multiparty Computation (SMC), Verifiable Computation (VC) and Homomorphic Encryption (HE). these are explained as follows.

- **SMC-based privacy preservation**: is an encryption protocol used in almost all encryption methods with different data analytics such as a distributed PPDM [80], [83], with two common techniques for MC garbled circuits and secret sharing [84]. However, the various studies of SMC have some limitations as their approaches could be attacked by several threats and they have high communication complexity that grows exponentially with an increasing number of parties.
- **VC-based privacy preservation**: is an approach that permits data holders to inspect the security of computations. An intermediate prover is a powerful entity responsible for obtaining the requirements for computations, checking their correctness and then passing the results to other parties [79]. Compared with SMC and HE approaches, VC can guarantee data integrity, but not data confidentiality, while performing computations which is essential in the presence of untrusted parties and adversaries.
- **HE-based privacy preservation**: the concept of HE was first introduced by Rivest *et al.* [85] because, although encryption is usually used to preserve the confidentiality of sensitive data, as conventional encryption techniques cannot operate on encrypted data, the data should be decrypted first [80], which means that users/parties cannot perform or use available services without sacrificing their privacy.

HE is a special type of encryption scheme that allows a third party (e.g., cloud, SCADA control) to conduct certain operations on encrypted data without the need to decrypt it in advance, such as is required by RSA and Paillier. In particular, it can preserve the format of encrypted data and computational features in which the original data (i.e., unencrypted data) are not revealed to third parties during computations. It can be categorised as three schemes based on the number of functions permitted to be performed on cipher data. The first, Partially HE (PHE), consists of only one type of operation (addition or multiplication but not both) and is allowed for any number of users. The second, Somewhat HE (SWHE), is a type of operation (addition or multiplication or both) for only limited usage. The third, Fully HE (FHE), provides any number of operations for any amount of usage. Because of the limited operations of PHE and SWHE as well as the increasing sizes of ciphertexts in each operation, they are not often used in real applications. In contrast, FHE supports the conduct of different arithmetic operations at the same time.

HE-based privacy has been extensively studied, primarily due to its homomorphic features for executing some arithmetic operations. There are several encryption techniques which support different homomorphic features, such as multiplicative homomorphism (RSA) [86]), additive homomorphism (Paillier [87]) and the recently proposed fully homomorphic scheme [88] for complicated functions. However, most HE techniques are still impractical because their computational overheads affect their efficiency; for instance, in [89], Sushmita and Amiya propose a framework for simultaneously aggregating the readings of a smart grid and protecting customers privacy in which an additive HE technique is applied. They use attribute-based encryption to support access control according to the stored data. One of

the obvious drawbacks of this approach is assuming the trustworthiness of the RTU that controls these operations. For the authentication of smart meters [90], the homomorphic hash function is applied using a non-square matrix to reduce the number of computations involved in smart meters. Although the probability of success in attack scenarios is used as a theoretical measure of its effectiveness in terms of security, the performance of the proposed method regarding execution time and memory usage is influenced by the security parameters defined.

Recently, in [91], an Extended Privacy-preserving Demand Response (EPPDR) scheme that uses HE for demand aggregation and efficient responses achieves privacy preservation and user confidentiality in the local area. Then, an adaptive-key evolutionary technique secures a user's session and private keys. An analysis demonstrates the efficiency of this scheme in terms of computational and communication costs compared with those of peer methods. Tassos and Awad [92] proposed two decentralised protocols for aggregating the measurements of smart meters, with one based on symmetric cryptography and the other on public-key encryption. They attempt to prevent untrusted entities from determining certain consumption patterns as this could lead to breaching a customer's privacy and profiling his behaviour. An evaluation shows that both protocols are scalable but only with respect to their limited memory and communication requirements. There are two other lightweight privacy-preserving data-aggregation schemes [93], [94] for handling the privacy of customers and data integrity. Both use asymmetric HE, with a key-exchange method (Diffie–Hellman (DH) or Elliptic Curve Diffie–Hellman (ECDH)) in [93] and an aggregate-signature scheme in [94]. The experimental analyses show their superiority in maintaining data integrity and users privacy with lower transmission overheads than comparative schemes but they still suffer from high levels of complexity and transmission overheads.

In [93], the ciphertext size increases linearly with the security parameters while, in [94], static secret keys are used so that forward and backward secrecies canot be disclosed, with these schemes also considered forgeable. A comprehensive review of HE techniques is provided in [80]. A practical framework for anomaly detection and privacy preservation of cloud data (i.e., sensor data) which applies a HE scheme over data processing to ensure a system's security and privacy is proposed in [79], in particular, Domingo-Ferrer's additive and multiplicative privacy homomorphism technique before the communication and processing stages. The experimental results show that it outperforms other comparative methods for the original plaintext and ciphertext in terms of detection accuracy. In another HE research study in [95], which is an extension of that in [96], an integer-based scale-invariant FHE scheme is proposed but with a new and interesting property called message-space hideability in which a message is hidden from the public key. Although it is efficient with large integers and satisfies the security requirement, HE often incurs a high computational time.

An approach for data integrity based on lightweight authenticated data using an encryption methodology for privacy preservation is proposed in [97]. It has three main entities that aim to act as prover and verifier while retaining evidence that enables the integrity of data streams. In more detail, a data user initiates a query to the cloud and, once the result is ready, its integrity is verified by evidential information transmitted from a secure channel. Its overall performance reveals that its computational overhead does not increase as much as those in the original methods but its data utility cannot be retained as there are no further analysis is conducted on the ciphertext. In [98], a method based on a parallel FHE algorithm which works on floating-point numbers, not only integers, and can eliminate security threats using any out-of-order ciphertexts is proposed. As homomorphic algorithms have low efficiency, this scheme uses a MapReduce platform through data blocks. The experimental results show that its speed ratio is better than those of traditional techniques but the time consumed by Reduce can increase with large volumes of data.

E. BLOCKCHAIN-BASED PRIVACY PRESERVATION

A blockchain, which was introduced at the beginning of the 1990s by Haber and Stornetta [99], is based on the theory of chaining time-stamped rows using cryptographic algorithms, i.e., the hash functions recently used in Bitcoin cryptography [100]. In a blockchain, an input such as a message can be mapped to another message with a set of n bytes. A Blockchain contains each block's metadata (the time stamp and hash value of the previous block) and payload (original data), with the time provided in each block usually represented by a discrete value that regularly increases as more blocks are added [101]. It is considered a public distributed and uncorrupted ledger database [101] with the potential to successfully achieve data integrity and reliability. Simply, transactions are chronologically recorded in a chain of blocks in which any participant can keep track of them without any central recording [26]. Since a blockchain is characterised mainly by its trustworthiness, persistence, decentralisation and anonymity [102] to achieve the integrity and security of an application, there can be multiple copies of it through different participants (i.e., computer systems). The participants form a network of nodes, each of which represents a computer system, with any change in the blockchain made by a participant sent as a duplicate copy to the others [102]. For more details, the key elements [26], [103] that characterise a blockchain are discussed below.

- **Decentralisation**: all involved parties (i.e., nodes/ participants) have the authority to control/add, change or verify the appended transactions instead of them being centrally coordinated (peer to peer) [26]. In a decentralised blockchain network, each user is considered a miner joining the consensus process and validating every newly provided transaction to expand the chain [101].

This feature reduces the risk of a single-point failure or data breach.

- **Trustworthiness**: data transactions (i.e., records) are continually verified and validated [26], [102], with their integrity achieved using a cryptographic mechanism (hash) created for each one which is kept in a block over the blockchain which guarantees that it cannot be altered or updated (persistence).
- **Immutability**: validated transactions recorded in the blockchain are immutable as any alteration to them requires the other nodes to verify and mark them as valid blocks [26], [103]. Also, the consensus process is employed later to maintain the integrity and validity of the blockchain's records whereby the consensus protocol at each node should generate the same corresponding output according to its rule (level of confidence) [102]
- **Contractual**: each miner applies a certain consensus process to ensure the precision and synchronisation of any monetary actions and includes some defined rules regarding the status of the data [103].
- **Anonymity**: in the blockchain network, the main element to be anonymised is the participants (miners) in order to achieve trustworthiness among them, with only its address required [26], [103]. Therefore, different and changeable public keys can be used to preserve the anonymity and privacy of each miner. This is a very attractive area of research in various applications not only for users but also data transactions to keep a system secure and privacy preserved.
- **Transparency**: this is the routine for examining the data in the same miner in each time interval for self-auditing purposes and to prevent corruption [26].

1) ARCHITECTURE OF BLOCKCHAIN FOR PRIVACY PRESERVATION

A blockchain is a series of blocks appended continuously by the network's nodes/participants (called a peer-to-peer network (P2P)) which are linked and secured by various cryptographic mechanisms and can offer privacy preservation for CPSs and their network nodes [103]. Each node in the network has the same authority as there is no central coordination (no central server), exchanges information with other nodes and verifies and synchronises data transactions and blocks [26], [103]. For each block in the chain, a pointer links it and its ancestor in a chronological order using a hash value it generates, with the first block known as a genesis one as it has no ancestor/parent block.

During the growth of a blockchain, the hash functions should follow several security requirements [104]. Firstly, a first-layer resistance denotes the struggle to recover the hash values, that is, a hash value (h) requires a complexity of $O(2n)$ to estimate an x input, where $H(x) = h$ and, secondly, a second-layer resistance indicates that an input (x) has a hash value with $O(2n)$ complexity for calculating the values $x_0 = x$, where $H(x_0) = h$. Finally, a hash-collision resistance requires a complexity of $O(2n/2)$ to obtain either

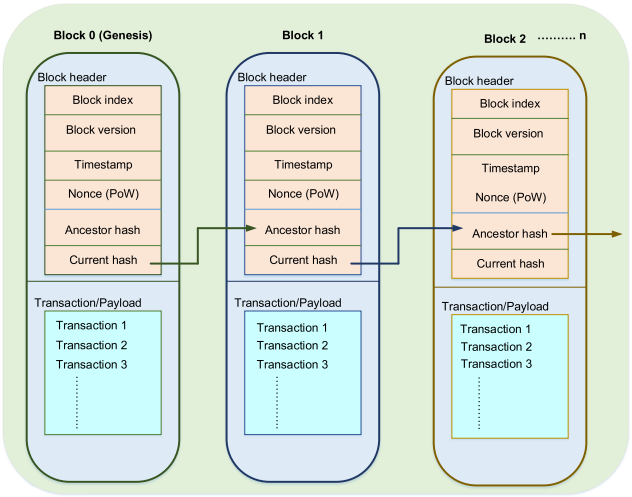

FIGURE 3. Elements of blockchain.

of the previous two hash values. As shown in Figure 3, each block encompasses a set of features/attributes, including an index, block version, ancestor hash, current hash, time stamp, transactions (data) and a nonce (i.e., proof), as described below.

- **Block index**: contains a sequential number for each block in the ledger/chain.
- **Block version**: is a set of rules for validation.
- **Ancestor hash**: is the hash value of the previous block in the chain. The hash function can be defined as a transformation method which takes an input sequence and returns a hash value that will be different if a single bit in the input sequence is changed. Hashing is extremely important in blockchain technology as it assures that no-one can change any data in the chain without providing the ledger with an updated copy of this change, thereby improving its trustworthiness and security.
- **Current hash**: is the hash value of the current block.
- **Time stamp**: is the time taken for the block message to be generated (in seconds) which can help data tracing and synchronisation as it also increases the security of data modifications made by different users.
- **Transactions:** are the data stored in each block which depend mainly on an application that uses a blockchain, such as finance, contracting and services ones, with the amount allowed to be stored based on the block's size.
- **Nonce**: this is also known as proof (i.e., consensus methods), with its value calculated for each block's hash (from 0 which increases for each block generation). It is a set of rules used to generate a new block and verify a chain. It is called a digital signature and different methods, such as symmetric cryptography, have been used, with encryption one of the main ones for spreading data over a network.

A digital signature can be identified as a two-step process of [26], [102] signing and verification, for which each participant in a P2P network uses its public and private keys.

Its private key is kept confidential and used to sign data transactions while its public one is available for later use by other participants/users to access the signed transactions and approve their correctness. For a better understanding, the following is an example of how blocks are generated, signed and verified. Assuming there is a network of ten users (U1, U2…, U10), if U1 has a transaction to add or alter, it needs to sign this transaction, generate the hash value for it and encrypt it using its private key. It then sends this transaction to everyone in the network and provides a copy to the ledger. If U3 receives this transaction (data and hash value), using U1's public key, it decrypts the encrypted hash and compares it with the one previously received from U1. If they are the same, U3 verifies this transaction and continues, otherwise the transaction is not accepted as an addition or alteration. As previously mentioned, there are different methods for consensus which are discussed in the next sub-section.

2) CONSENSUS METHODS AND BLOCKCHAIN-ENABLED PRIVACY

The idea behind consensus comes from the Byzantine General (BG) problem [105] in which finding a consensus among some of the nodes in an untrusted environment is attempted. The problem begins when many generals want to attack a city and others to retreat. Since an attack should include all the generals, it is important to reach a consensus. The same challenge occurs with blockchain technology when the environment/network is distributed without central control and no trust among the participants is required. The two most popular consensus approaches are described below.

- **Proof of Work (PoW):** this approach, which is used for blockchain authentication, focuses on discouraging DoS attacks and network spams in which a device's computational time is affected. To add transactions, a complicated computational procedure is required as the dominant node should calculate a hash value equal to or less than a predefined threshold (nonce). Each participant in a decentralised blockchain network has to continuously estimate the hash values until the required one is reached and then broadcast it to the other participants. In this process, the participant nodes are miners and the consensus strategy (PoW) mining as different valid blockchains could be generated simultaneously. Sometimes, a block later becomes an authentic one that could not have been tampered with but the problem of this strategy is the computational time and resources it consumes.
- **Proof of Stake (PoS)**: this approach allows a participant or miner to work on a block's transactions based on trust [26], [106] which is determined by the users with more currency or data. As, when these users have many transactions, it is possible for them to assault the network [26] and any participant should hold at least a base of cryptocurrency [26], [102] to be considered a miner and/or validator. The PoS is considered to save more energy than the POW [102], [107] as its users are required to provide proof of ownership instead of finding a nonce.
- **Practical Byzantine Fault Tolerance (pBFT)**: this is a common consensus protocol presently deployed on the Hyperledger Fabric platform [108]. It is usually applied in a private blockchain as trustworthiness is embedded between participants unlike in the PoeT, PoW and PoS protocols. Also, it is energy-efficient for conveying a high quantity of transactions without the requirement to optimise the network to involve a large number of participants; for instance, its algorithms in blockchains are divided into two groups, general active and passive replications. A basic replication is selected from the active ones which receive transactions from a consumer and transfers them to the other replications. This process has four phases: pre-preparing; planning; agreeing; and responding. In the first stage, all the transactions are referred to mainly as general active replications, each of which signs and exchanges its transaction with the other replications. In the response phase, all the active replications provide their responses to the main one with proofs of consensus. Finally, the main one collects all the signed transactions and places them in a stack [109].

Privacy preservation has attracted major attention to blockchains although many methods have security aspects of pseudonymity and tamper-proof techniques. Using asymmetric-key cryptography to numerically sign transactions and approve the right participants does not promise privacy or guarantee anonymity as all transactions are visible [110]. Recent studies have shown the practicality of de-anonymising attacks using cryptocurrencies [111], [112]. Biryukov *et al.* [113] linked an encoded transaction to real participants by recognising heuristic groups in order to classify digital wallets and other previously acquired services. Many approaches developed to improve blockchain confidentiality and anonymity can be categorised as two types: mixing services; and zero-knowledge proof. The former provide the fund transfers of a client and randomly exchange them for other clients funds to disclose their ownership. Zero-knowledge proof-based methods use the cryptographic accumulator to verify transactions with a digital signature so that clients can swap random funds. However, they lead to high computational costs and expose transaction funds. To handle these issues and further enhance the anonymity of transactions, Zerocash [114] is considered.

Although private and consortium blockchains achieve greater privacy protection than public ones with less exposure to cyber attacks, their integration in a single CPS would make them less efficient and exposed to a single point of failure [115]. In contrast, public, distributed and decentralised ledgers suffer from untrustworthiness among network participants. Therefore, CPSs are generally hesitant to share information or article intrusions due to anxiety about data

confidentiality and integrity as it is relatively difficult to quantify the reputational levels of untrusted individuals. The capability to maintain data storage with a supervisory capacity can incur computational overheads in terms of time and cost [104], [109]. Corporations are progressively using CPSs to scale their storages of various datasets as security and privacy are still challenging. Furthermore, blockchains work in various jurisdictions where it is difficult to guarantee compliance with all the rules. Therefore, a decentralised privacy-preserving architecture would enable compliance with procedures and the control of costs and policies related to a CPS.

Securing CPSs, especially modern power systems, against cyber attacks has received a great deal of attention over the last few years [116]. The interconnection of their objects (such as sensors and actuators) as well as their communications with the Internet (Internet of Things (IoT)) and ITs increase their complexity as they require the control and data management of multiple users at one time [117]. A CPS is considered an IoT because many of its objects are connected with its communication with the Internet which could increase an outsider's capability to violate its systems [118], including its SCADA control one which could be threatened because its primary responsibilities are to monitor and control the CPS.

Malicious or advanced adversaries of external sources in CPSs using Internet Protocol (IP)-driven proprietary or local-area networks can cause devastating consequences by misusing communication faults to launch simple or dismissive attacks which may lead to the corruption of control operations, catastrophic failures or DoS. Consequently, the safety and stability of a power system could be compromised [119] and, even more seriously, the big data generated by it can become vulnerable [118], [120]. There are two main types of attacks, physical and cyber, with the former targetting physical components/devices such as the power grid's PMU and the latter aiming to gain access to the network's operations and system information [120]. Cyber attacks that target system data, as in data-poisoning ones, are considered serious due to their capabilities to manipulate system data without being identified by an IDS or bad detection method.

A new paradigm called a blockchain was introduced in 2008 to provide a significant solution to security and privacy issues in different applications (e.g., medical, economic, social and power system control) as it works basically on the concept of a decentralised and shared ledger. It enables communicating devices/users to store, exchange, backtrack and update information in a secure way without any authority from other parties, as illustrated in the previous section. Although a blockchain is successful in achieving security through a P2P network using encryption, the privacy of surrounding transactions is not confirmed due to data sharing within this network. Therefore, researchers are introducing privacy-protecting methods based on blockchains using different approaches, such as DP, encryption, smart contract or hybrid.

Researchers are increasingly exploiting blockchains for CPSs as, generally, IoT applications introduce new possibilities and strategies for securing and protecting their information due to the decentralisation and trustless characteristics of blockchains. Many approaches based on blockchains for addressing security and privacy issues in the IoT and CPSs are proposed in the literature; for example, Zyskind *et al.* [121] introduced an access control management protocol-based blockchain technology for preserving the privacy of personal data against third parties since, as the data collected by companies and social networks are a valuable asset for any organisation to improve its services and profit, the issue of user privacy is of concern. Three entities are involved in this platform, users, services and a blockchain's nodes, with the first two able to query the nodes and access them for permission to change. However, this platform is computationally expensive and lacks data analytics as the data in it are encrypted.

In [122], a Healthcare Data Gateway (HDG) platform based on blockchain storage whereby patients have the control to own, access and share their private health records without breaching their privacy is proposed. However, although this privacy is achieved through system access control, the data and all the computations are not considered secure. Azaria *et al.* [123] proposed a decentralised data management system called MedRec which allows patients complete and immutable access control and data storage management but its time complexity is high and its data processing limited and not well preserved. However, it can be considered an access control approach for privacy preservation.

In [124], a blockchain in a M2M transmission system is collaboratively designed through: (1) unifying the data format of building blocks in/of public-area networks in order to provide essential communication and conduct queries; (2) connecting the public and private areas in a/the device to pass queries and their results; (3) keeping data records of the M2M communication process in private-area blocks. To demonstrate the applicability of a blockchain for securing M2M in a CPS, a case study of a cotton production system in which multiple copies of all the data are stored in a blockchain is conducted. Using a blockchain allows a system to increase its number of machines which avoids any illegal tampering of data and ensures an efficient and secure system. However, this paper doesn't examine the system's complexity and only considers one production system. Blockchain technology is used in [125] to achieve the privacy and integrity of healthcare data while different authorised parties, such as patients, have the privileges of storing data, conducting computations and requesting queries from the system. In a blockchain, cryptographic techniques are applied to encrypt sensitive data to protect them against various vulnerabilities and ensure the pseudonymity of patients. However, this method is not evaluated using health data, especially the privacy level it achieves or its computational cost.

In [126], a new model based on a blockchain and online ML for the privacy preservation of healthcare data is

introduced. The blockchain adapts decentralisation between different institutional sites and has additional proof-of-information as well as its PoW to achieve its priority of applying ML on the blockchain's parties. Although this framework achieves privacy protection while learning a model based on the patients data without transferring them, it is still computationally expensive for transaction mining and determining learning priorities using the additional proof-of-information. Also, a threshold has to be set in advance for it to perform well. Finally, as it is not evaluated and compared with other algorithms and applications, it lacks applicability. In [127], an authorisation framework is proposed as a distributed privacy-preserving access control through IoT devices using a smart contract and is integrated with a blockchain to ensure a fair distribution among various entities. However, it requires identity and policy checks every time before an entity is authorised to process a transaction and its storage and time costs are quite high.

In 2018, a privacy preserving-based blockchain called BPDS [128] in which the EMRs are stored on the cloud and the associated indices kept in a tamper-proof consortium blockchain to reduce the chance of the RMRs data being leaked and altered is developed. In this scheme, the consensus method is improved to increase the trust of selected medical organisations in reliable data sharing. Despite eliminating the risk of patients privacy being compromised, the time and storage resources required are very expensive. Also, a hypothetical level of trust is assumed for some selected organisations which would not be applicable in reality. In another research study of a blockchain [129], an attribute-based signature scheme with multiple authorities based on a blockchain and ABS scheme that provides a secure protocol in a distributed system with better performance than comparative studies in terms of efficiency is proposed. However, its sign-verification computational overhead increases linearly with the number of authorities and attributes while only the authorities granted access, not data privacy, are considered.

A privacy preserving-based data aggregation and blockchain technology for securing the electrical consumption data in a smart grid is proposed in [130] In it, users are split into groups which record their data in the blockchain, with each group using pseudonyms and bloom filters to anonymise their identities and authentications, respectively. The computational cost of this method is evaluated by comparing it with traditional authentication and aggregation schemes and it is shown that it takes the least time. However, its privacy level and system utility are not evaluated. In [131], the e-government system's privacy preservation is considered using a framework-based blockchain technology for gaining a high level of trust in public sectors. Although it enhances convenience, security and reliability, the time required to validate each transaction is still high. Also, it is not evaluated and compared with other work and presents only a theoretical discussion.

Since it is crucial for medical data to be protected from unauthorised parties, in [132], blockchain-based data (DPS) is implemented on an ethereum platform on which medical data can be preserved and any tampering can be discovered and verified. A performance evaluation shows that the cost of DPS is less than 2 USD for 50 MB of data but increases dramatically with increases in the number of preserved files. Also, it requires improvements to optimise the data structure and cannot precisely distinguish any tampering of multimedia files. In [133], a blockchain-oriented technique for tackling the issue of privacy in a smart grid and defending it against cyber threats is proposed. It simulates power meters as network nodes (a blockchain network) with their readings stored in blocks. Although effective for protecting power nodes, it requires many computational resources.

Since 2019, the IoT's data have been securely shared using blockchain technology with a secure Support Vector Machine (SVM) algorithm [134] in which each data provider encrypts its data and uploads them as block transactions. In the data blocks, the IoT is encrypted using a homomorphic cryptosystem to enable SVM training without any third-party intervention. Although the experimental results reveal the effectiveness of using a SVM training classifier, the time consumed increases relative to the amount of trained data. Blockchain and cryptographic methods are deployed for a distributed storage scheme in [135] in which blockchain miners verify the upcoming transactions. Using certificateless cryptography, these transactions are audited and broadcast among parties IoT devices. This proposed scheme is used to evaluate a blockchain's design and system's efficiency. Although it reveals the accountability of such systems, they are not applicable in a complicated IoT environment and also require many computational resources for the blockchain and authentication purposes.

3) EVALUATION METRICS FOR ASSESSING PRIVACY PRESERVATION AND INTRUSION DETECTION

The levels of data privacy preserved are quantified by computing variations between the original and transformed data using the term'privacy level index (p_{index}) provided in [3] as

$$p_{index} = \frac{var(O) - var(U)}{var(O)} \tag{1}$$

where O and U refer to the original and updated data, respectively (i.e., before and after applying the privacy method), with a larger p_{index} indicating a higher level of privacy. The dissimilarity (DISS) level, which is the difference between the feature frequencies of the two datasets before and after data sanitisation, is given by

$$DISS = \sum_{i=1}^{N} |O(i) - U(i)| \sum_{i=1}^{N} O(i) \tag{2}$$

such that i is a counter for all N observations in the dataset features $O(i)$ and its transformed version $U(i)$.

The information loss (IL) measure is also applied, which estimates the information loss rate occurred by reconstruction functions while computing the density function O_x of features

s, as provided by

$$IL = \frac{1}{2}E\left[\int_{\Omega x} |O_x - \hat{U}_x)|dx\right] \quad (3)$$

where half of the mean values of L_1 norm between O_x and $\hat{U}_x$ are computed by the density distributions before and after data modifications.

To assess the quality of intrusion detection, as the effectiveness of the transformed data is tested based on ML criteria, the following Accuracy, Detection Rate (DR) and False Positive Rate (FPR) measures are used.

The Accuracy is the ratio of all normal and attack records correctly classified, that is,

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (4)$$

The DR is the proportion of correctly detected attack records, that is,

$$DR = \frac{TP}{TP + FN} \quad (5)$$

The FPR is the proportion of wrongly detected attack records, that is,

$$FPR = \frac{FP}{FP + TN} \quad (6)$$

These measures depend on the four terms true positive (TP), true negative (TN), false negative (FN) and false positive (FP) which refer to the numbers of actual attack vectors categorised as attacks, of actual legitimate vectors identified as legitimate, of actual attack vectors identified as legitimate and of actual legitimate vectors identified as attacks, respectively.

IV. CHALLENGES AND RESEARCH OPPORTUNITIES

Since CPSs are connected to the Internet using network models such as Modus TCP/IP, there are several challenges related to cyber security and data privacy [1], [6], [136]– [10]. Cybersecurity problems are linked to identifying new variants of cyber- and zero-day attacks as well as safeguarding CPSs cyber and physical components [16], [75] as such attacks significantly violate the objectives of availability and confidentiality, and disrupt legitimate operations. There are also problems related to integrity attacks that illegally sniff, steal and modify the original data, including those of the network traffic and telemetry data of CPSs devices and networks [6], [10]– [13]. The open challenges related to the security and privacy of CPSs and their networks are discussed in the following.

- The availability of data for evaluating approaches for privacy preservation and intrusion detection is a major challenge as many organisations do not share their data due to privacy concerns. There is a lack of heterogeneous data sources (i.e., datasets) that involve measurements and telemetry data of CPSs and their network traffic [6], [118]. As existing datasets [137], [138] do not involve new attack activities that disrupt the operations of CPSs and their networks, evaluations of the implementations of privacy preservation and intrusion detection will likely be inaccurate [3], [10], [136]. There is also a limited number of ground truths that demonstrate the validity of security events that occur. Consequently, there is a real need for the design of a realistic dataset that involves the telemetry and network data of CPSs to measure the reliability of new security and privacy mechanisms based on AI algorithms.
- Handling the heterogeneity of a CPS's data and protecting its original data against cyber and physical attacks are also significant challenges. CPSs generate large-scale data collected from the sensors and actuators as well as network traffic of their industrial and network systems [3], [37]. These data require effective data analytical methods-based privacy preservation that can process their large volumes obtained from physical and network elements, and ensure their protection against integrity attacks that attempt to illegally modify the original data [16], [17], [52], [139]. These data collections can help the understanding of system dynamics using privacy-preserving models, prevent integrity attacks and enhance the performances of CPSs.
- While protecting CPSs original data using privacy-preserving models, discovering zero-day attacks requires an anomaly-based IDS that produces high false alarm rates [7], [79], [118]. This problem is related to accomplishing the high reliability versus privacy of a system because most existing privacy-preserving models add noises and schemes for fully anonymising and keeping their identities secure but degrade the detection accuracy of anomaly-based IDSs [69], [70]. It is important to develop highly efficient privacy-preserving anomaly-detecting methods that can safeguard CPSs data and identify new attack data without disclosing any sensitive information across their networks.
- Building a comprehensive profile that includes all possible normal events is very difficult to accomplish efficiently, especially if the data are collected from measurements obtained from sensors and network packets as their boundaries between legitimate and suspicious activities are usually not precise. There are errors regarding FP and FN rates when a normal event falls in a cyber-attack region and a suspicious one in a legitimate region, respectively. As these errors could increase by implementing privacy-preserving models, it is important to ensure high detection accuracy and privacy levels to achieve a defense-in-depth strategy that protects CPSs.
- Developing real-time techniques for privacy preservation and anomaly detection is also very challenging for several reasons. Firstly, the features created from the data of sensors and network traffic include a set of noisy and irrelevant attributes that should be handled using FS-based privacy-preserving mechanisms. Secondly, the light weights of attack detection-enabled privacy techniques need to be carefully designed to

enhance performances for accurate detection and privacy protection. If these issues are not successfully resolved, these methods consume high computational resources and produce high false alarm rates, resulting in low privacy levels.

- Methods for privacy preservation and intrusion detection cannot be directly implemented for CPSs without considering their complex natures that involve physical and communication parties as well as network protocols and resource-constrained devices that have limited computational power and storage capacity. Therefore, any proposed methods require high computational capabilities that can handle the complexity of protocols and devices, discover new attack types and protect sensitive data from illegal disclosure. They should be adaptive and reliable in order to handle the dynamic states of CPSs, such as power networks, by considering feature projection and reduction mechanisms that reduce the data's high dimensionality.
- Integrating techniques for privacy preservation and intrusion detection is still complex due to their difficult deployment and the high computational processing they require for applications across CPSs networks. An intrusion detection model should be combined with a database management system-enabled privacy protection that permits the creation of alerts in real time. Also, adapting a privacy-preserving methodology requires further exploration to ensure the hiding of CPSs' confidential data and a high degree of reliability for discovering attack events. Numerous research challenges in this domain are addressed in this thesis.

V. CONCLUSION

In this paper, the current state of privacy preserving techniques for protecting the CPSs is discussed. This work begins with a detailed background of CPSs concepts; outlining the uniqueness of these systems and the high impact for cybersecurity breaches. This work also outlines the need for data privacy, especially given the advanced persistent threats that are likely to target such installations. As discussed, there are the three key challenges for the development of methods for privacy-preserving-enabled anomaly detection in CPSs. Firstly, the lack of datasets that include heterogeneous data sources including recent normal and malicious behaviours that can be used to estimate the performances of new methods in respect to their applicability for CPSs. Secondly, how to manage the data heterogeneity of CPSs data and preserving their original data against cyber attacks. Since a CPS generates large amount of data gathered from physical and network systems, it needs efficient data analytical method-based privacy preservation to be processed and kept safe against integrity attacks that try to illegally alter the original data. The third challenge is how to protect CPSs' data by identifying zero-day attacks with low false alarm rates. This is related to achieving the high credibility of systems while maintaining their privacy levels as most existing privacy-preserving techniques add noises and anonymous approaches to fully anonymise and keep their identities secure but cannot achieve high reliability in terms of data protection and attack detection. Although CPS security is an active field of research, there is a need for additional work to overcome these unique challenges. CPS installations represent high-impact cybersecurity targets, and as such require novel research to be applied specifically to this domain. Future research is necessary in several areas to ensure the safety of global critical infrastructure; specifically in the development of datasets, balancing data utility and privacy, and how to effectively detect advanced persistent threats with a high accuracy in these challenging ecosystems.

REFERENCES

[1] J. Cortes, G. E. Dullerud, S. Han, J. L. Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 4252–4272.

[2] R. Jia, R. Dong, P. Ganesh, S. Sastry, and C. Spanos, "Towards a theory of free-lunch privacy in cyber-physical systems," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2017, pp. 902–910.

[3] A. Fahad, Z. Tari, A. Almalawi, A. Goscinski, I. Khalil, and A. Mahmood, "PPFSCADA: Privacy preserving framework for SCADA data publishing," *Future Gener. Comput. Syst.*, vol. 37, pp. 496–511, Jul. 2014.

[4] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, no. 4, p. 40, Jul. 2016.

[5] H. Zakerzadeh, C. C. Aggarwal, and K. Barker, "Privacy-preserving big data publishing," in *Proc. 27th Int. Conf. Sci. Stat. Database Manage.*, Jun. 2015, pp. 1–11.

[6] M. Cinque, D. Cotroneo, R. D. Corte, and A. Pecchia, "A framework for on-line timing error detection in software systems," *Future Gener. Comput. Syst.*, vol. 90, pp. 521–538, 2019.

[7] M. Keshk, N. Moustafa, E. Sitnikova, and G. Creech, "Privacy preservation intrusion detection technique for SCADA systems," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2017, pp. 1–6.

[8] T. W. Chim, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 85–97, Jan. 2015.

[9] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proc. IEEE*, vol. 106, no. 1, pp. 113–128, Jan. 2018.

[10] C. Feng, V. R. Palleti, A. Mathur, and D. Chana, "A systematic framework to generate invariants for anomaly detection in industrial control systems," in *Proc. NDSS*, 2019, pp. 3–5.

[11] N. Moustafa, G. Creech, and J. Slay, "Big data analytics for intrusion detection system: Statistical decision-making using finite Dirichlet mixture models," in *Data Analytics and Decision Support for Cybersecurity*. Cham, Switzerland: Springer, 2017, pp. 127–156.

[12] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 4, pp. 577–590, Jul./Aug. 2016.

[13] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE Trans. Cybern.*, vol. 48, no. 6, pp. 1862–1876, Jun. 2018.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[15] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.

[16] N. Rajesh, K. Sujatha, and A. A. Lawrence, "Survey on privacy preserving data mining techniques using recent algorithms," *Int. J. Comput. Appl.*, vol. 133, no. 7, pp. 30–33, Jan. 2016.

[17] C. C. Aggarwal and S. Y. Philip, "A general survey of privacy-preserving data mining models and algorithms," in *Privacy-Preserving Data Mining*. Springer, 2008, pp. 11–52.
[18] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2411–2419, Sep. 2017.
[19] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on paillier encryption," 2018, *arXiv:1805.01065*. [Online]. Available: http://arxiv.org/abs/1805.01065
[20] S. Hajian, J. Domingo-Ferrer, and O. Farràs, "Generalization-based privacy preservation and discrimination prevention in data publishing and mining," *Data Mining Knowl. Discovery*, vol. 28, nos. 5–6, pp. 1158–1188, Sep. 2014.
[21] S. R. M. Oliveira and O. R. Zaıane, "Privacy preserving clustering by data transformation," *J. Inf. Data Manage.*, vol. 1, no. 1, p. 37, 2010.
[22] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "A survey on privacy-preserving schemes for smart grid communications," 2016, *arXiv:1611.07722*. [Online]. Available: http://arxiv.org/abs/1611.07722
[23] B. R. Mistry and A. Desai, "Privacy preserving heuristic approach for association rule mining in distributed database," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–7.
[24] Y. Guo, "Reconstruction-based association rule hiding," in *Proc. SIGMOD Ph.D. Workshop Innov. Database Res.*, 2007, pp. 51–56.
[25] A. Sohani and K. Sawant, "PSDS: Privacy preserving system for data security implementation and countermeasures," *Int. J. Comput. Appl.*, vol. 156, no. 4, pp. 21–25, Dec. 2016.
[26] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.
[27] S. Sharma and S. Ahuja, "Privacy preserving data mining: A review of the state of the art," in *Harmony Search and Nature Inspired Optimization Algorithms*, N. Yadav, A. Yadav, J. C. Bansal, K. Deep, and J. H. Kim, Eds. Singapore: Springer, 2019, doi: 10.1007/978-981-13-0761-4_1.
[28] V. Srivastava, S. Singh, and S. Shukla, "Utilization of encryption for security in SCADA networks," in *Proc. Pragyaan*, 2015, p. 17.
[29] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. CRC Press, 2016.
[30] A. Dinesh and K. E. Bijoy, "Privacy preserving speech, face and fingerprint based biometrie authentication system using secure signal processing," in *Proc. 2nd Int. Conf. Commun. Syst., Comput. IT Appl. (CSCITA)*, Apr. 2017, pp. 164–168.
[31] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 493–508, Jun. 2014.
[32] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Des. Test*, vol. 34, no. 4, pp. 7–17, Aug. 2017.
[33] S. M. A. Kabir, A. M. Youssef, and A. K. Elhakeem, "On data distortion for privacy preserving data mining," in *Proc. Can. Conf. Electr. Comput. Eng.*, Apr. 2007, pp. 308–311.
[34] P. Cheng, J. F. Roddick, S.-C. Chu, and C.-W. Lin, "Privacy preservation through a greedy, distortion-based rule-hiding method," *Appl. Intell.*, vol. 44, no. 2, pp. 295–306, 2016.
[35] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 598–607, Jun. 2014.
[36] G. Li and R. Xue, "A new privacy-preserving data mining method using non-negative matrix factorization and singular value decomposition," *Wireless Pers. Commun.*, vol. 102, no. 2, pp. 1799–1808, Sep. 2018.
[37] R. V. Banu and N. Nagaveni, "Evaluation of a perturbation-based technique for privacy preservation in a multi-party clustering scenario," *Inf. Sci.*, vol. 232, pp. 437–448, May 2013.
[38] G. Chandrashekar and F. Sahin, "A survey on feature selection methods," *Comput. Elect. Eng.*, vol. 40, no. 1, pp. 16–28, Jan. 2014.
[39] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and M. J. Deen, "Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2896–2903, Aug. 2018.
[40] H. Nguyen, D. Zhuang, P.-Y. Wu, and M. Chang, "AutoGAN-based dimension reduction for privacy preservation," *Neurocomputing*, vol. 384, pp. 94–103, Apr. 2020.
[41] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, S. Halevi, and T. Rabin, Eds. Berlin, Germany: Springer, 2006, doi: 10.1007/11681878_14.
[42] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.
[43] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath, "The staircase mechanism in differential privacy," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1176–1184, Oct. 2015.
[44] C. Uhler, A. B. Slavković, and S. E. Fienberg, "Privacy-preserving data sharing for genome-wide association studies," *J. Privacy Confidentiality*, vol. 5, no. 1, p. 137, Aug. 2013.
[45] L. Chen, R. Lu, Z. Cao, K. AlHarbi, and X. Lin, "MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-Peer Netw. Appl.*, vol. 8, no. 5, pp. 777–792, Sep. 2015.
[46] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.
[47] Z. Guan and G. Si, "Achieving privacy-preserving big data aggregation with fault tolerance in smart grid," *Digit. Commun. Netw.*, vol. 3, no. 4, pp. 242–249, Nov. 2017.
[48] C. Lin, Z. Song, H. Song, Y. Zhou, Y. Wang, and G. Wu, "Differential privacy preserving in big data analytics for connected health," *J. Med. Syst.*, vol. 40, no. 4, p. 97, Apr. 2016.
[49] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 619–626, Mar. 2017.
[50] L. Ni, C. Li, H. Liu, A. G. Bourgeois, and J. Yu, "Differential private preservation multi-core dbscan clustering for network user data," *Procedia Comput. Sci.*, vol. 129, pp. 257–262, 2018, doi: 10.1016/j.procs.2018.03.073.
[51] E. Hammer-Lahav. (2010). *The Oauth 1.0 Protocol*. [Online]. Available: http://tools.ietf.org/html/rfc5849
[52] P. Harding, L. Johansson, and N. Klingenstein, "Dynamic security assertion markup language: Simplifying single sign-on," *IEEE Secur. Privacy Mag.*, vol. 6, no. 2, pp. 83–85, Mar. 2008.
[53] S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. Das, "A key management framework for AMI networks in smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 30–37, Aug. 2012.
[54] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, Oct. 2013.
[55] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *IEEE Netw.*, vol. 27, no. 4, pp. 64–71, Jul./Aug. 2013.
[56] Y. Xu, T. Price, J.-M. Frahm, and F. Monrose, "Virtual u: Defeating face liveness detection by building virtual models from your public photos," in *Proc. 25th USENIX Secur. Symp.*, 2016, pp. 497–512.
[57] J. C. L. Cheung, T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Credential-based privacy-preserving power request scheme for smart grid network," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–5.
[58] K. Fan, W. Jiang, Q. Luo, H. Li, and Y. Yang, "Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV," *J. Franklin Inst.*, vol. 358, no. 1, pp. 193–209, Jan. 2021.
[59] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019.
[60] A. Sachan, D. Roy, and P. V. Arun, "An analysis of privacy preservation techniques in data mining," in *Advances in Computing and Information Technology*, N. Meghanathan, D. Nagamalai, and N. Chaki, Eds. Berlin, Germany: Springer, 2013, doi: 10.1007/978-3-642-31600-5_12.
[61] Y. Rizk, M. Awad, and E. W. Tunstel, "Cooperative heterogeneous multi-robot systems: A survey," *ACM Comput. Surv.*, vol. 52, no. 2, Apr. 2019, Art. no. 29, doi: 10.1145/3303848.

[62] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 1, pp. 92–106, Jan. 2006.

[63] G. Loukides and A. Gkoulalas-Divanis, "Utility-preserving transaction data anonymization with low information loss," *Expert Syst. Appl.*, vol. 39, no. 10, pp. 9764–9777, Aug. 2012.

[64] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond K-anonymity," *ACM Trans. Knowl. Discovery Data*, vol. 1, no. 1, p. 3, 2007.

[65] J. Wang, Z. Cai, Y. Li, D. Yang, J. Li, and H. Gao, "Protecting query privacy with differentially private k-anonymity in location-based services," *Pers. Ubiquitous Comput.*, vol. 22, no. 3, pp. 453–469, Jun. 2018.

[66] R. Mendes and J. P. Vilela, "Privacy-preserving data mining: Methods, metrics, and applications," *IEEE Access*, vol. 5, pp. 10562–10582, 2017.

[67] N. Li, T. Li, and S. Venkatasubramanian, "T-closeness: Privacy beyond K-anonymity and l-Diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Apr. 2007, pp. 106–115.

[68] F. C. Sangogboye, R. Jia, T. Hong, C. Spanos, and M. B. Kjærgaard, "A framework for privacy-preserving data publishing with enhanced utility for cyber-physical systems," *ACM Trans. Sensor Netw.*, vol. 14, nos. 3–4, pp. 1–22, Dec. 2018.

[69] R. Jia, F. C. Sangogboye, T. Hong, C. Spanos, and M. B. Kjærgaard, "PAD: Protecting anonymity in publishing building related datasets," in *Proc. 4th ACM Int. Conf. Syst. Energy-Efficient Built Environ.*, Nov. 2017, pp. 1–10.

[70] S. A. Abdelhameed, S. M. Moussa, and M. E. Khalifa, "Restricted sensitive attributes-based sequential anonymization (RSA-SA) approach for privacy-preserving data stream publishing," *Knowl.-Based Syst.*, vol. 164, pp. 1–20, Jan. 2019.

[71] N. H. Domadiya and U. P. Rao, "Hiding sensitive association rules to maintain privacy and data quality in database," in *Proc. 3rd IEEE Int. Advance Comput. Conf. (IACC)*, Feb. 2013, pp. 1306–1310.

[72] J. Lai, Y. Li, R. H. Deng, J. Weng, C. Guan, and Q. Yan, "Towards semantically secure outsourcing of association rule mining on categorical data," *Inf. Sci.*, vol. 267, pp. 267–286, May 2014.

[73] K. Iqbal, X.-C. Yin, H.-W. Hao, Q. M. Ilyas, and X. Yin, "A central tendency-based privacy preserving model for sensitive XML association rules using Bayesian networks," *Intell. Data Anal.*, vol. 18, no. 2, pp. 281–303, Feb. 2014.

[74] C. N. Modi, U. P. Rao, and D. R. Patel, "Maintaining privacy and data quality in privacy preserving association rule mining," in *Proc. 2nd Int. Conf. Comput., Commun. Netw. Technol.*, Jul. 2010, pp. 1–6.

[75] M. O. Sayin and T. Başar, "Secure sensor design for cyber-physical systems against advanced persistent threats," in *Decision and Game Theory for Security*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds. Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-68711-7_6.

[76] X. Zhang and H. Bi, "Research on privacy preserving classification data mining based on random perturbation," in *Proc. Int. Conf. Inf., Netw. Autom. (ICINA)*, vol. 1, Oct. 2010, pp. V1–173.

[77] X. He, H. Chen, Y. Chen, Y. Dong, P. Wang, and Z. Huang, "Clustering-based K-anonymity," in *Advances in Knowledge Discovery and Data Mining*, P.-N. Tan, S. Chawla, C. K. Ho, and J. Bailey, Eds. Berlin, Germany: Springer, 2012, doi: 10.1007/978-3-642-30217-6_34.

[78] R. B. Ghate and R. Ingle, "Clustering based anonymization for privacy preservation," in *Proc. Int. Conf. Pervasive Comput. (ICPC)*, Jan. 2015, pp. 1–3.

[79] A. Alabdulatif, H. Kumarage, I. Khalil, and X. Yi, "Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption," *J. Comput. Syst. Sci.*, vol. 90, pp. 28–45, Dec. 2017.

[80] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–35, Sep. 2018.

[81] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Syst. J.*, vol. 8, no. 2, pp. 641–654, Jun. 2014.

[82] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[83] S. Yakoubov, V. Gadepally, N. Schear, E. Shen, and A. Yerukhimovich, "A survey of cryptographic approaches to securing big-data analytics in the cloud," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2014, pp. 1–6.

[84] P. Pullonen and S. Siim, "Combining secret sharing and garbled circuits for efficient private IEEE 754 floating-point computations," in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Germany: Springer, 2015, doi: 10.1007/978-3-662-48051-9_13.

[85] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.

[86] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[87] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT*, J. Stern, Ed. Berlin, Germany: Springer, 1999, doi: 10.1007/3-540-48910-X_16.

[88] C. Gentry and D. Boneh, *A Fully Homomorphic Encryption Scheme*, vol. 20, no. 9. Stanford, CA, USA: Stanford Univ., 2009.

[89] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[90] Y.-S. Kim and J. Heo, "Device authentication protocol for smart grid systems using homomorphic hash," *J. Commun. Netw.*, vol. 14, no. 6, pp. 606–613, Dec. 2012.

[91] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053–2064, Aug. 2014.

[92] T. Dimitriou and M. K. Awad, "Secure and scalable aggregation in the smart grid resilient against malicious entities," *Ad Hoc Netw.*, vol. 50, pp. 58–67, Nov. 2016.

[93] M. Badra and S. Zeadally, "Lightweight and efficient privacy-preserving data aggregation approach for the smart grid," *Ad Hoc Netw.*, vol. 64, pp. 32–40, Sep. 2017.

[94] J. Hur, D. Koo, and Y. Shin, "Privacy-preserving smart metering with authentication in a smart grid," *Appl. Sci.*, vol. 5, no. 4, pp. 1503–1527, Dec. 2015.

[95] J. Kim, S. Kim, and J. H. Seo, "A new scale-invariant homomorphic encryption scheme," *Inf. Sci.*, vol. 422, pp. 177–187, Jan. 2018.

[96] J.-S. Coron, T. Lepoint, and M. Tibouchi, "Scale-invariant fully homomorphic encryption over the integers," in *Public-Key Cryptography—PKC*, H. Krawczyk, Ed. Berlin, Germany: Springer, 2014, doi: 10.1007/978-3-642-54631-0_18.

[97] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system," *Future Gener. Comput. Syst.*, vol. 108, pp. 1287–1296, Jul. 2020.

[98] Z. Min, G. Yang, A. K. Sangaiah, S. Bai, and G. Liu, "A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 15, Dec. 2019.

[99] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in *Advances in Cryptology—CRYPTO*, A. J. Menezes and S. A. Vanstone, Eds. Berlin, Germany: Springer, 1991, doi: 10.1007/3-540-38424-3_32.

[100] A. J. M. Milne, A. Beckmann, and P. Kumar, "Cyber-physical trust systems driven by blockchain," *IEEE Access*, vol. 8, pp. 66423–66437, 2020.

[101] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[102] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[103] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[104] T. Kim, J. Ochoa, T. Faika, A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Jan. 21, 2020, doi:10.1109/JESTPE.2020.2968490.

[105] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Concurrency: The Works of Leslie Lamport*. Association for Computing Machinery, 2019, doi: 10.1145/3335772.3335936.
[106] F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. Financial Stud.*, vol. 34, no. 3, pp. 1156–1190, 2021.
[107] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Open Problems in Network Security*, J. Camenisch and D. Kesdoğan, Eds. Cham, Switzerland: Springer, 2016, doi: 10.1007/978-3-319-39028-4_9.
[108] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *Proc. Italian Conf. Cyber Secur.*, Jan. 2018. [Online]. Available: https://eprints.soton.ac.uk/415083/
[109] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54371–54401, 2020.
[110] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.
[111] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed. Berlin, Germany: Springer, 2013, doi: 10.1007/978-3-642-39884-1_2.
[112] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names," in *Proc. Conf. Internet Meas. Conf.*, Oct. 2013, pp. 127–140.
[113] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in Bitcoin P2P network," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 15–29.
[114] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from Bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 459–474.
[115] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.
[116] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.
[117] Y. Cui, B. Pan, and Y. Sun, "A survey of privacy-preserving techniques for blockchain," in *Artificial Intelligence and Security*, X. Sun, Z. Pan, and E. Bertino, Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-24268-8_21.
[118] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, and I. Khalil, "An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 66–79, Jan. 2021.
[119] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1092–1102, Jun. 2014.
[120] G. A. Fink, T. W. Edgar, T. R. Rice, D. G. MacDonald, and C. E. Crawford, "Security and privacy in cyber-physical systems," in *Cyber-Physical Systems* (Intelligent Data-Centric Systems), H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, Eds. Boston, MA, USA: Academic, 2017, pp. 129–141. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128038017000092, doi: 10.1016/B978-0-12-803801-7.00009-2.
[121] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.
[122] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, Oct. 2016.
[123] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.
[124] S. Yin, J. Bao, Y. Zhang, and X. Huang, "M2M security technology of CPS based on blockchains," *Symmetry*, vol. 9, no. 9, p. 193, Sep. 2017.
[125] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain based privacy preserving platform for healthcare data," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-72395-2_49.
[126] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*. [Online]. Available: http://arxiv.org/abs/1802.01746
[127] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, A. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-46568-5_53.
[128] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.
[129] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
[130] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.
[131] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving E-government system," *Wireless Netw.*, pp. 1–11, 2018.
[132] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, no. 8, p. 141, Aug. 2018.
[133] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.
[134] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.
[135] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale Internet of Things data storage and protection," *IEEE Trans. Services Comput.*, vol. 12, no. 5, pp. 762–771, Sep. 2019.
[136] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32910–32924, 2018.
[137] (May 2017). *Power Systems Datasets*. [Online]. Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets
[138] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.
[139] M. Z. Alom, T. M. Taha, C. Yakopcic, S. Westberg, P. Sidike, M. S. Nasrin, M. Hasan, B. C. Van Essen, A. A. S. Awwal, and V. K. Asari, "A state-of-the-art survey on deep learning theory and architectures," *Electronics*, vol. 8, no. 3, p. 292, Mar. 2019.

MARWA KESHK received the bachelor's degree in computer science from the Faculty of Computer and Information, Helwan University, Egypt, in 2012, and the master's degree in computer science from the UNSW of Canberra, in 2017, where she is currently pursuing the Ph.D. degree with the School of Engineering and Information Technology (Australian Centre for Cyber Security). She is also a Research Candidate with Data61-CSIRO, Australia. Her research interests include cyber Security, privacy preservation, evolutionary computation, artificial intelligence techniques, and statistical methods.

BENJAMIN TURNBULL has been working in digital forensics, network security and simulation for a period of 17 years. He is currently a Senior Lecturer with the University of New South Wales, Australian Defence Force, Canberra. His research focuses on the intersection of cyber-security, simulation, scenario-based learning and the security of heterogeneous devices, and future networks. He is also a Certified Information Systems Security Professional (CISSP). His previous work as a defence research scientist saw him develop and deploy new technologies to multiple clients, globally.

ELENA SITNIKOVA received the B.E. (Hons.) and Ph.D. degrees. She is currently a Researcher and academic within the Australian Centre for Cyber Security (ACCS), University of NSW at ADFA. She is also a CSSLP. She currently leads the Critical Infrastructure area, carrying out research projects in cyber security in Industrial Internet of Things (IIoT) and IDS for SCADA and industrial control systems. Her main research interests include critical infrastructure protection and cyber security, software and systems engineering, quality assurance, and enterprise process capability improvement.

DINUSHA VATSALAN is currently a Research Scientist with Data61-CSIRO, Australia, and an Honorary Lecturer with the Research School of Computer Science, Australian National University. Her research interests include privacy preserving techniques, including privacy in data matching and mining, privacy in social media, privacy preserving counting in stream data analytics, privacy risk evaluation and prediction, health informatics, and population informatics.

NOUR MOUSTAFA (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from the Faculty of Computer and Information, Helwan University, Egypt in 2009 and 2014, respectively, and the Ph.D. degree in cyber security from the University of New South Wales (UNSW) Canberra, Australia, in 2017. From June 2017 to December 2018, he was a Postdoctoral Fellow with UNSW Canberra. He is currently a Lecturer with SEIT, UNSW Canberra. He has several research grants with totalling over AUD 1.2 million. His research interests include cyber security, in particular, network security, the IoT security, intrusion detection systems, statistics, deep learning, and machine learning techniques. He has been received the 2020 prestigious Australian Spitfire Memorial Defence Fellowship Award. He is an ACM Distinguished Speaker, as well as CSCRC and Spitfire Fellow. He has also served over seven conferences in leadership roles, involving vice-chair, session chair, technical program committee (TPC) member, and proceedings chair, including 2020IEEE TrustCom and 2020 33rd Australasian Joint Conference on Artificial Intelligence. He has served his academic community, as the Guest Associate Editor for the IEEE transactions journals, including the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE INTERNET OF THINGS JOURNAL, as well as the journals of IEEE ACCESS, *Future Internet and Information Security Journal: A Global Perspective*.