Modelling Industrial IoT Security Using Ontologies: A Systematic Review

JARWAR, Muhammad Aslam <http://orcid.org/0000-0002-5332-1698>, FRENG, Jeremy Watson CBE and ALI, Sajjad

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version 11 January, 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.011100

Modelling Industrial IoT Security using Ontologies: A Systematic Review

Muhammad Aslam Jarwar[1] *(Senior Member, IEEE)*, Jeremy Watson CBE FREng [2], AND Sajjad Ali [3] *(Senior Member, IEEE)*

[1]School of Computing and Digital Technologies, Sheffield Hallam University, United Kingdom, S1 1WB
[2]Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London, United Kingdom, WC1E 6JA
[3]School of Computing, Engineering and Intelligent Systems, Ulster University, Northern Ireland, United Kingdom, BT48 7JL

CORRESPONDING AUTHOR: Muhammad Aslam Jarwar (e-mail: a.jarwar@shu.ac.uk).

This work has been supported by the PETRAS National Center of Excellence in IoT Systems Cybersecurity, which is funded by the UK EPSRC under grant number EP/S035362/1.

ABSTRACT The significance of Industrial Internet of Things (IIoT) is undeniable, yet many critical industries remain hesitant to adopt it due to fundamental security, transparency and safety concerns. Developing a mechanism to address these concerns is challenging, as it involves a large number of heterogeneous devices, complex relations and human-machine contextual factors. This article presents a comprehensive analysis through a systematic review of ontologies and key security attributes essential for modelling the security of IIoT environments. Our review includes an extensive analysis of research articles, semantic security ontologies, and cybersecurity standards. Through this analysis, we identify critical security concepts and attributes, which can be leveraged to develop standardised security ontologies tailored for IIoT. Additionally, we explore the potential of integrating ontologies into the Industry 5.0 paradigm, which emphasises human-centricity, resilience, and sustainability. While ontologies offer structured modelling capabilities, their alignment with Industry 5.0's unique collaborative and adaptive security needs remains limited. Our review suggests that existing security ontologies are not fully aligned with security goals, exposing many important research gaps. These gaps include areas such as semantic mapping techniques, security-by-design ontologies, holistic security standards, and ontologies that address the sociotechnical aspects of IIoT.

INDEX TERMS Security ontology, Industrial Internet of Things (IIoT), Cyber physical systems, Cybersecurity, Security attributes

I. INTRODUCTION

The Industrial Internet of Things (IIoT) refers to interconnected sensors, actuators, instruments, machines, and other networked devices. These IIoT systems can range from advanced embedded systems to simple single-board computers, equipped with sophisticated prediction, analytics, and visualisation services. All these services facilitate automation in various sectors, including supply chain management, manufacturing, construction, and energy efficiency in buildings [1]–[4]. The IIoT enhances work efficiency, ensures the safety of production facilities, and provides advanced energy efficiency solutions in Building Management Systems (BMS) and addressing the impacts of climate change. Conversely, the Consumer Internet of Things (CIoT) supports applications designed to make consumers' lives more convenient and easier [5], [6]. From an architectural view, the key difference between Internet of Things (IoT) and IIoT is the variation in types of service functionality requirements at the service layer. In order to review security ontologies, we refer the IIoT as "A system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product and service information, in the industrial environment" [7].

The exponential proliferation of IoT devices, coupled with their deployment in Critical National Infrastructures (CNIs) and privacy-sensitive applications, and the prevalent defi-

ciency in built-in security measures make these systems attractive targets for attacks [8]. Consequently, sectors involving highly critical buildings, citizen services, and industries exhibit reluctance in adopting IIoT technologies [9], [10]. For instance, consider the extent of damage stemming from security breaches and the breakdown of IIoT systems that manage water resources, autonomous rail networks, smart traffic signals, food chillers, smart grids and food supply chain [11]–[13]. Most of these security issues stem from the integration of legacy Industrial Control Systems (ICS) with IIoT devices [9]. The integration of IIoT devices with legacy ICS aims to enhance functionality, performance, and productivity. However, this integration broadens the threat landscape, introducing additional attack vectors that can be exploited to target industrial systems, because legacy ICS devices often lack the necessary security functionalities [14].

The security of IIoT devices is challenging for several reasons. The IIoT contains numerous heterogeneous devices installed into industrial controls and they lack operate-time permissioning to communicate and exchange data with different machines and the way these are operated and serviced [9], [14]–[16]. For example, there is an issue with applying patches or testing untrusted security solutions on live industrial systems and managing default passwords. Thus, security modelling is considered one of the viable alternatives which enables the capability to support operate-time security testing and to predict the cascading effects of device failure in advance. Ontology is one of the recognised and acceptable approach to identifying and modelling the cascading effects during operate-time and represent the complex environments in other domains including banking, social networks, clinical diagnosis [17]–[21]. Ontological methods are also prevalent in smart city modelling, Machine-to-Machine (M2M) communication, devices virtualisation and modelling sensors' observations [22]–[24]. The use of ontologies in security modelling is also gaining importance [25]–[27]. In ontology, a concept is a core component which represents entities or things, such as IoT devices. Along with other ontology components such as relations, instances, and axioms, it provides a structured and semantic way for modelling complex security relationships among devices. In this way, it enables detailed threat modelling by facilitating the identification of vulnerabilities and the development of mitigation strategies through automated reasoning. Ontologies play a key role in advancing Industry 5.0 by enabling the representation of security mechanisms that facilitate interoperability and support value creation in the complex context of IIoT applications. [28]. This approach chimes with Industry 5.0's accent on resilience and human-centric technologies. Ontologies would be used by organisations in strengthening cybersecurity through intelligent threat detection and responses. AI-driven ontologies will make it possible to describe controlled and uncontrolled factors that exploit vulnerabilities to allow dynamic classification, prediction, and real-time response to cyber threats [29]. The integration ensures decentralized control and enforces data privacy along the supply chain-a key and necessary aspect for Industry 5.0, aiming for sustainable and secure operations. For example, security ontologies are utilised for identifying relations among threats and appropriate countermeasures [30], [31], cyber threat intelligence [29], [32], intrusion detection, representing prevalent machine learning threats and countermeasures [33], complement machine learning for analysing and predicting of threats in supply chain [34], Web of Things (WoT) security modelling [35], IoT devices security modelling in IIoT applications [8]. However, these approaches lack the standardized security ontology to support IIoT security modelling. For example, there is no standardized ontology that contains essential concepts for security goal oriented modelling as well as enabling design-time and operate-time security features.

A. CONTRIBUTION OF THIS STUDY

This article presents the findings of a systematic review of security ontologies that either fully support or can be extended for modelling the security of IIoT devices. The central focus of this review is to analyse the ontologies with respect to security goals and to pinpoint the crucial security attributes that facilitate the security modelling of IIoT devices. In addition, we briefly explain the succinct research gap and potential future directions on security ontologies for IIoT.

Our review is advanced from the state-of-the-art in several aspects:

- Firstly, to the best of our knowledge, this is the first systematic review conducted on security modeling of IIoT using semantic methods.
- Secondly, the existing surveys are lacking in critically reviewing and identifying the security attributes to support the security modelling of IIoT devices.
- Thirdly, this review investigates the extent to which ontologies facilitate goal-based representation and modelling of cybersecurity knowledge.
- Fourthly, our survey presents the research gap and future directions for developing the IIoT's security ontologies.

B. ORGANISATION OF THE PROPOSED ARTICLE

The rest of the paper is organised as follows. Section II presents related work. Sections III and IV provide details of data collection and the strategy of data analysis, respectively. Section V provides a review of ontologies which could be used for IIoT security modelling. Important acronyms are defined in Table 5. Section VI showcases the key security concepts and attributes. Section VII outlines the research gaps, recommendations and future work. Finally, Section VIII concludes the study.

II. RELATED RESEARCH WORK

In this subsection, we critically analyse the state-of-the-art surveys on cybersecurity ontologies in the context of IIoT. Recently, the literature has seen numerous reviews and research studies aimed at exploring potential ontologies for IIoT, including their implementation, applications, and future research directions [7], [25], [26], [31], [32], [36], [37], [38], [39], [40], [41]–, [42], [43], [44], [45], [46], [47], [48]. For instance, Boyes et al. [7] provide an exposition of IIoT system security requirements and a proposed comprehensive framework for the systematic analysis of security threats and vulnerabilities. In particular, surveys [36], [38] focus on cyberattack taxonomies and categorise attacks according to their methods, locations, and consequences. Additionally, they categorise industrial security challenges and link them to relevant enabling technologies. Similarly, study [43], focuses on ontologies in the context of security assessment and categories based on their characteristics, research issues addressed, and application domains. Martins et al. [31] showcase a comprehensive review of cybersecurity ontologies, identifying twenty eight distinct examples. Based on their analysis, they developed a framework that classifies ontologies according to their application level, generality level, formalization level, and axiomatization level. Another survey study [41], focuses on categorisation of ontologies based on their various functions in IoT, such as sensor representation, observation description, and service discovery. Further, review by Adach et al. [25] pointed out that existing ontologies in the security domain are difficult to categorize and may not adhere to security standards, thereby leading to inconsistencies in security knowledge. Survey [32] examines the use of ontologies to model and enhance supply chain security, focusing on connectivity, data integrity, and system convergence. Similarly, [42] explores various blockchain consensus algorithms and develops a formally specified ontology to facilitate reasoning about these algorithms. Survey [46] assesses how ontologies address critical aspects of Operational Technology Systems (OTS), such as safety, security, and operational requirements. The role of ontologies in the context of industry 4.0 reviewed in [39], this review suggests that ontologies can provide a standardized way to enable seamless communication and data exchange between various intelligent systems, both human and artificial, in smart manufacturing environments. Explainable Artificial Intelligence (XAI) facilitates decision-making in complex industrial systems by providing interpretable and actionable insights, particularly in scenarios involving data fusion from multiple sources. Authors in study [47] highlight the integration of XAI in Industry 5.0 to address transparency and trust challenges in cybersecurity. Study [48] introduces a Digital Twin Workshop (DTW) that integrates ontologies to allow semantic reasoning on unsafe states in human-centric Industry 5.0 environments. Article [49] Proposes a lightweight ontology for Industry 5.0, integrating humans, devices, and processes. The research automated the identification and mitigation of safety risks in manufacturing by using ontology-based models and AI-driven detection methods. Ontologies enhance the interpretation of relationships between system entities, contributing to proactive safety management.

Several surveys [26], [40], [43], [47], [48] have found that there is a lack of research on critical issues such as safety, trust, transparency in the context of industry 5.0 cybersecurity decisions, knowledge reuse, automation, interoperability, heterogeneity, human factors, and assessment coverage. Specifically, [37] revealed that ontologies are primarily utilised to enhance compatibility, maintainability, and usability in IoT, with a focus on architectural and contextual modelling. However, significant gaps remain in areas such as efficiency, reliability, and the modelling of system states and objectives, underscoring the need for further research. To the best of our knowledge, no existing survey has focused on ontologies in the context of cybersecurity goals. In Table 1, we compare and contrast the above-discussed state-of-the-art with this article in terms of key aspects of ontologies for IIoT security.

TABLE 1: Comparison and summary of related surveys.

Study	Ontology classification	Features	Concepts/properties	Attributes	Cybersecurity focus	Cybersecurity goals focus	IoT, IIoT, CPS focus	Applications & use cases	Research gap analysis & recommendation	Remarks - Relevance to the IIoT security ontologies
Szilagy et al.,2016 [41]	✓	✓	L	✗	L	✗	✓	M	✗	Focus on categorisation of ontologies based on their various functions in IoT.
Rosa et al., 2017 [43]	✗	✓	✗	✗	✓	✗	✗	✓	✗	Focus on ontologies and taxonomies concerned with security assessment.
Boyes et al., 2018 [7]	✗	✗	✓	✗	✓	✗	✓	✓	✓	Focus on IIoT security, definition, and taxonomy.
Kumar et al., 2019 [39]	✓	✓	✗	✗	L	✗	M	✓	✗	Focus on the role of ontologies for formal knowledge representation systems in the context of industry 4.0.
Sobb et al., 2020 [44]	✗	✗	L	✗	✓	✗	M	✓	✗	Focus on using ontologies in supply chain and cyber-physical system security for military applications.
Rivad et al., 2021 [40]	✗	✓	✗	✗	✓	✗	✗	✓	✗	Focus on application of ontologies in the context of cybersecurity.
Liao et al., 2021 [45]	✗	L	✗	✗	✓	✗	✓	M	✓	Focus on security assessment and practices studies in IoT.
Lenin et al., 2022 [37]	✗	✓	✗	✗	✗	✗	✓	✓	✗	Focus on using ontologies to manage the complexity of IoT environments.
Khan et al., 2022 [42]	✗	✓	L	✗	✓	✗	✓	✗	✓	Focus on ontologies for blockchain consensus algorithms in the context of IoT services.
Qaswar et al., 2022 [26]	✗	L	✗	✗	✓	✗	✓	L	✓	Survey on various ontologies in the context of IoT applications.
Martins et al., 2022 [31]	✓	✗	✓	✓	✓	✗	✗	✗	✓	Focus on classifying cybersecurity ontologies.
Adach et al., 2022 [25]	✗	✗	✓	✓	✓	✗	✗	✗	✗	Focus on security ontologies and standards.
Figliè et al., 2023 [36]	✗	✗	✓	✗	L	✗	✓	✓	✓	Focus on industrial challenges, including cybersecurity.
Rahman et al., 2023 [38]	✗	✗	✓	✓	✓	✗	✓	✓	✓	Focus on cyberattack taxonomies, which categorise attacks based on methods, locations, and consequences.
Bratsas et al., 2024 [32]	L	L	✗	✗	✓	✗	✗	✓	M	Survey the use of ontologies and knowledge graphs in cyber threat intelligence.
Hollerer et al., 2024 [46]	L	L	✗	✗	✓	✗	M	✓	✓	Survey on the features of ontologies in order to address the requirements of the OTS.
Wang et al., 2024 [48]	✗	✗	✗	✗	L	L	M	L	✗	Focus on integrating ontologies for semantic reasoning about unsafe states in human-centric Industry 5.0 environments.
Arazzi et al., 2024 [49]	✗	L	M	L	✗	✗	✓	L	✗	Proposes a lightweight ontology for Industry 5.0, integrating humans, devices, and processes.
Our Article	✓	✓	✓	✓	✓	✓	✓	✓	✓	Our review investigates whether the ontologies support goal-based IIoT cybersecurity knowledge representation and modelling, as well as their applicability for security modelling or potential for extension. We explore various use cases and applications, identify research gaps, and summarize future research directions.

✓	High coverage	M	Medium coverage	L	Low coverage	✗	Absent/No coverage

III. METHODOLOGY OF THIS SURVEY

A. SYSTEMATIC REVIEW PROTOCOL

The aim of this review is to analyse ontological and non-ontological resources to identify key security attributes for modelling safe and secure IIoT systems for critical and highly sensitive applications. To achieve this, we followed the well-known PRISMA guidelines and the Grant-Booth framework [50], [51]. These approaches ensured the inclusion of high quality and relevant articles while maintaining a comprehensive focus on the objectives of our study [52], [53]. Systematic reviews offer several advantages, such as: (I) enables comprehensive searching, filtering, analysis and comparison of existing research related to the topic of interest; (II) helps to identify contributions in the fields and understanding of concepts and terminologies; (III) supports identification of open problems, challenges, and research gap; and (IV) aids development and synthesis of ideas to improve the efficacy of existing methods or to innovate a new method to solve issues. Furthermore, the methodology of review protocol is summarised in Figure 1.

Research questions:

RQ: What are the key concepts, attributes, and ontological approaches to support safe and secure IIoT applications?

We refined the main research question into the following more specific sub-questions:

- **RQ 1:** What type of key security concepts and properties are being developed to secure IIoT devices?
- **RQ 2:** What are the main security concepts to represent the IIoT data collection and dissemination?
- **RQ 3**: What kind of security ontologies and vocabularies are available that can be used for the security modelling of IIoT devices and applications?
- **RQ 4**: Do existing security ontologies provide concepts and properties for security goals relevant to safe and secure IIoT applications?

Following the definition of the research questions, a set of key terms are derived and agreed upon by the authors. These terms were then combined using the Boolean operator to maximise the retrieval of relevant literature.

Search strings : Industrial Internet of things or IIoT ontologies or taxonomy or knowledge representation and security or cybersecurity

Inclusion filters: Selected studies had to satisfy at least one of the following three criteria. These criteria were carefully chosen to clearly define the boundaries of data collection for this review.

1) The research addresses the security of IIoT devices, including sensors, actuators, wireless routers, and any central or edge devices.
2) The research proposes security frameworks and attributes for dissemination of IIoT data to and from IIoT devices and infrastructure.
3) The semantic ontologies standard, developed by focus groups.

Exclusion filters: Non peer-reviewed or pre-print research except the following:

1) Unpublished IoT ontologies developed by the standardization bodies.
2) Research articles presented as poster papers, although they proposed security ontologies for IIoT devices.
3) Research that did not propose any framework, security attributes or ontologies.

B. DATA COLLECTION PLAN AND REPOSITORIES

To mitigate the bias in data collection, it is further decided that all authors will separately search by using search strings in a parallel and iterative manner. Adhering to the planned strategy, we performed a double semi-automatic search while focusing on article titles and abstracts. The rationale for performing double searching in title and abstract fields stems from evidence suggesting that title-only searches do not yield sufficiently relevant research data [54]. However, some researchers argue that the title, abstract, and keyword screening alone is not enough, advocating instead for full-text searches [55]. To minimise the retrieval of excessive unrelated and low-quality data, we avoided full-text searching. After defining the data collection plan, searches for relevant data were conducted in IEEE Xplore Digital Library, ScienceDirect, Springer, ACM Digital Library, Web of Science, Google Scholar, and GitHub repositories.

IV. CRITERIA FOR ONTOLOGIES ANALYSIS

Ontology classification is a criterion for observing and analysing characteristics of ontologies [56]. For the analysis, we consider several factors, including the type of ontology, supported features, online availability, conceptual and terminological similarities, and alignment with the security goals that can be achieved through the ontology.

A. CLASSIFYING ONTOLOGY TYPES

For analysis, ontologies are categorised in two distinct classifications: *the general or top-Level ontology* and *the application-level ontology*. The top-level or upper-level ontology includes abstract and overarching concepts that are universally applicable across various domains and these concepts are consolidated in a unified logical framework to represent the most general aspects of reality, such as the distinction between continuants (also known as endurants) and occurrents (also referred to as perdurants) [27], [31], [54], [55]. General security ontologies are abstract ontologies that could be extended to any domain applications, and

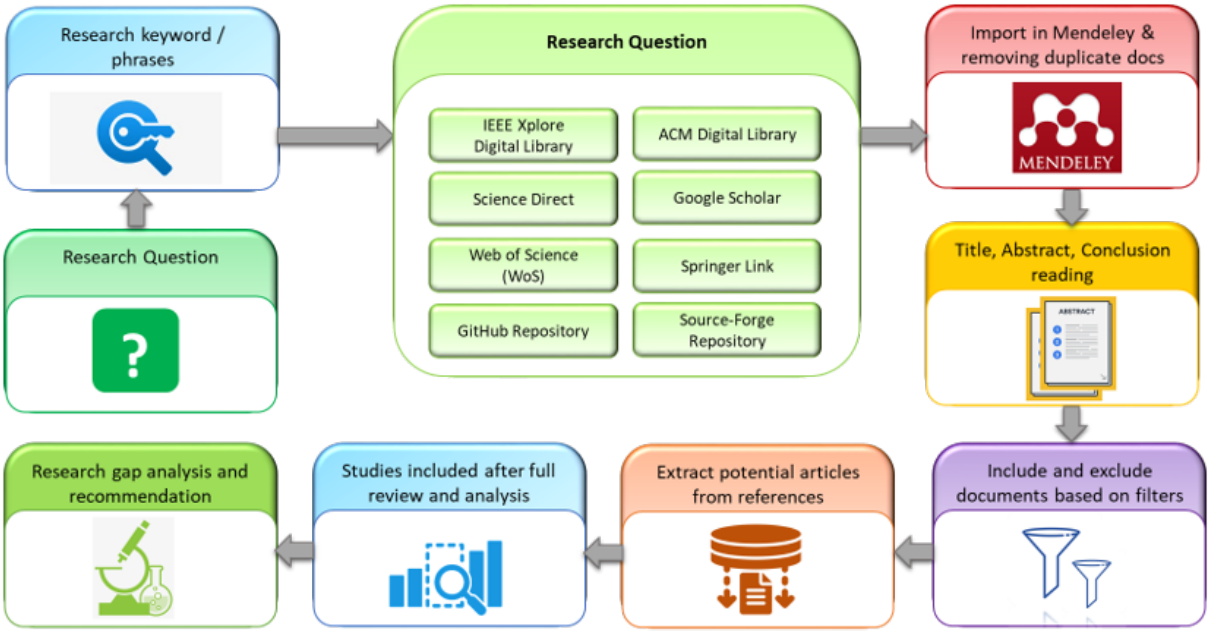

FIGURE 1: Research data collection and filtering methodology.

their specific features are modelled according to the targeted environment [57].

B. CLASSIFYING ONTOLOGY FEATURES

We analyse how concepts and properties in security ontologies differ from related ontologies, often using identical concepts under different names. Our analysis focuses on clarity, stability, and extensibility. *Clarity* assessment emphasises well-defined concepts and properties with sufficient metadata and annotations, ensuring their intended functionality in the security ontology [58]–[60]. *Stability* evaluation checks coherence and logical integrity across hierarchical structures of classes and object properties [61]. For *extensibility*, we verify that concepts and properties are broadly defined without unnecessary constraints, promoting reuse in other ontologies [60], [62].

C. SECURITY GOAL CRITERIA ANALYSIS

To address the security challenges of Cyber Physical Systems (CPS), a set of eight security goals has been identified from [63]. However, in the context of IIoT, Industry 5.0 framework and insights from a cybersecurity consultant, the scope of this study focuses on five security goals to ensure a more targeted and practical approach. We analysed how security ontologies address a set of five security goals such as availability, resiliency, safety, integrity, and confidentiality by examining their classes, properties, and cohesiveness [25], [64], [65]. From *availability*, we mean that the security ontology classes and concepts represent the situation of consistent accessibility of resources, assets and processes when needed in a timely manner and should also be able to self-heal within the stipulated time in case of successful cyberattack. For *resiliency*, we assess whether the security ontology provides any classes, properties and sufficient metadata to support the recovery and transformation of services, processes, or assets after causalities in a reasonable time [64], [65]. For *safety* goal we focus the safety definition as "the designed system should not put health of individuals, environments and associated assets at risk and also should be able to identify and mitigate the potential vulnerabilities" [63], [64]. *Integrity* mean that data or IoT device is accurate, consistent, and unaltered during sensing, actuating, storage or transmission. For *integrity*, we assess whether the ontology's concepts and classes adequately support integrity objectives. A security ontology must be equipped with the necessary metadata, classes, and properties to prevent and report any unauthorized alterations to the system's state, processes, or assets. For example, integrity of data is compromised if unauthorized change is made to the data received from industrial sensors or equipment. It is essential to guarantee modelling and implementation of integrity goals to ensure authorized update to a system. To analyse a security ontology for *confidentiality*, we examine whether it provides classes to support data protection in accordance with the UK Data Protection Act (UDPA) and ensure measures necessary to protect the privacy of collected and aggregated personal data.

V. MODELLING IIOT SECURITY WITH ONTOLOGIES

A. VULNERABILITY DESCRIPTION ONTOLOGY

The Vulnerability Description Ontology (VDO) developed by the National Institute of Standards and Technology (NIST) for characterising vulnerabilities found in various

forms in software, and hardware including Information Technology Systems (ITS), ICS, and medical devices [66], [67]. The classes and properties defined in the VDO support the Vulnerability Management Process (VMP) and facilitate the sharing of information among diverse stakeholders through a common language. This utility arises from the VDO's provision of a minimal yet comprehensive set of required classes and properties to model vulnerabilities across different devices and systems using ontological methods.

Contributions:

- The VDO provides metadata for vulnerabilities knowledge representation and management.
- It provides a comprehensive list of classes to represent and automate the analysis of vulnerabilities.
- It describes the relationships between various classes. For example, VDO identifies the scenario class semantic relationships with vulnerability, context, attack theater, product and type classess, where the scenario is a placeholder to allow a description of events surrounding the possible use of a single vulnerability.
- It comprises a minimum number of required classes for analysing and managing the vulnerabilities in any type of system, hardware or IIoT infrastructure.
- All classes are well explained, this increases the VDO's usability and extensibility and suitability to be used for IoT devices' VMP.

Limitations:

- The rigid classification of VDO classes into three categories—mandatory, recommended, and optional, as depicted in Figure 2) —may vary in pragmatic approaches. Moreover, classes might shift from one category to another.
- The VDO does not offer classes focused on security goals.

B. WEB OF THINGS SECURITY ONTOLOGY

The WoT working group has recently released Web of Things Security Ontology (WoTSO) for cross-domain interoperable security modelling [68]. It's main objective is to represent machine interpretable security mechanisms that could be applied to things in the IoT environments. The WoTSO contains nine classes, six objects, and eight data properties. Among them, the *SecurityScheme* is the main class that contains eight subclasses and relevant properties such as *name* and *in*. The *SecurityScheme* class like concept was previously proposed in Internet of Things Security (IoTSEC) with the name of *SecurityMechanism* [69]. The WoTSO is a partially general ontology because it describes some related concepts at the instance level. This ontology provides classes and properties with clear definitions and sufficient metadata so it can be extended independently. The WoTSO partially passes the security goals: resiliency and safety with *SecurityScheme* class and *authorisation*, *token* and *refresh* properties; the confidentiality security goal with *OAuth2SecurityScheme* class; the integrity security goal with *PSKSecurityScheme* class. Nevertheless, this ontology does not support the availability security goal.

Contributions:

- The WoTSO provides a basic set of classes, objects and data properties for managing the access and control of things over the web.
- The WoTSO defines classes and properties tailored to specific technologies and security protocols, facilitating the development and implementation of application-level ontologies.

Limitations:

- In WoTSO the classes are specialised and thus not suitable for reuse in top-level ontologies.
- WoTSO ontology exhibits significant issues regarding clarity, stability, and extensibility, as it lacks sufficient metadata for its classes and properties. For instance, object properties are specified without defining their corresponding range and classes.
- The WoTSO failed to include classes that address availability and recovery security goals.

C. REFERENCE ONTOLOGY FOR IOT SECURITY

The IoTSEC ontology focuses on semantic relationships among threats and security risks [69]. It is founded on the basis of component risk analysis and information security issues [70], [71]. The IoTSEC ontology contains several key classes, including *Asset, Threat, Vulnerability, SecurityMechanism, SecurityProperty, and TypeOfDefense* classes. The IoTSEC ontology has been used to model the security of IoT systems at design-time and operate-time [72]. The Design-Time Modelling (DTM) provides security services at the business processes and application-level, whereas operate-time security is aligned with monitoring and actuating of IoT devices for the industrial access and control. We categorise IoTSEC ontology as an application level ontology, characterised by limited metadata for its classes and properties. It supports safety security goals by providing the *SecurityProperty* class and partially addresses the confidentiality goal via the *AccessControlMethod* and *AuthenticationMethod* classes. Furhtermore, it contributes to the integrity goal through the *EncryptionAlgorithm* and *ChecksumAlgorithm* classes. However, it is important to note that the IoTSEC ontology did not explicitly state its security goals, which is our understanding.

Contributions:

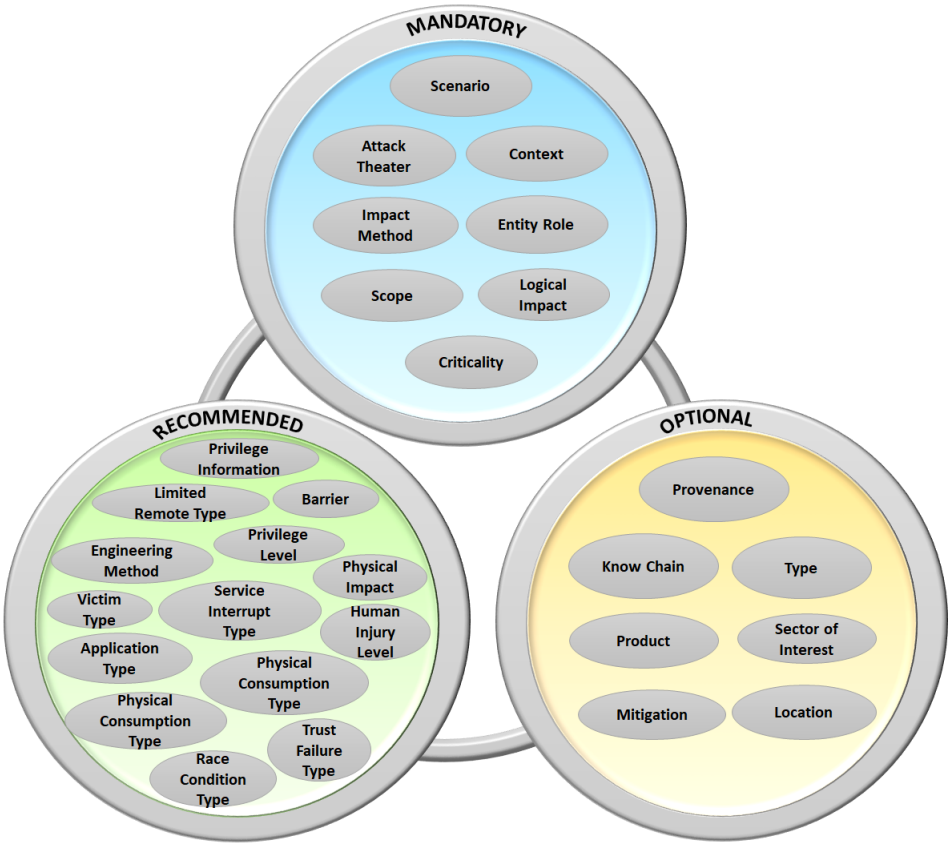

FIGURE 2: Vulnerability description ontology concepts classification.

- IoTSEC is a reference ontology for IoT security modeling, featuring clearly defined classes and properties.
- IoTSEC translates top level classes into second and third levels, encompassing subclasses and instances, to effectively represent application-level knowledge.
- The well-defined relationships among cybersecurity concepts will support analysis of the causes and effects of vulnerabilities on the assets in IoT and can be used to develop IIoT security ontologies.
- The proposed ontology introduces a *SecurityProperty* class, which can be utilised to enhance the articulation of security objectives for IoT devices and systems.

Limitations:

- The vulnerabilities related to human factors were not considered in the reference security ontology, which are essential for a comprehensive security model for IoT devices.
- Some concepts such as *Correction, Detection, Prevention, Recovery, Response* are represented as individuals. which limits the ability to add further attributes.

D. ATTACK AND COUNTERMEASURE

The Security Toolbox - Attacks & Countermeasures (STAC) is an an extension of M3 ontology [73], [74]. This ontology was specifically developed to enhance the security of M2M communication devices in the context of sensor network. To encapsulate various security concepts pertinent to this domain, the ontology introduces several key classes, including but not limited to *Attack*, *SecurityMechanism*, *Technology*, *SecurityProperty*, and *OSI Model*. According to our ontology feature definitions (section IV), STAC ontology supports the extendable feature. Due to strong cause and effect relationships among the classes, STAC ontology provides classes and properties to support resiliency, safety, integrity, and confidentiality security goals. Additionally, this ontology provides security mechanisms that can satisfy one or more security goals. For instance, Virtual Private Network (VPN) class satisfies integrity and confidentiality. The STAC ontology is available online in Web Ontology Language (OWL) format and can be accessed from [75].

Contributions:

- Propose classes and properties for threats and security mechanisms classification in the context of various technologies such as Sensor, Cellular, Wireless and M2M.

- Categorise attacks and security mechanisms according to the Open Systems Interconnection (OSI) model.
- Specifies the relationships between security mechanisms and security properties.
- Although the security goals are not explicitly discussed in STAC ontology, however, it provides a *SecurityProperty* class that can be used to complement security goals, including resiliency, safety, integrity, and confidentiality.

Limitations:

- The ontology lacks consideration of human factors influencing the security of IoT devices.
- Classes addressing security risks stemming from vulnerabilities and cyberattacks on IoT devices are absent.

E. CYBERSECURITY VULNERABILITY ONTOLOGY

While Cybersecurity Vulnerability Ontology (CVO) [57] was initially proposed to model general cybersecurity issues, its abstract concepts are versatile and can effectively apply to security modelling for the IIoT environments. The CVO was developed based on the NIST-VDO [70], [76]. It contains five core classes: *Vulnerability*, *Intelligence*, *Threat*, *Product* and *Countermeasure*. The *Countermeasure* class is focused on security mechanisms designed to address and mitigate vulnerabilities in products or assets, including firewalls, access control systems, and digital signatures [25]. The CVO's CounterMeasure concept is similar to IoTSEC and STAC's ontologies *SecurityMechanism* class [69], [73] and WoTSO's *SecurityScheme* class. Our review suggest that the *Intelligence* class might be useful for Industry 5.0 applications -where human and machine work together to protect the IIoT environments' security.

The CVO is not merely a general ontology; it offers clarity and extensibility in its features. The Semantic Sensor Network (SSN) ontology [77] can leverage the classes and properties provided by the CVO for modelling the security of IIoT devices. As shown in Figure 3, the SSN classes: Sensor and System (depicted in grey), have been assigned attributes such as *Threat*, *Impact*, and *Attack Complexity*, which have been adapted from the CVO ontology. These attributes enable the detailed representation of threats, impacts, and attack metadata in the context of IIoT devices.

Contributions:

- Proposed an ontology for vulnerability knowledge representation and threat intelligence.
- Evaluated a developed ontology through various quality parameters: accuracy, completeness, consistency.
- Ontological and non-ontological resources were used to develop CVO ontology classes and properties.
- A conceptual model for cyber intelligence was presented to provide insights into the relationships among various classes that enable cyber intelligence alerts and countermeasures.
- CVO classes and properties were defined with sufficient metadata and clarity that make it a better choice for modelling the security of IoT devices and applications.

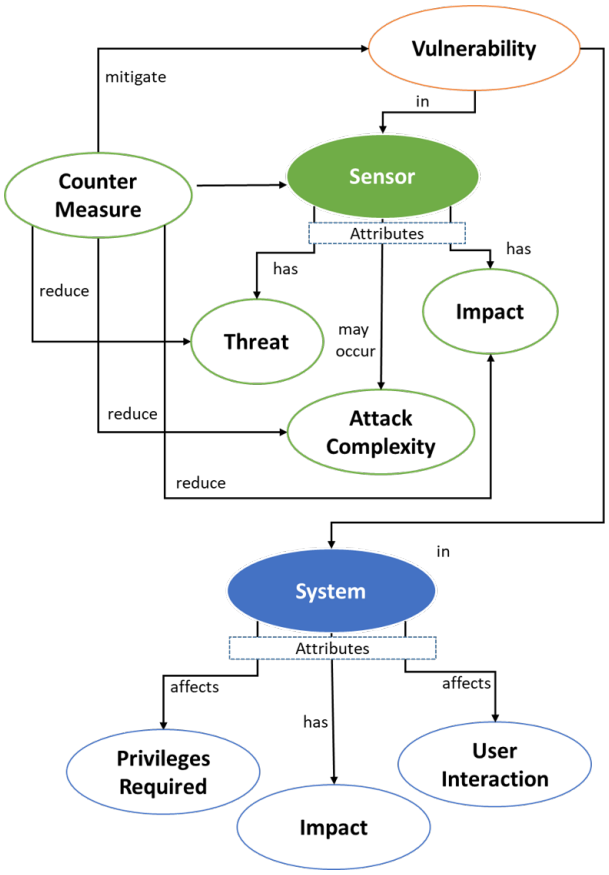

FIGURE 3: Example for using CVO with SSN ontology-classes from SSN are highlighted with green and blue colour.

Limitations:

- In CVO, many concepts have been reused from other ontologies and Twitter data that should be properly investigated for IIoT systems vulnerability management and threat intelligence alert systems.
- The CVO lacks classes that represent vulnerability management and threat intelligence alert systems in relation to security goals. Additionally, it does not account for the four key security domains: *People*, *Physical*, *Process*, and *Technical*.

F. SECURITY THREAT ONTOLOGY

The IoT Security Threat (IoTST) ontology delineates security attributes and includes inference rules for detecting attacks in the IoT environment [77]. This ontology contains five main classes: *Platform*, *Vulnerability*, *Weakness*, *Attack-*

Pattern, and *Campaign*. *Platform* represent entities that can be affected due to vulnerability. The *vulnerability* class is introduced to represent any weakness in IoT devices and communication systems, a similar concept used in other ontologies to address related issue such as IoTSEC [69] and CVO ontologies [57]. Additionally, IoTST proposes a new concept called *Campaign*, which represents a series of activities or attacks targeting a specific IoT device over a certain period. We classify this ontology as an application-level or non-general ontology, originating from the domain of security. The current structure of IoTST ontology is designed to support resiliency, integrity and confidentiality security goals. A side from the research paper by Zhang et al. [77], we were unable to locate any other online resources for IoTST.

Contributions:

- Developed reasoning process aids in the identification of vulnerabilities in IoT platforms and the isolation of nodes that are susceptible to these vulnerabilities.
- Proposed framework extends the existing information of network security and contributes to security threat ontologies domain.

Limitations:

- Similar concepts have been reinvented including *Platform, Weakness*, etc. Likewise, IoTST mainly focuses on threats and insufficiently addresses security goals including availability and safety.
- The IoTST metadata is insufficient for establishing connections to the four pillars of security domains: people, process, physical, and technology.

G. IOT NETWORK SECURITY AWARENESS

For analysing the security of IoT networks, Guangquan et al. [78] proposed the IoT Network Security Situation Awareness (INSSA) ontology. This ontology contains rules written in Semantic Web Rule Language (SWRL) and defines six core classes — *Context*, *Attack*, *Vulnerability*, *NetworkFlow*, *Alert*, and *Sensor*. The *Context* class represent various circumstances and aspects of security situation of IoT networks, devices, and applications. For instance, the IoT device situations could be safe, under attack, under a threat, or not accessible due to attack. The INSSA ontology contains *Alert* and *Sensor* classes, however, it does not provide metadata for classess, which weakens this ontology's clarity and extensibility feature. As researchers cannot reuse this ontology without sufficient metadata. Resiliency and safety goals are partially supported through the *Alert*, *Vulnerability* classes [64]. We were unable to find the online version of INSSA ontology.

Contributions:

- Support situation awareness to express the numerous circumstances and aspects of IoT environment's security.
- Introduce a new class of *NetworkFlow* to represent IoT data sources and network traffic.
- INSSA supports the modelling of safety and resiliency goals to some extent by introducing classes such as *Vulnerability* and *Alert*.

Limitations:

- INSSA does not provide enough metadata, thereby limiting extensibility and clarity. For example, while it mentions *Alert* and *Sensor* classes, their definitions, and purposes are not elaborated.
- Insufficient object property descriptions, lack of semantic relationships among the security classes, and insufficient metadata hinder the reuse of INSSA.

H. MODELLING INDUSTRIAL THREAT AND RISK ASSESSMENT

Alanen et al. [66] argue that the conflict between security and safety is intrinsically linked with the service's availability. They suggest that reducing service's availability can mitigate cyberattacks and threats, which result the protection of assets and infrastructure. However, they also highlight that if safety functions require continuous availability of processes and services then it is important to prioritise the protection of availability components such as network communications and devices. To balance the security, safety, and availability of a system in the industrial domain, they proposed four core concepts: *Imperfection*, *RAMSS*, *Riskcontrol* and *NegativeImpact*. The nomenclature of these concepts and their associated sub-concepts in the security threat modelling and risk assessment ontology is illustrated in Figure 4. This ontology meets the specified security goals of availability, resiliency, safety, integrity, and confidentiality. However, it falls short of being a general security ontology. Furthermore, it is adaptable for cybersecurity risk assessment in the IIoT environments, given its provision of adequate metadata and relevant classes.

Contributions:

- Proposed an ontological-based approach for safe vs available industrial control systems and risk analysis in case of fault and safety hazards.
- Developed a hybrid risk assessment ontology to harmonize the basic concepts between dependability, safety, and security.
- The developed hybrid ontology classes provide sufficient metadata for security goals: safety, availability, integrity, confidentiality, etc. in the industrial control systems domain, which can be reused for IoT devices' safety and availability modelling [79].

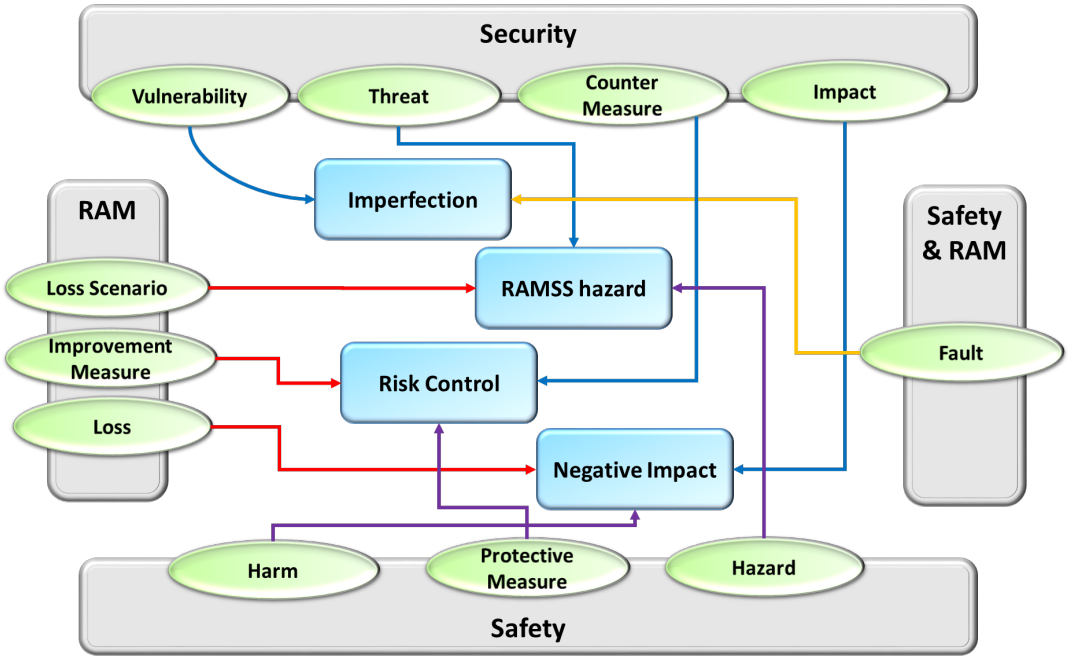

FIGURE 4: Key concepts in risk assessment and threat analysis model ontology.

- The hybrid ontology provides concepts to express events and processes for prevention and detection of confidentiality. As well, the ontology supports concepts to express violation of integrity through malicious alteration of data such as degrading the integrity of required service or system.
- The ontology is also useful for modelling balanced actions e.g., safety vs availability, by considering security threats and failure of devices; however, this work needs substantial extensions and changes.

Limitations:

- Proposed classes are insufficient for a holistic safe and secure industrial control systems representing people, process, physical and technical.
- Human factors have not been considered for risk assessment and analysis in the industrial control environment, which reduces the efficacy of the proposed ontology.

I. UNIFIED CYBERSECURITY ONTOLOGY

Zareen et al. [80] developed the Unified Cybersecurity Ontology (UCO) by extending Intrusion Detection System (IDS) ontology and reused many concepts from security databases including Common Vulnerabilities and Exposures (CVE)[1], Common Configuration Enumeration (CCE)[2], Common Vulnerability Scoring System (CVSS)[3], and Common Attack Pattern Enumerations and Classifications (CAPEC)[4]. Although UCO was not developed for IIoT systems, but can

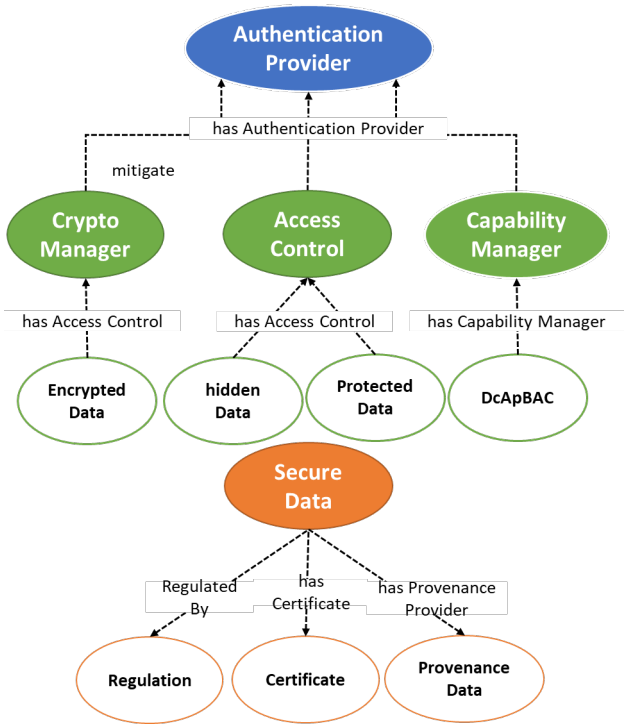

FIGURE 5: Access control and secure data classes relationships with other classes using object properties.

[1]https://cve.mitre.org/
[2]https://cce.mitre.org/
[3]https://www.first.org/cvss/
[4]https://capec.mitre.org/

be used for them as it contains many well known classes such as *Attack*, *AttackPattern*. The core classes of UCO - namely *Attack*, *AttackPattern* , *Exploit*, *Exploit Target*, and *Indicator*, these classes characterise the various methods used for executing cyberattacks, including techniques such as buffer overflow, SYN flood, port scanning, and delays in sensing. The Attack class describes a threat that exploits vulnerability of assets, this class was similarly proposed in INSSA ontology [78]. The *AttackPattern* class describes common patterns or campaigns used by attackers to exploit asset weaknesses. For example, attackers may use specific types of activities with data instances to deceive a machine learning-based protection system. Another example is a kill chain attack, where a series of actions are executed to destroy an asset or IIoT infrastructure. The *AttackPattern* class is used with the same name for a similar purpose in IoTST ontology [77], and under the different name *AttackPopularity* in STAC ontology [73]. The *Exploit* class provides descriptions of an individual exploitation of vulnerability of an asset or product or an IIoT device. The *ExploitTarget* class supports the representation of cybersecurity vulnerabilities or weaknesses in IIoT devices, software components, or communication channels that are susceptible to exploitation by the tactics, techniques, and procedures (TTP) of threat actors [81]. The *Indicator* class describes certain patterns and observable conditions regarding the cybersecurity attack and effects of countermeasures. The UCO is available online in OWL format and can be accessed from [82]. We classify UCO as a general cybersecurity ontology with potential applications in IIoT environments.

The UCO provides extensive metadata, thereby supporting the clarity and extensibility features of ontology. However, it lacks stability due to inconsistencies among classes; for instance, discrepancies exist between the vulnerability and weakness classes. UCO supports resiliency and safety security goals through *Consequences* and *CourseOfAction* classes, which provide metadata to model relevant features. Additionally, UCO offers partial support for the confidentiality goal by incorporating subclasses such as *LossOfConfiguration*, *UnAuthUser*, and *PrivilegeEscalation*.

Contributions:

- Unlike other ontologies, UCO supports integration with existing cybersecurity knowledge available in public knowledge bases.
- UCO provides a cybersecurity ontological method for several use cases to identify vulnerabilities and provide coalescing real-world information with cybersecurity knowledge.

Limitations:

- UCO has limited support for time-based reasoning as the present version has only basic time representation which can limit the security of IoT devices time series data. Currently, in UCO, time is expressed as a data property that is linked with the event class.
- UCO does not support sociotechnical factors, nor does it support the stability and availability security goal.

J. SAFETY, SECURITY, AND RESILIENCY METAMODEL

To enhance safety and security of CPS, the metamodel ontology proposed by Bakirtzis et al. [83]. It contains five categories of basic classes: *Safety*, *Security*, *Resiliency*, *Physical* and *Functional*. The classes for safety, security and resiliency elements include *Resilient_Mode*, *Attack_Vector*, *Loss_Scenario*, *Sentinel*, *Unsafe_Action*, *Hazard*, *Loss*, *Context*, *Control_Action* and *Feedback*.

Based on the classes and properties descriptions, this ontology meets three security goals (Resiliency, Safety, and Confidentiality) and two ontology features (Clarity and Extensibility). Metamodel ontology cannot be characterised as stable due to class inconsistencies and lack of semantic connections among the classes. For example, the classes *LossScenario* and *Loss* are related, but it does not define any relationship or purpose linking the two. Similarly, the *Feedback* class should have a relation to the *ResilientMode* class to provide feedback before or after the resilient mode trigger, but the ontology lacks properties to support this connection. This ontology is available online at [84].

Contributions:

- The proposed approach complies with safety, resiliency and availability security goals as well as clarity and extensibility ontology features.
- To achieve resilience, safety and security requirements a metamodel was proposed. Based on the safety model, a cybersecurity system is developed to provide a linkage between security and safety concepts.
- The metamodel supports trade-space analysis for resiliency, safety and security related defilement harms.
- GraphQL-based implementation is given to incorporate ontological properties and attributes.

Limitations:

- Due to the variation and inconsistency in classes and missing properties among several classes, a semantic gap is realised.
- This ontology could not be characterised as a stable version because there is inconsistency in classes and some classes are not semantically connected through properties with other classes, including *Loss scenario*, *Loss* and *Feedback*.

TABLE 2: Ontology classification and feature comparison.

Study	Ontology type	Feature				Security goal					Online availability
		Security base	Clarity	Stable	Extendable	Availability	Resiliency	Safety	Integrity	Confidentiality	
[67]	△	✓	✓	✓	✓	✗	✗	✗	✗	✓	Not available online
[68]	□	✓	✓	✗	✓	✗	✓	✓	✓	✓	Yes, can be accessed from [85]
[69]	△	✓	✓	✓	✓	✗	✗	✓	✓	✓	Yes, available in OWL format [86]
[73]	△	✗	✗	✗	✓	✗	✓	✓	✓	✓	Yes, can be accessed from [87]
[57]	△	✓	✓	✗	✓	✗	✓	✗	✗	✗	Not available online
[77]	△	✓	✗	✗	✓	✗	✓	✗	✓	✓	Not available online
[78]	△	✓	✗	✗	✗	✗	✓	✓	✗	✗	Not available online
[66]	□	✗	✓	✗	✓	✓	✓	✓	✓	✓	Not available online
[80]	□	✓	✓	✗	✓	✗	✓	✓	✗	✓	Yes, available in OWL [88]
[83]	□	✗	✓	✗	✓	✗	✓	✓	✗	✓	Yes, available in GraphQL [89]
[90]	△	✓	✗	✗	✓	✗	✗	✗	✓	✓	Yes, available in OWL format [91]

□ General △ Not-general ✓ Supported feature ✗ Unsupported feature

K. IOT DATA SECURITY ONTOLOGY

Gonzalez-Gil et al. [90] have developed ontology for IoT data security (DS4IoT) by utilising a bottom-up approach. The bottom-up approach involves building the ontology by identifying and organising specific instances or data into broader concepts. DS4IoT's main contribution is provisioning of classes to address integrity security goal, which is pivotal to ensure that data is transmitted from sensor nodes to edge or central storage locations without unauthorised modification or leakage [64]. Additionally, it guarantees the detection of any alterations resulting from malicious injections by attackers. The DS4IoT contains twenty-five classes including two core classes: *SecureData* and *AccessControl*, sixteen object properties and three data properties. The *SecureData* class is further sub-categorised into *SecretData* and *ProtectedData*. In the context of IoT applications, secret data refers to hidden and encrypted information, while protected data is accessible to authorised users. Similarly, *AccessControl* class is sub-categroised into Attribute based Access Control (ABAC), Identity based Access Control (IBAC), Organization based Access Control (OrBAC), Rule based Access Control (RAC), Distributed Capability based Access Control (DcApBAC) and Role based Access Control (RBAC). These categorisation can support the access control mechanism modelling of IIoT devices. Figure 5 shows the semantic relations between the DS4IoT classes for core concepts *SecureData* and *AccessControl*. As DS4IoT ontology was developed using bottom-up approach, so we classify this as non-general ontology. However, it can be considered domain-specific security ontology, as it was built from scratch to address IoT security. Authors of DS4IoT ontology did not provide sufficient metadata, so it can not be ticked for ontology clarity feature. The DS4IoT ontology is available online in OWL format and can be accessed from [92].

Contributions:

- The DS4IoT approach supports the integrity security goal and improves the ontological representation of security behaviours associated with the exchange and accessibility of data.
- The DS4IoT provides a common vocabulary for security concepts related to data access and exchange. It also offers mechanisms for data annotation to support access control, maintain data provenance, and ensure compliance with certification standards.

Limitations:

- The ontological method limits clarity and stability features due to insufficient metadata.
- The DS4IoT ontology does not provide classes that support the availability, resiliency, and safety goals required to comply with IIoT security requirements.

The ontologies discussed have several limitations, including rigid classification, lack of focus on security goals, and insufficient consideration of human factors. Certain ontologies have poor clarity, stability, and extensibility, while others fail to address key security domains like availability, safety, and recovery, hence limiting their practical use in IIoT security. For contrast and comparative analysis, summaries of ontology classifications, feature comparisons, and individual limitations are presented in Tables 2 and 3, respectively.

VI. KEY CONCEPTS AND ATTRIBUTES FOR MODELLING IIOT SECURITY

Building on our systematic review and the discussions in Sections V and VI, Figure 6 provides a high-level summary of key security attributes, required security goals, principal area of vulnerability and things in the IIoT context. Additionally, this section provides a detailed analysis of key concepts and attributes used in security ontologies, frameworks, and methodologies.

A. THREAT CONCEPT

Threat is a potential danger to an asset that affects specific security attributes when it exploits any vulnerability, whether physical, technical, or administrative [57], [76]. Mozzaquatro et al. [69] contended that the concepts of threat and attack are analogous, defining both as indications of potential harm to assets. Cyber threats can be both active and passive. Active threats disrupt and interrupt IIoT devices, potentially hampering their availability and safety [93]. Conversely, passive threats can be more detrimental to privacy in CIoT and secrecy in IIoT. Information obtained through passive threats can also be used for opportunistic attacks. The threat definition by Fenz and Ekelhart [76] is particularly relevant to potential attacks on Industrial Control Units (ICUs) when connected to computer networks and IIoT devices. For example, threats to safety may arise from exposed private Message Queuing Telemetry Transport (MQTT) server on the internet that are used to actuate and control fire exit doors in a shopping centre.

Definition (Threat): *Threat concept represents the characteristics of a potential danger to physical and non-physical IIoT assets that impact on enterprise entities and jeopardise safety, availability, accountability, productivity, and reputation.*

Attributes: The attributes identified for the threat concept are described in detail below and illustrated in Figure 7.

- **Source:** Source describes the nature of threat, categorising it as either accidental or intentional [76], [94], [95]. For example, Distributed Denial of Service (DDOS) attack on sensing and actuating devices used to manipulate industrial process is a kind of intentional threat, however crashing the MQTT server due to too many pub/sub requests from the Operational Technology (OT) device error is a kind of accidental threat. Usually, the accidental threat arises due to failure of processes or unexpected technical issues, whereas intentional threat refers to purposeful actions that are normally preceded by human beings or bots.
- **Origin**: The origin of a threat can be classified as either human or natural [76]. For example, the risk of potential attacks arising from human habits and mistakes when interacting with IIoT devices is referred as the human-origin threat. By contrast, natural-origin threats may arise from events such as fire, flood, wind, or earthquakes and, in their turn, they can affect communication devices, sensors and actuators. Human-origin threats can be prevented with training, such as awareness programs, and quite commonly implemented as the Standard Operating Procedures (SOPs).
- **Capability:** Whether the threat capability is active or passive and does it have the capability to control and stop the functions of IIoT devices, or it can just monitor the exchange of data. For example, in eavesdropping attack the attacker monitors data and in spoofing attack they insert fake sensor or actuator device in the network for illegitimate advantage through exploiting MQTT or Constrained Application Protocol (COAP) [69], [96].
- **Campaign:** Campaign describe whether the threat is part of a coordinated crusade using a specific cyberattack method [80]. Mostly, targeted threats are carried out against the critical CPS, BMS, and payment gateways. For example, the Ukrainian power grid experienced a cyberattack that disrupted the availability of grid services, it's resulting in the tripping of breakers and the interruption of electricity supply to 225,000 customers [97].
- **Impact:** The impact attribute provides information on whether the threat can affect people, processes, and physical and technical assets. A threat can impact IIoT devices and services, and compromise their safety, availability, integrity, and privacy functions [66], [98]. For instance, a potential eavesdropping threat can negatively impact the integrity of IIoT data, and it may also restrict the accessibility of IoT devices, as a result it reduces the availability of IIoT services.

B. VULNERABILITY CONCEPT

The NIST standard 800-12 and VDO characterise vulnerability as a weakness in system hardware, internal controls, or system codes as well as these sources emphasise that system deficiencies can be exploited by an attack source [67], [98]. Most cybersecurity ontologies and frameworks [25], [57], [66], [69], [77] adhere to the vulnerability definition proposed by the NIST [98]. According to the Industrial Internet Consortium Security Framework (IICSF), the vulnerability is a weakness of system that can be exploited by a threat to target the same asset or other interconnected assets [64].

TABLE 3: Identified Limitations in Ontologies for IIoT Security Modelling.

Title	Reference	Limitation
Vulnerability description ontology (VDO)	[67]	The rigid classification of VDO classes into mandatory, recommended, and optional categories may vary in pragmatic approaches and classes might shift between categories. Additionally, VDO does not offer classes focused on security goals.
Web of things security ontology (WoTSO)	[68]	The WoTSO ontology is unsuitable for reuse in top-level ontologies, lacks classes for safety and recovery, and exhibits issues in clarity, stability, extensibility, and metadata, including undefined object properties.
Reference ontology for IoT security	[69]	The vulnerabilities related to human factors were not considered, which are essential for a comprehensive security model for IoT devices. Some concepts such as correction, detection, prevention, recovery, and response are represented as individuals. Which limits the ability to add further attributes.
Attack and countermeasure (STAC)	[73]	The STAC ontology lacks consideration of human factors influencing the security of IoT devices. Classes addressing security risks stemming from vulnerabilities and cyberattacks on IoT devices are absent.
Cybersecurity vulnerability ontology (CVO)	[57]	CVO reuses concepts from other ontologies and Twitter data without fully addressing IIoT vulnerabilities and threat intelligence. It lacks security-focused classes and excludes the key domains: People, Physical, Process, and Technical.
Security threat ontology (IoTST)	[77]	Similar concepts have been reinvented including Platform, Weakness, etc. Likewise, proposed ontology mainly focuses on threats and insufficiently addresses security goals. The IoTST metadata is insufficient for establishing connections to the four pillars of security domains: people, process, physical, and technology.
IoT network security situation awareness (INSSA)	[78]	INSSA lacks sufficient metadata, limiting clarity and extensibility. Definitions for key classes like Alert and Sensor are vague, while inadequate object property descriptions and semantic relationships hinder reuse and functionality.
Industrial threat and risk Assessment	[66]	Proposed classes are insufficient for a holistic safe and secure industrial control systems representing the four pillars of security domains. Human factors have not been considered for risk assessment and analysis in the industrial control environment, which reduces the efficacy of the proposed ontology.
Unified cybersecurity ontology (UCO)	[80]	UCO does not support sociotechnical factors, nor does it support the stability and availability security goal.
Safety, security, and resiliency metamodel	[83]	This ontology could not be characterised as a stable because there is inconsistency in classes and some classes are not semantically connected through properties with other classes, including Loss scenario, Loss and Feedback.
IoT data security ontology (DS4IoT)	[90]	DS4IoT ontology lacks classes for availability, resiliency, and safety, limiting IIoT security compliance. It also lacks clarity, stability, and essential features due to insufficient metadata.

ISO/IEC 27000 also addresses vulnerability, defining it as a "weakness of an asset or control that could be exploited by one or more threat sources." Vulnerability can be in administrative, physical, or technical fragility form that affects tangible and non-tangible assets and subsequentially has impacts on various security goals. Vulnerability definition from the National Vulnerability Database (NVD) is more relevant in the context of IIoT vulnerabilities [99].

Definition (Vulnerability): *A vulnerability is a weakness in the targeted IIoT system (that has significance), arising from either administrative or technical reasons, which could be exploited by a threat to gain unauthorized access.*

Attributes: The identified attributes for *Vulnerability* concept are illustrated in Figure 8 and described as follows:

- **Type:** This attribute represents the metadata whether the vulnerability is technical, administrative, or physical. Research studies [67], [76] used vulnerability type attribute to explain the relationship between the relevant weakness and appropriate required control to safeguard assets from the threat. Research article [100] applied vulnerability type attribute to indicate various types of vulnerabilities. For example, DDOS, overflow, memory corruption of IoT devices, bypass security checks of interfaces used to connect with industrial machines, etc. CVO [57] also has adopted vulnerability type from [100] and used as a sub-concept of vulnerability to represent various types of vulnerabilities in the cyber ecosystem.

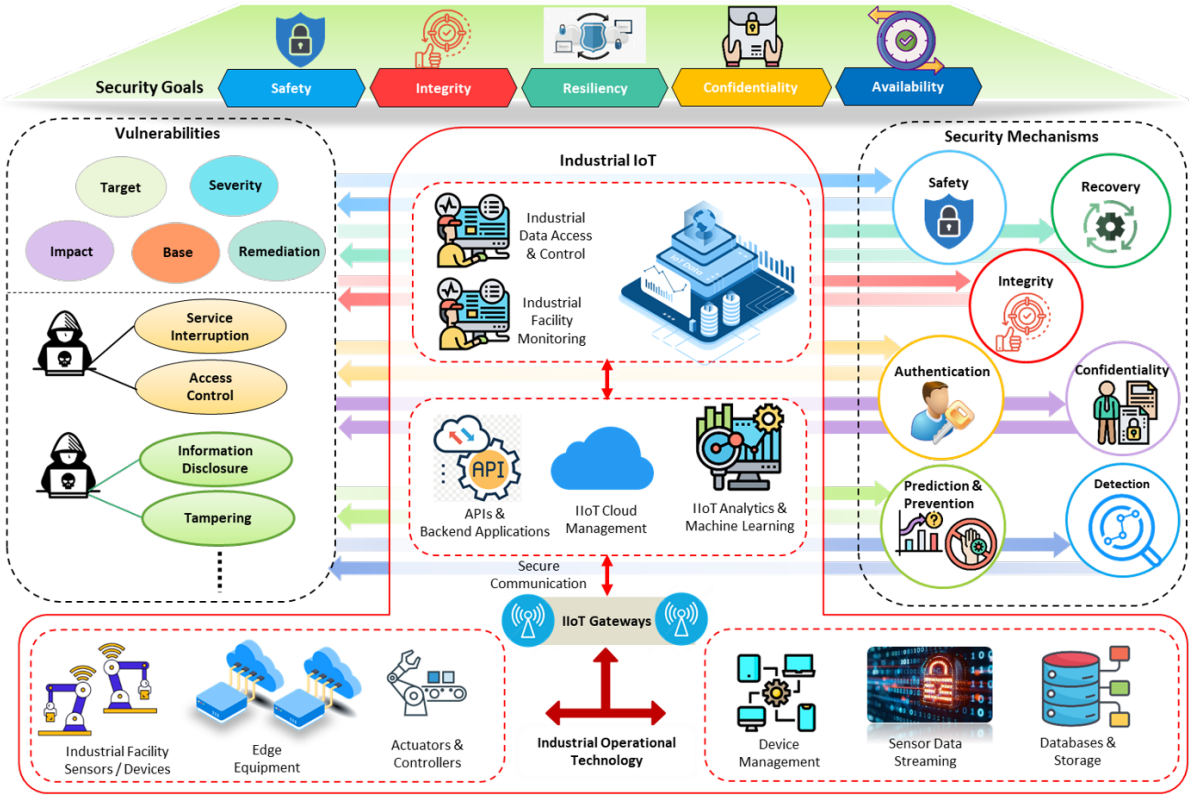

FIGURE 6: High-level summary of key security attributes and components in IIoT.

FIGURE 7: Attributes for threat concept.

- **Target:** This attribute showcase metadata for specific security weakness of asset which potentially be exploited by the threat for a specific period. For example, in the Critical National Infrastructure (CNI) IoT device is attacked when a communication link established for collecting data for a limited period. Another example is in IIoT ecosystem where communication channels are protected, however, IoT devices are left unprotected due to energy harvesting or any other miscellaneous issues. Even if IoT devices are well-protected, vulnerable connected legacy OT devices could still enable a cyberattack [64]. This attribute plays a critical role in facilitating a prioritised response to potential threats based on the specific and focused data and metadata available [77], [80], [101]. It further enables the triggering of appropriate actions, such as ensuring safety, availability, resiliency, and recovery.
- **Severity:** This attribute represents the characteristics of vulnerability levels such as low, medium, and high [76], [102]. It further determines which security measure or control could be useful to mitigate the level of vulnerability [69]. For instance, which control should be activated through a Supervisory Control and Data Acquisition (SCADA) system to prevent the threat. Study [57] suggests that the range for vulnerability severity should be from 0 to 10 with some related qualitative severity ranking – the score between 9.0 and 10.0 labelled as critical vulnerability. The greater the vulnerability severity value, the greater impact of threat on the asset and requires sophisticated mitigation con-

FIGURE 8: Attributes for vulnerability concept.

trol. The severity of vulnerability could be determined through the potential scale of damage to the critical infrastructure, threat impact on the assets, and affected security goals (i.e., confidentiality, availability, safety, resilience, integrity).

- **Impact:** Studies [103], [104] refers that the impact attribute represents the characteristics of effects on the assets when the vulnerability is successfully exploited. Article [66] suggests that security vulnerability impacts in a negative sense, however, this attribute also represents the positive side of impact. The impact attribute can be used in both logical and physical consequences [67]. Logical consequences include actions such as unauthorized write or read access to IoT devices, device removal, service interruption, or privilege escalation. Physical consequences may involve asset damage, human injury, or physical resource depletion. Examples of logical and physical consequences include unauthorized access to smart grids and machines, information disclosure, unauthorized modification of device configurations, and excessive electricity and water usage resulting from the exploitation of vulnerabilities.
- **Environmental/Contextual:** In cybersecurity, the contextual attribute is used as a main class for situation detection, threat risk analysis and transitioning the CPS state from resiliency to safety and availability [78], [83], [105]. This attribute represents the characteristics of a vulnerability that are only relevant in a particular context and environment [100]. The data characteristics of this attribute can be either dynamic or static, depending on the context. Additionally, the severity of a vulnerability can be deduced from the contextual attribute. For instance, a vulnerability that an attacker can successfully exploit in order to gain access to the connected machine whose unpredictable behaviour can be harmful to the workers on other hand attacker exploits vulnerability of a device that controls the temperature of chiller have two different context and severity. Furthermore, some vulnerabilities may instantiate when the connected IIoT device transmits or receive data to or from a central server or edge device.
- **Temporal:** This attribute represents the characteristics of a current level of vulnerability that change over the time and not among the contextual [100]. For instance, outdated and legacy industrial controls and relevant IIoT components often fail to update their firmware and that vulnerability could eventually emerge and easily exploited if the devices are not updated.
- **Base:** The *Base* attribute characterises vulnerabilities that are invariant, independent of specific contexts and consistent across different environments. These vulnerabilities are intrinsic to the system and unaffected by external factors, making them constant threats regardless of situational changes or environmental conditions [100], [106].
- **Remediation:** Article [102] consider the remediation as a process which is required to control the vulnerability. Study [57] used remediation as a control level that is required to solve the existence vulnerability, however, study [67] used mitigation keyword for the same purpose which describes protection mechanism that limit vulnerability from further expansion. Therefore, the remediation attribute represents the characteristics of processes that are required to fix the asset's vulnerability before it is used by the attacker against the asset. For example, a remedy of multi-factored authentication can solve weak authentication vulnerability and limit the attacker to gain access to autonomous excavator arm and alteration of its pre-programmed behaviour which can further improve the safety concerns in the IIoT. Another example of multi-factored authentication remedy could make it difficult and challenging for attackers to gain access to smart meters in the smart grid, which could be used to infect other smart meters in device hijacking cyberattacks [107].

C. SECURITY MECHANISM CONCEPT

The STAC [73] and IoTSEC ontology [69] sheds light on *SecurityMechanism* concept and describes it as "a process that satisfies the security properties" where security properties are the attributes of devices and information that might be affected by the successful cyberattack. Syed et al. [57] have used *CounterMeasure* instead of *SecurityMechanism* and described it as a protection mechanism that is required to

secure devices, machines, protocols, firewalls, authentication mechanism, digital signature and data. similarly, Alanen et al. [66] proposed *ProtectiveMeasure* and *CounterMeasure* concepts instead of *SecurityMechanism* concept. According to research study [66], the *ProtectiveMeasure* property reduces the risk which is involved in the safety and increase the availability of services. Additionally, authors [66] characterise cryptography, access control of machines and backup of data and metadata actions with the *CounterMeasure* concept. The WoTSO proposed *SecurityScheme* concept and explains that it is the metadata that represent the configuration of security mechanism [68]. Study [98] informed that security controls[5], *Safeguard*, and *CounterMeasure* are synonyms and we believe that these are the attributes of *SecurityMechanism* concept, which can be described as "the management, operational, and technical controls for a system to protect the confidentiality, integrity, and availability of system and its information". The NIST definition is more relevant in the context of IIoT which necessitates a holistic cybersecurity approach that ensures the safety of people, availability of processes, accessibility of controls with secure authentication and security of physical assets. Therefore, we proposed that the *SecurityMechanism* aptly represent the cybersecurity metadata and configuration aspects for IIoT ecosystem that characterises various types of measures: predictive, deductive, detective, preventive, corrective, recovery, safety, availability, and confidentiality.

Definition (Security Mechanism): *This concept characterises the practices that protect IIoT systems from threats and keep them safe and intact as designed and ensure the availability, confidentiality, and integrity.*

Attributes: The attributes identified for *SecurityMechanism* concept are described below and illustrated in Figure 9.

- **Availability:** This attribute represents the characteristics of security mechanism designed to ensure the timely and reliable access to sensors, actuators and their data in the IIoT ecosystem [64], [98], [108]. However, in some cases, these security mechanisms tries to reduce the availability of IIoT devices to protect them from the cyberattack [66], [109]. While this reduction in availability can enhance security, it may also compromise safety in the IIoT environments.
- **Integrity:** This attribute represents metadata associated with security mechanisms that ensure the truthfulness of devices and their data originality as well. It focuses that the capability of security mechanisms to safeguard data during transmission between devices to industrial units (i.e., machines) or central database servers, additionally, it ensures that the devices operate as designed throughout the process [64], [110]. The ISO/IEC 27000 categorises the integrity as a primary attribute of a security and it is also directly related to the safety attribute [108], [111].
- **Safety:** From a cybersecurity perspective, the safety attribute represents metadata related to protecting the people, assets, and environments against potential risks arising from system malfunctions or cyberattacks targeting safety-critical IIoT devices and networks [112]. The security mechanism should be capable to detect potentially hazardous conditions caused by cyberattacks and respond in a way that could minimize the damage. The ISO/IEC 27000 categorises safety as a primary security attribute, emphasizing its direct relationship with availability and integrity [108], [111]. Several ontologies, such as the ontology for safety, security, and dependability risk assessments, and STAC [73], [74], as well as the ontological metamodel for safety, security, and resilience [66], explore the safety attribute and related concepts in the context of ICS.
- **Confidentiality:** Confidentiality is a primary security attribute that defines mechanisms designed to prevent the disclosure of information to unauthorized parties [64], [108]. This attribute is particularly crucial when IoT devices capture sensitive personal data, such as in healthcare monitoring use cases, where enhanced protection mechanisms are required. Confidentiality can be further divided into sub-attributes that address protection mechanisms for data at rest, data in motion, and data in use [113].
- **Prediction:** This attribute characterises the security mechanism that enables the forecasting of security incidents, such as device failures due to severe weather conditions, cyber threats, or successful cyberattacks. The prediction attribute is directly related to availability, safety, and confidentiality. For example, a cybersecurity mechanism capable of predicting cyberattacks by detecting malicious behaviour in safety-critical IoT devices and industrial control units can mitigate potential hazards to people, environments, and assets [64], [114], [115].
- **Detection:** The detection attribute refers to the metadata associated with a security mechanism's ability to differentiate between malicious and non-malicious events in the IIoT ecosystem. For example, detection of modified sensor data, detection of false devices in the network, device failure detection, eavesdropping detection, etc. This attribute represents various detection approaches: proactive, retroactive, automated dynamic or static, manual automatic or dynamic [116], [117]. The selection of an appropriate detection approach depends on the services' criticality and IoT devices' computing and energy resources capability. The detection attribute has direct relationship with availability, safety, resiliency, and confidentiality [108].

[5]Security controls are attributes that protect various forms of assets (e.g., data, IoT devices, workstations, reputation) and are important to an organisation.

FIGURE 9: Attributes for security mechanism concept.

- **Prevention:** This attribute characterises the security mechanisms that provide deterrence against both static and dynamic cyberattacks, protecting people, assets, and the environment from potential negative consequences. The prevention attribute can also be viewed as part of resiliency, equipping devices to withstand cyberattacks [118]–[120]. In the realm of cybersecurity, prevention mechanisms typically react based on the output of detection mechanisms [64], [108]. For example, if an intruder is identified within a segment of the network and workstations through proactive threat detection, that information is relayed to the prevention mechanism, which then isolates and disconnects only the affected part of the network and its nodes/machines. This targeted response can prevent a system-wide shutdown and mitigate the risk of commercial disruption (e.g., in supply chain and factory scenarios). Prevention mechanisms can take many forms, similar to detection, such as preventing data loss, unauthorized access, and device control breaches.
- **Correction:** The corrective attribute represents the metadata of security controls that implement corrective measures to mitigate the impact of hazardous cybersecurity incidents [121], [122]. These measures help to protect IoT devices, their data, and related systems from further damage, which is why some studies consider corrective actions as countermeasures [57], [66], [95]. For example, if a cyberattack infects an edge device in a larger IIoT network, causing it to behave abnormally and send broadcast packets that congest the network, corrective controls would take several actions: isolate the infected edge device, install a new instance of the edge device, and re-route IIoT traffic through the new instance.
- **Recovery:** The recovery attribute has a direct relation to availability and safety aspects in the IIoT. It characterises those aspects of security mechanism which automatically or manually restore devices or services from a death state to a normal runtime state [64], [83]. In critical IIoT applications, a replica of the system operates in parallel with the main components, allowing for restoration if the primary system fails due to vulnerabilities or security breaches. Incident response and recovery security mechanisms are crucial attributes for critical IIoT infrastructure. These mechanisms can be developed through accurate estimation and analysis of security risks, vulnerabilities, and cascading impacts on assets [123]. It is also recommended that the replica system be physically isolated from the main system while continuously updated and maintained.
- **Authentication:** This attribute characterises the security mechanism's capability to establish that IIoT devices are what they claim to be and includes security controls that attest to and can verify the authenticity of the IoT devices [108], [124]. For example, a lightweight multi-factor authentication controls are vital for restricting false devices entry into the IoT network and protecting the authenticity of communicating parties

and confidentiality and integrity of exchanged data [64], [67], [125]. Authentication attribute is also important for IoT enabled CNIs domain because it has direct relationship to availability, resiliency, and safety aspects of security.

- **Authorisation:** This attribute represents the capability of security mechanism that ensure the access rights to devices in relation to assets and limit access to privileged devices [108], [124]. Authorisation attribute has been used in WoT ontology to represent Uniform Resource Identifier (URI) of security controls that deals with such a function [68]. Vulnerabilities could impact authorisation security controls in which IoT devices might be exploited illegitimately beyond the authorised privileges [57]. For instance, a train passenger device may receive privileges to access on-board services (e.g., music, movies), but that device might gain access to other system controls beyond the authorised services.
- **Non-Repudiation:** The ability of security mechanism which traces the devices' involvement in a particular event or transaction during normal situation as well as security attack. The IIoT security framework [64] explain repudiation as "denial that a person or device involved in a particular transaction or event" whereas Sangchoolie et al. [108] consider non-repudiation as a security attribute which has "ability to prove the occurrence of event and its originating entities to ensure that an entity or device cannot deny that it performed the action". NIST standar 800-213A [124] consider logging instead of non-repudiation which might needed to know that how organisation has implemented security mechanism. Additionally, NIST elaborate logging is the ability of the device or an interfaced system, to generate and store the device specific events, similarly [126] suggested non-repudiation as a subclass which is used to represent the metadata for security mechanism's accountability.

D. ASSET CONCEPT

W3C - Asset Description Metadata Schema (ADMS) defines an asset as highly reusable metadata and reference data [127]. The term "Asset" is both a common and abstract that has been used in many security ontologies. It can be suitable for a base security ontology [25], [66], [69], [72], [128]. Asset can represent configuration management in Information Technology (IT), OT, software and hardware, or integrated subsystems which can be impacted by vulnerabilities as well as used to protect other components in the IIoT ecosystem [64]. Jbair et al. [129] defines that "Assets are Industrial Cyber Physical Systems (ICPS) components and services that threat actors aim to compromise". Assets can include information, software, devices, people[6] and their skills and knowledge [66]. The IoT security maturity model [95] emphasizes that asset management is the sub-domain of security enablement and can be put in place to protect physical assets as well as digital assets, which requires the strong collaboration between the digital security team and physical security team. In IoTST ontology [69], authors explain that the asset concept is highly abstract and vital to the success of an organisation. It needs to be protected according to its value to the organization. In IIoT settings, the asset can represent anything like robots, power grids, sensors, actuators, Programmable Logic Controllers (PLC), digital twins, edge devices and cloud networks [7], [130]. The key attributes of asset concept are shown in Figure 10.

FIGURE 10: Attributes for asset concept.

Definition (Asset): *An asset can refer to both tangible and intangible entities that are essential and used for developing security controls and protecting other critical assets from vulnerabilities or cyberattacks.*

Attributes: The attributes identified for *Asset* concept are:

- **Asset Type:** This attribute characterises the classification of asset [127]. Examples include information, data, code, sensor, security control, machine, power grid, connection (e.g., wireless, non-wireless). The *Asset Type* attribute was used in CVO with *ProductType*[7]

[6](ISO/IEC 27000, 2009) define assets without mentioning people as an asset which is included later in (ISO/IEC 27000, 2018) version.

[7]In cybersecurity Asset and Product concepts have been used for similar purpose. However, Asset is more abstract and general term than the product and can be suitable for base cybersecurity ontologies.

term, which represent product classification [57]. Moreover, *Asset Type* attribute requires a controlled domain vocabulary to fully support the realisation of holistic security.

- **Asset Theme:** This attribute represents the domain to which an asset applies, for example, environment, law, healthcare, supply chain, transport, smart factory, or agriculture [127]. In the context of cybersecurity, this attribute can be helpful in various ways. For instance, it aids in localising vulnerabilities and threats, pinpointing risks, and designing appropriate security controls that enable security goals strongly relevant to the asset's domain [66].
- **Asset Spatial:** In much of the IoT and cybersecurity literature, spatial and location terms have been used interchangeably. The spatial attribute represents the geographic region to which an asset applies [127]. The physical location of an asset is a significant factor in the exposure of a system [7], [63]. Therefore, the spatial attribute is relevant in terms of an asset's exposure to risks from both physical and cybersecurity perspectives. For example, industrial assets in gas pipeline, supply chains, and transport systems are widely distributed across various geographic regions, where location and position are relevant to exposure to both types of risks. The spatial attribute value can be absolute, relative, static, or dynamic, and it influences the cyber risk impact on the asset [131]. For instance, a fixed CCTV camera deployed at the edge of a street or attached to a drone for surveillance can have relative, absolute, static, and dynamic positions with relevant security impacts on the asset. Additionally, this attribute enables the security monitoring and maintenance of remotely connected devices and services in accordance with the local legalities in the geographic region where the asset is deployed.
- **Asset Period of Time:** This attribute refers to the validity of an asset, for instance, the validity of a device, code, data, information, or even firewall in the context of security [127]. It also relates to when an asset faces an attack and how quickly security measures step in to protect it or restore its function. For example, when the spoofing device entered the network, and detected and isolated by the deployed cybersecurity controls. The impact of an attack can be severe if the assets stays compromised for a longer period without being detected. Therefore, this attribute can also be used to audit the security of a relevant asset which requires tracking, monitoring and ensuring its availability during or after a cyberattack.
- **Status:** This attribute refers to the condition of an asset in the context of a particular workflow process [127]. In this case, the workflow process can be a security mechanism which is used to protect IIoT devices from vulnerabilities and cyberattacks. The IoTST ontology describe *Status* as the level of vulnerability that affects the *Platform* [77]. In IoTST, *Platform* is analogues to an asset, which represents software, hardware, and operating systems affected by the threats. In industrial settings, the *Status* attribute represents the state of a machine in relation to its environment. Based on the above facts, we can define *Status* as the state of an asset throughout its lifecycle under the influence of internal and external factors. The *Status* attribute can be useful for updating, changing, and orchestrating devices with respect to cyber threats and vulnerabilities and ensuring the availability, safety, and protection of assets critical to the organisation.

E. LOSS SCENARIO CONCEPT

The *LossScenario* concept has been researched over the years in industrial control security ontologies, which mainly focus on resiliency and safety aspects in the IIoT environment. Alanen et al. [66], argued that the *Loss* and *LossScenario* are two distinct concepts. They described *Loss* as "Evaluated consequence of failure to keep or to continue to achieve the required availability performance", while *LossScenario* is a "combination or chain of circumstances leading from the initial cause to the loss". The VDO [67] contains *Scenario* as one of the mandatory concepts for vulnerability analysis, describing it as a placeholder that focuses on the various ways in which a vulnerability can be exploited by an attacker. For example, an attacker can access the main server and destroy data by exploiting a vulnerability in a connected smart grid or edge device. Bakirtzis et al. [83] suggest that the *LossScenario* represent metadata of system vulnerabilities, which lead the system to a transition from a safe to an unsafe state, causing devices to behave unpredictably due to cyberattacks and security breaches. Additionally, authors [83] argue that the *LossScenario* concept is relevant to the notions of recovery and resiliency.

Definition (LossScenario): *LossScenario can be defined as a sequence of events triggered by vulnerabilities in the given asset (e.g. IIoT device, software), which leads to a transition from a secure state to an unsafe state.*

Attributes: The attributes identified for *LossScenario* concept are:

- **Detection Pattern:** This attribute represents a design pattern of sentinel type. It involves analysing patterns, signals, or behaviours to detect potential losses or failures early for prompt corrective actions.
- **Threat Category:** The attribute denotes a category associated with a threat. A threat in the IoT environment can be of several types, including denial of IoT service or threat related to the tampering of IoT device. Threat can also involve repudiation, where an IoT system fails to appropriately log or control actions.

FIGURE 11: Loss scenario concept.

- ***Constraint:*** The *lossscenario* is detected through the observations and monitoring of system constraints. A constraint is considered violated when designed security criteria set by the system are not respected. For example, exceeding predefined limits of a security function or compromising sentinel-enforced device boundaries would indicate such an intrusion.
- **Detection Time:** This attribute characterises the time required to detect a loss scenario which depends on various factors, for instance, the type of security control and sentinel interfaces used. In the context of IoT applications, both polling centred and event centred approaches are popular. In polling centred, the IoT device is actively queried for the status updates in order to detect changes. On the other hand, in an event centred method, intruder activity is detected when a certain threshold is crossed.

VII. ANALYSIS OF RESEARCH GAP AND RECOMMENDATIONS

In this section, we explore the security modelling of IIoT systems by addressing key challenges, presenting recommendations, and outlining future directions. To provide a consolidated view, Table 4 summarises these challenges, while detailed discussions are presented in the subsequent subsections.

A. DATA INTEROPERABILITY FOR SECURE DIGITAL TWINS

Digital twins also face interoperability challenges related to different CPS domains, like manufacturing and healthcare. Some of the key issues are secure orchestration, cybersecurity, data governance, and spatiotemporal considerations that affect the accurate digital-physical mirroring based on location and time-based data [132]. To support holistic security in digital twins, IoT data should be machine-interpretable and interoperable across domains. This interoperability enhances advanced threat modelling and countermeasures. Security ontologies provide metadata for argumentation which can enable agents to select the best available security controls against cyberattacks. In order to secure cross-domain digital twins through data interoperability with ontologies there is a need for mapping and semantic techniques [133], [134]. These techniques provide interoperability at the semantic level and improve alignment among domain data models. The improved mapping approaches are highly required to align security ontologies and support interoperable cross-domain applications for secure digital twins [135], [136]. Ontology mapping can enable semantic matching among attributes of diverse security ontologies and fosters interoperable machine interpretation among cross-domain service agents for emerging digital twins. While Ontology mapping techniques have been studied in the past, existing interactive techniques require a significant inevitable human in the loop. Advanced AI-based methods are strongly needed to automate ontology alignment security attributes matching.

Additionally, research is also required to investigate the effects on the security of digital twins caused by changes in their ontology attributes for improvement or corrections. It is crucial because none of the security ontologies have a perfect solution to fit in with a system's needs [137]. Hence, ontology alignment needs to be considered as a continuous improvement process to reduce the consequences of changes in ontology.

B. DESIGN-TIME AND OPERATE-TIME SECURITY

The concept of security-by-design is gaining prominence in the development of security solutions for IIoT applications. Considering security parameters from the design phase helps identify potential threats and vulnerabilities early, which will improve the security of IIoT systems during the testing and production phases. To support secure IIoT systems, ontologies for security need to consider attributes not only at operate-time, but also during the design-time.

C. SECURITY ONTOLOGIES FOR DIGITAL TWINS

Current security ontologies either focus on data or network part of IoT devices' security, often lacking in decoupling between the physical side and digital side, there is a need for a holistic approach. Security ontologies for the digital twins should focus on three dimensions: Physical, digital communication networks, and data. Additionally, there is a need for ontologies that focus on interfacing between the digital and physical parts. In this direction, Application Programming Interface (API)s for digital twins should be sufficiently secure and robust.

D. DEDUCING COMPLEX RELATIONSHIPS

The usage of IoT devices in consumer and industrial IoT applications has several advantages as well as poses several risks, which requires end-to-end security solutions. Achieving holistic security measures requires identifying complex relations among OT and IT systems including IoT devices [138]–[140]. However, existing security solutions are lacking in terms of standardised approaches, highlighting the urgent need for a universally accepted ontology. A security ontology standard would support the representation of knowledge pertaining to incidents and countermeasures, enabling robust reasoning processes for deducing relationships between vulnerabilities and attack prevention measures.

E. INSUFFICIENT METADATA AND REUSABILITY

Metadata provides essential information about a security ontology, such as its purpose, scope, creator, version, licensing, etc. Failure to provide metadata can lead to confusion, misinterpretation, and hinder effective use. In the absence of adequate metadata, reusability and extensibility become difficult, limiting the ontology's value across several contexts. Insufficient metadata in existing security ontologies significantly hampers their reusability, as essential details required for adaptation and integration are often missing. For instance, metadata standards have proven to facilitate interoperability and data integrity by providing structured descriptors that help bridge data silos, which make it easier to integrate and adapt ontologies in cross-domain applications.

F. PRIORITISING IoT DEVICE SECURITY BEYOND JUST DATA SECURING

Most existing security ontologies are derived from information security, therefore, they do not focus on the constraints of IoT devices, such as limited computing power and energy resources. Moreover, these security ontologies solely offer concepts and properties for modelling the security of IoT data, disregarding the security considerations that are specific to the devices [141], [142].

G. SOCIO-TECHNICAL ASPECTS FOCUSED IIoT DEVICES SECURITY

In this challenge, security ontologies primarily focus on sociotechnical aspects, which need rigorous analysis of interactions between human operators/users and IIoT devices. For instance, the security ontologies for IIoT devices should consider classes and properties for human device interactions, as well as address social and emergency requirements of users. Access to IIoT devices should be updated based on the context of human users or operators. This involves modelling security concepts that account for human-device interactions and addresses risk related to human errors, and considering how users or operators may impact the security of IIoT systems under various operational scenarios. For example, Mauri and Damiani (2022) [143] emphasise the growing importance of user-centric security in IoT-based systems, while others also underline the necessity of risk management strategy, bridging technical protections with social and operational contexts to ensure holistic IoT security frameworks [144]–[146].

H. MAPPING OF SECURITY CONTROLS AND SECURITY GOALS

Current security ontologies lack comprehensive mapping between security concepts and security goals, which is crucial for assessing the requisite level of security for critical infrastructures and highly sensitive IIoT applications [25]. To enhance the security levels in an organisation multiple security standards may need to be adopted which requires the mapping of standards that are currently being used for the optimised management of security controls. Utilising security ontologies for this purpose can significantly reduce the complexity involved in the mapping process [147].

I. MAPPING OF SECURITY ONTOLOGIES

Security ontology mapping refers to the process of establishing linkages between concepts, terms, and entities in several security ontologies. Ontology mapping enables interoperability and facilitates data integration by aligning the semantics of concepts across various ontologies. Research in this direction is highly required because some security ontologies use different concepts to represent the same thing. This causes issues in sharing and exchanging security knowledge. Machine learning-based ontology mapping processes will facilitate the integration of security knowledge, Large Language Models (LLMs) can also be explored to mitigate this issue [148] Consequently, it will enhance the security of industrial assets, improve confidentiality, integrity, and authenticity, and reduce the risk of failure.

Ontologies are developed for a common understanding of things, and phenomena and for sharing knowledge via machines; however, existing security ontologies are not interoperable enough for exchanging threats and countermeasures. Interoperability in security ontologies is hindered due to several factors, including contextual, semantic and syntactic mismatches. Firstly, contextual mismatch implies to inconsistencies in the environment, situation, or setting that determine the sense of occurrence, often shaped by the requirements of participant entities. Addressing contextual mismatch has become an important area of investigation in security ontologies research, where approaches like reconciliation of contexts being actively explored. Secondly, semantic mismatch requires that the meaning of exchanged concepts align with the contextual information and remain coherently interpretable across the involved IoT systems. This type of problem has been explored in several other domains, similarly like [149], [150]. Thirdly, the syntactic mismatch is one of the significant interoperability issues in

security ontologies [151]. This issue arises from differences in the expressive capabilities of source languages that define these security ontologies, such as the Resource Description Framework (RDF) Schema or the OWL - description logic.

J. INTERPRETABILITY OF COUNTERMEASURES

Ontologies can model threats, security controls, and dependencies, yet are mostly devoid of representations for dynamically changing threats or real-time decision-making. Much ontology-based explanation is underutilized in order to explain relations among the layered defences, adaptive safeguards, and cascading impacts due to countermeasures. Stakeholders, therefore, do not get an appropriate feel about how different countermeasures might lower one risk and open up another. This can make it difficult for stakeholders to trust the countermeasure. Recent research suggests the need to enhance the semantic interoperability and explainability of security ontologies by integrating them with automated reasoning tools [46], [152]. This integration aims to support the development of adaptive, context-aware, and easily interpretable defence mechanisms.

K. BEYOND KNOWLEDGE REPRESENTATION AND QUERYING

Many researchers have developed security ontologies for knowledge representation, yet they have not taken advantage of these ontologies beyond SPARQL Protocol and RDF Query Language (SPARQL) queries. Security ontologies should be explored for their potential in reasoning and inferring new facts, identifying emerging threats, vulnerabilities and optimization of machine learning models used for intruders and anomaly detection. Testing and evaluating machine learning-based anomaly detection systems requires advanced approaches, as traditional testing methods pose safety and security concerns due to the non-deterministic nature of these systems. The use of ontological approaches to improve machine learning systems by sharing safety and security knowledge about threats and protection mechanisms has rarely been explored, apart from a few recent studies [153], [154].

L. SECURITY ONTOLOGY ENRICHMENTS

With massive repositories of information detailing attacks, vulnerabilities, security controls, and advisories available on the web, there exists potential to harness this wealth of data to enrich the knowledge encoded in security ontologies. Such information can be utilised to improve threat identification and countermeasures. Several machine learning based ontology enrichment methods proposed in the past, yet they suffer limitations in extracting contextual concepts from the existing knowledge bases [155], [156] . Recently, researchers are working to overcome such limitations using advanced approaches, including LLMs [157], [158]. No doubt these advanced methods offer significant promises to extracting embedded security information, which not only aids in reasoning and attributing vulnerabilities and attacks but also contributes to intelligent threat and anomalous behaviour detection.

M. CONTEXT BASED SECURE ACCESS AND CONTROL OF IoT DEVICES

The existing research studies primarily focus on developing security ontologies for knowledge collection and representation. Additionally, current access control mechanisms often struggle with implementing dynamic and context-aware policies due to the highly heterogeneous and rapidly changing nature of IoT environments [159]. This limits the ability to enforce fine-grained, real-time access decisions based on situational awareness. The true potential of ontologies lies in their use in argumentations, negotiations, and decision-making during the cyberattacks and enabling the safeguarding of assets in full or partial ways. For instance, several studies have used ontologies to address complex issues such as blockchain consensus mechanisms, legal decision-making for autonomous vehicles, and secure monitoring and tracing of pharmaceutical supply chain in the IoT environment [42], [160], [161].

N. MULTI-SOURCE DATA FUSION FOR ENHANCED SECURITY

Multi-source data fusion faces challenges due to the diverse nature of data sources, which can vary in format, structure, and type. Handling such heterogeneity complicates the integration process and often requires advanced preprocessing techniques. Several studies in other domains, including [77], [162]–[164], underscore the benefits of ontology-based multi-source integration in enhancing decision-making processes. Security ontologies and semantic IoT middlewares, can be developed to securely collect and aggregate data from multiple IoT devices. This approach aids in identifying anomalies in IoT data, illegitimate IoT devices, detection of cascading security impacts, vulnerabilities, threat prevention policies. Additionally, The concept of Social Internet of Things (SIoT) can also be leveraged to address these challenges effectively [165].

O. DISCOVER SEMANTIC RELATIONSHIP IN IoT DEVICES

Identifying semantic relationship in security ontologies to facilitate proactive measures for ensuring compliance with security standards and implementing necessary countermeasures in the rapidly growing IIoT systems is a promising future research area. As the IoT systems grow, it also leads to the growth of vulnerabilities and threats. Addressing and managing security issues in a growing IIoT ecosystem can be achieved by identifying relevant changes in instances within

the security ontology. A similar work has been done by study [166], in which authors has proposed ontologies for evolving software security in response to changing security context knowledge.

P. MODELLING INDUSTRY 5.0 SECURITY

Ontology provides a structured approach for modelling complex cybersecurity concepts, but their adoption in the Industry 5.0 context is extremely limited. Industry 5.0 focuses on human-centricity, sustainability, and resilience, introducing singular cybersecurity challenges that traditional ontologies do not fully address, such as the semantic modelling of human-machine collaboration vulnerabilities and adaptive threat responses. Most of the current efforts are focused on the mere extension of traditional ontologies to AI-driven systems, without considering the peculiar collaborative and social human factors dimensions of Industry 5.0. Such gaps need interdisciplinary approaches like the Internet of Everything (IoE), collective intelligence, which combines advanced technologies, ontologies with human-centered and adaptive cybersecurity mechanisms tailored for the evolving landscape of Industry 5.0.

TABLE 4: Challenges, recommendations and future directions for IIoT security modelling.

Challenge	Description	Future Directions/Recommendations
Data interoperability for secure digital twin	When composite digital twins collaborates for threat intelligence and countermeasures, the lack of cross-domain data interoperability poses significant risks to the physical assets.	Future research should focus on enhancing digital twins' data interoperability through the development of semantic approaches, AI-driven ontology mapping techniques, and continuous alignment strategies. It will improve security, accuracy, and cross-domain integration.
Design-time and operate-time security	The IIoT is still growing and lacks secure architecture and standards. While operate-time challenges involve real-time threat detection, response, and resource constraints.	Considering design-phase security parameters helps identify vulnerabilities early, improving IIoT system security during production.
Security ontologies for digital twin	Current security ontologies either focus on data or network part of IoT devices' security, often lacking in decoupling between the physical side and digital side.	Security ontologies for digital twins should address physical, network, and data dimensions while ensuring secure, timely decoupling of digital and physical components.
Deducing complex relationship	Lack of standardized approaches to represent and deduce complex relationships among OT, IT, and IoT systems. Vulnerabilities in one system can compromise others.	Future research should prioritize the development of a standardized security ontology to enable robust reasoning and deduce relationships between vulnerabilities and countermeasures. This advancement will enhance the security and safety of IIoT systems.
Insufficient metadata and reusability	Metadata provides key details like purpose, scope, creator, and licensing; its absence can lead to confusion, misinterpretation, and hinder effective ontology use.	A security ontology with sufficient metadata enhances reusability and security-related knowledge sharing in cross-domain IIoT applications, such as Industry 5.0.
IoT device vs data security	Most security ontologies focus on data security; hence data cannot be secured until the device is secured.	Existing security ontologies are derived from information security; therefore, they do not focus on the constraints of IoT devices, such as limited computing power and energy resources. These constraints should be prioritized while modeling the security of devices.
Socio-technical aspects	The risk of human errors and lack of context awareness exponentially increase the vulnerability of IIoT.	Security ontologies should integrate human-device interaction, risk management, and context-aware access control to enhance the IIoT security.
Mapping of security controls and Security goals	The lack of comprehensive mapping between security concepts, properties, and goals hinders the assessment of security requirements for critical infrastructures and highly sensitive IIoT applications.	Standard security ontologies mapping key concepts, properties, and security goals can aid in assessing security requirements and deploying threat prediction mechanisms and countermeasures effectively.
Interpretability of countermeasures	The interpretability of countermeasures for the IIoT devices is limited due to a lack of representations for dynamically evolving threats and real-time decision-making. undermines stakeholder trust in countermeasures, complicates risk assessment, and may leave vulnerabilities unaddressed.	Improved semantic and syntactic interoperability, enhanced explainability, and integration with automated reasoning tools will enable adaptive and comprehensible security measures.
Beyond knowledge representation and querying	Current research focuses on knowledge representation but does not fully utilize ontologies for argumentation, negotiation, or adaptive safeguarding of assets.	Recommendations include the leveraging of security ontologies for advanced reasoning, identification of emerging threats, optimization of machine learning models, and sharing of safety and security knowledge to enhance anomaly detection and address traditional testing limitations effectively.
Security ontologies enrichments	Massive repositories of attack, vulnerability, and security control information are available on the web. However, existing approaches are insufficient to extract contextual concepts effectively. This limitation hampers the ability to enhance threat identification, reasoning, and countermeasure development.	Mining and creating rich metadata for threat prevention and countermeasures, combined with integrated reasoners, argumentation, and machine learning approaches, can significantly enhance security ontologies.

Continued on next page

TABLE 4: Challenges, recommendations and future directions for IIoT security modelling. (Continued)

Context based secure access and control of IoT devices	Existing research primarily focuses on developing security ontologies for knowledge representation, while access control mechanisms lack dynamic, context-aware policies for evolving, heterogeneous IoT environments.	It is recommended to use security ontologies for argumentations, negotiations, and decision-making for threat prevention and vulnerability detection, it will enable the safeguarding of assets in full or partial ways.
Multisource data fusion for enhanced security	Diverse data sources, formats, structures, and types complicate the integration process, leading to delays in adaptive security measures, high false-positive rates, and inadequate detection accuracy.	Security ontologies can be developed to securely collect and aggregate data from multiple IoT devices. This approach aids in identifying anomalies in IoT data and illegitimate IoT devices.
Discover semantic relationships among the IoT devices	IoT/IIoT applications can involve thousands of heterogeneous devices deployed across various locations. Poorly designed relationships can lead to severe security breaches and vulnerabilities.	Detection of cascading security impacts, vulnerabilities, and threat intelligence can be enhanced through semantic interoperability and IoT middleware. The concept of SIoT can also be leveraged to address these challenges effectively.
Modelling industry 5.0 security	Limited adoption of ontology models in Industry 5.0 in addressing human-machine collaboration vulnerabilities and adaptive threat responses.	This limitation affects poor exploitation of ontology models in Industry 5.0, particularly in the case of vulnerabilities and adaptive threat responses regarding human-machine collaboration. Such gaps need security ontologies with interdisciplinary approaches like the IoE, collective intelligence, etc.

VIII. CONCLUSIONS

This paper has reviewed key ontological approaches for IIoT security modelling, identifying critical cybersecurity concepts and attributes, which include threat, vulnerability, security mechanism, asset, loss scenario, capability, and criticality. An analysis of ontologies literature revealed that most existing ontologies focus on data security rather than the IIoT devices themselves. Our review found that current security ontologies, often derived from the information security domain, lack sufficient mapping to security goals and fall short in addressing the sociotechnical aspects of IIoT ecosystem security. Furthermore, we identified several research gaps such as the need for improved interoperability and integration of multisource knowledge, improved metadata for reusability, and the development of standardized cybersecurity ontologies. We also recommended that these ontologies should not be developed in silos that limiting their clarity, completeness, and reusability, particularly for emerging technologies like Digital Twins and Industry 5.0.

TABLE 5: List of important acronyms.

Acronym	Definition
ABAC	Attribute based Access Control
ADMS	Asset Description Metadata Schema
API	Application Programming Interface
BMS	Building Management Systems
CAPEC	Common Attack Pattern Enumerations and Classifications
CCE	Common Configuration Enumeration
CIoT	Consumer Internet of Things
CNI	Critical National Infrastructure
COAP	Constrained Application Protocol
CPS	Cyber Physical Systems
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CVO	Cybersecurity Vulnerability Ontology
DDOS	Distributed Denial of Service
DS4IoT	IoT data security
DTM	Design-Time Modelling
DTW	Digital Twin Workshop
IICSF	Industrial Internet Consortium Security Framework
ICPs	Industrial Control Systems
ICUs	Industrial Control Units
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things

Continued on next page

TABLE 5: List of important acronyms. (Continued)

INSSA	IoT Network Security Situation Awareness
IoE	Internet of Everything
IoMT	Internet of Medical Things
IoT	Internet of Things
IoTSEC	Internet of Things Security
IoTST	IoT Security Threat
IPST	Internet Protocol Spoofing Threat
IT	Information Technology
ITS	Information Technology Systems
LLMs	Large Language Models
M2M	Machine-to-Machine
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OrBAC	Organization based Access Control
OSI	Open Systems Interconnection
OT	Operational Technology
OTS	Operational Technology Systems
OWL	Web Ontology Language
PLC	Programmable Logic Controllers
RBAC	Role based Access Control
RDF	Resource Description Framework
SCADA	Supervisory Control and Data Acquisition
SIoT	Social Internet of Things
SOFIoTS	Secure Ontologies for Internet of Things Systems
SOPs	Standard Operating Procedures
SPARQL	SPARQL Protocol and RDF Query Language
SSN	Semantic Sensor Network
STAC	Security Toolbox - Attacks & Countermeasures
SWRL	Semantic Web Rule Language
TTP	Tactics, Techniques, and Procedures
UDPA	UK Data Protection Action
UCO	Unified Cybersecurity Ontology
URI	Uniform Resource Identifier
VDO	Vulnerability Description Ontology
VMP	Vulnerability Management Process
VPN	Virtual Private Network
WoT	Web of Things
WoTSO	Web of Things Security Ontology

Continued on next page

TABLE 5: List of important acronyms. (Continued)

XAI	Explainable Artificial Intelligence

ACKNOWLEDGMENT

This work has been supported by the PETRAS National Center of Excellence in IoT Systems Cybersecurity, which is funded by the UK EPSRC under grant number EP/S035362/1.

REFERENCES

[1] T. Deepu and V. Ravi, "A review of literature on implementation and operational dimensions of supply chain digitalization: Framework development and future research directions," *International Journal of Information Management Data Insights*, vol. 3, no. 1, p. 100156, 2023.

[2] K. Li, Y. Zhang, Y. Huang, Z. Tian, and Z. Sang, "Framework and capability of industrial iot infrastructure for smart manufacturing," *Standards*, vol. 3, no. 1, pp. 1–18, 2023.

[3] X. Cao, J. Wang, Y. Cheng, and J. Jin, "Optimal sleep scheduling for energy-efficient aoi optimization in industrial internet of things," *IEEE Internet of Things Journal*, 2023.

[4] D. Serpanos, "Industrial internet of things: Trends and challenges," *Computer*, vol. 57, no. 1, pp. 124–128, 2024.

[5] Q. H. Lai, C. S. Lai, and L. L. Lai, *Smart Health Based on Internet of Things (IoT) and Smart Devices*, 2023, pp. 425–462.

[6] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and industrial iot (in)security: Attack taxonomy and case studies," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 199–221, 2022.

[7] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361517307285

[8] M. A. Jarwar, J. Watson CBE FREng, U. P. D. Ani, and S. Chalmers, "Industrial internet of things security modelling using ontological methods," in *Proceedings of the 12th International Conference on the Internet of Things*, ser. IoT '22. New York, NY, USA: Association for Computing Machinery, 2023, p. 163–170. [Online]. Available: https://doi.org/10.1145/3567445.3571103

[9] S. Shah, S. H. Hussain Madni, S. Z. B. M. Hashim, J. Ali, and M. Faheem, "Factors influencing the adoption of industrial internet of things for the manufacturing and production small and medium enterprises in developing countries," *IET Collaborative Intelligent Manufacturing*, vol. 6, no. 1, p. e12093, 2024.

[10] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial iot infrastructures," *Ad Hoc Networks*, vol. 156, p. 103414, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870524000258

[11] "Advanced Persistent Threat," https://bit.ly/3mt8iBm, accessed on: 2023-01-11.

[12] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[13] N. Tuptuk, P. Hazell, J. Watson, and S. Hailes, "A systematic review of the state of cyber-security in water systems," *Water*, vol. 13, no. 1, p. 81, 2021.

[14] V. Varadharajan, U. Tupakula, and K. K. Karmakar, "Techniques for enhancing security in industrial control systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 8, no. 1, jan 2024. [Online]. Available: https://doi.org/10.1145/3630103

[15] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial iot devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 20, no. 2, pp. 1–24, 2020.

[16] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1–6.

[17] M. D. P. Salas-Zárate, R. Valencia-García, A. Ruiz-Martínez, and R. Colomo-Palacios, "Feature-based opinion mining in financial news: An ontology-driven approach:," *http://dx.doi.org/10.1177/0165551516645528*, vol. 43, no. 4, pp. 458–479, may 2016. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/0165551516645528

[18] A. Rodríguez-González, Á. García-Crespo, R. Colomo-Palacios, F. Guldrís Iglesias, and J. M. Gómez-Berbís, "CAST: Using neural networks to improve trading systems based on technical analysis by means of the RSI financial indicator," *Expert Systems with Applications*, vol. 38, no. 9, pp. 11 489–11 500, sep 2011.

[19] R. Valencia-García, F. García-Sánchez, D. Castellanos-Nieves, and J. T. Fernández-Breis, "OWLPath: An OWL ontology-guided query editor," *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, vol. 41, no. 1, pp. 121–136, jan 2011.

[20] A. Rodríguez-González, J. E. Labra-Gayo, R. Colomo-Palacios, M. A. Mayer, J. M. Gómez-Berbís, and A. García-Crespo, "SeDeLo: Using semantics and description logics to support aided clinical diagnosis," *Journal of Medical Systems*, vol. 36, no. 4, pp. 2471–2481, aug 2012. [Online]. Available: https://link.springer.com/article/10.1007/s10916-011-9714-1

[21] P. Trucco, B. Petrenj *et al.*, "An ontology-based approach to vulnerability and interdependency modelling for critical infrastructure systems," *T. Nowakowski et al*, pp. 49–56, 2015.

[22] M. Compton, P. Barnaghi, L. Bermudez, R. García-Castro, O. Corcho, S. Cox, J. Graybeal, M. Hauswirth, C. Henson, A. Herzog, V. Huang, K. Janowicz, W. D. Kelsey, D. Le Phuoc, L. Lefort, M. Leggieri, H. Neuhaus, A. Nikolov, K. Page, A. Passant, A. Sheth, and K. Taylor, "The ssn ontology of the w3c semantic sensor network incubator group," *Journal of Web Semantics*, vol. 17, pp. 25–32, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570826812000571

[23] "TS 118 112 - V2.0.0 - oneM2M; Base Ontology (oneM2M TS-0012 version 2.0.0 Release 2)," https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx, Tech. Rep., 2016.

[24] V. Charpenay, S. Käbisch, and H. Kosch, "Introducing Thing Descriptions and Interactions: An Ontology for the Web of Things." [Online]. Available: http://purl.oclc.org/net/unis/OWL-IoT-S.owl

[25] M. Adach, K. Hänninen, and K. Lundqvist, "Security ontologies: A systematic literature review," in *International Conference on Enterprise Design, Operations, and Computing*. Springer, 2022, pp. 36–53.

[26] F. Qaswar, M. Rahmah, M. A. Raza, A. Noraziah, B. Alkazemi, Z. Fauziah, M. K. A. Hassan, and A. Sharaf, "Applications of ontology in the internet of things: A systematic analysis," *Electronics*, vol. 12, no. 1, p. 111, 2022.

[27] P. Smart, M. Boniface, M. A. Jarwar, and J. Watson, "Sofiots: ontological framework, demonstration outcomes, and recommendations for further work," Project Report 10.5258/SOTON/P1165, July 2023. [Online]. Available: https://eprints.soton.ac.uk/490073/

[28] J. Ordieres-Meré, M. Gutierrez, and J. Villalba-Díez, "Toward the industry 5.0 paradigm: Increasing value creation through the robust integration of humans and machines," *Computers in Industry*, vol. 150, p. 103947, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361523000970

[29] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, "Multi-aspect rule-based ai: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures," *Internet of Things*, vol. 25, p. 101110, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524000520

[30] M. Adach, K. Hänninen, and K. Lundqvist, "A combined security ontology based on the unified foundational ontology," in *2022 IEEE 16th International Conference on Semantic Computing (ICSC)*, 2022, pp. 187–194.

[31] B. F. Martins, L. J. Serrano Gil, J. F. Reyes Román, J. I. Panach, O. Pastor, M. Hadad, and B. Rochwerger, "A framework for conceptual characterization of ontologies and its application in the cybersecurity domain," *Software and Systems Modeling*, vol. 21, no. 4, pp. 1437–1464, 2022.

[32] C. Bratsas, E. K. Anastasiadis, A. K. Angelidis, L. Ioannidis, R. Kotsakis, and S. Ougiaroglou, "Knowledge graphs and semantic web tools in cyber threat intelligence: A systematic literature review," *Journal of Cybersecurity and Privacy*, vol. 4, no. 3, pp. 518–545, 2024. [Online]. Available: https://www.mdpi.com/2624-800X/4/3/25

[33] D. Preuveneers and W. Joosen, "An ontology-based cybersecurity framework for ai-enabled systems and applications," *Future Internet*, vol. 16, no. 3, 2024. [Online]. Available: https://www.mdpi.com/1999-5903/16/3/69

[34] A. Yeboah-Ofori, H. Mouratidis, U. Ismai, S. Islam, and S. Papastergiou, "Cyber supply chain threat analysis and prediction using machine learning and ontology," in *Artificial Intelligence Applications and Innovations: 17th IFIP WG 12.5 International Conference, AIAI 2021, Hersonissos, Crete, Greece, June 25–27, 2021, Proceedings 17*. Springer, 2021, pp. 518–530.

[35] "Web of Things (WoT) Security Ontology," https://www.w3.org/2019/wot/security, last Accessed:2021-12-18.

[36] R. Figliè, R. Amadio, M. Tyrovolas, C. Stylios, Ł. Paśko, D. Stadnicka, A. Carreras-Coch, A. Zaballos, J. Navarro, and D. Mazzei, "Towards a taxonomy of industrial challenges and enabling technologies in industry 4.0," *IEEE Access*, vol. 12, pp. 19 355–19 374, 2024.

[37] L. Erazo-Garzon, J. Avila, S. Pinos, and P. Cedillo, "A systematic review on the use of ontologies in the internet of things," in *Applied Technologies*, M. Botto-Tobar, S. Montes León, P. Torres-Carrión, M. Zambrano Vizuete, and B. Durakovic, Eds. Cham: Springer International Publishing, 2022, pp. 509–524.

[38] M. H. Rahman, T. Wuest, and M. Shafae, "Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies," *Journal of Manufacturing Systems*, vol. 68, pp. 196–208, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278612523000602

[39] V. R. S. Kumar, A. Khamis, S. Fiorini, J. L. Carbonera, A. O. Alarcos, M. Habib, P. Goncalves, H. Li, and J. I. Olszewska, "Ontologies for industry 4.0," *The Knowledge Engineering Review*, vol. 34, p. e17, 2019.

[40] W. F. B. Rivadeneira and O. S. Gómez, "Cybersecurity ontologies: A systematic literature review," *ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica*, vol. 9, no. 2, pp. 1–18, 2020.

[41] I. Szilagyi and P. Wira, "Ontologies and semantic web for the internet of things - a survey," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, 2016, pp. 6949–6954.

[42] M. Khan, F. den Hartog, and J. Hu, "A survey and ontology of blockchain consensus algorithms for resource-constrained iot systems," *Sensors*, vol. 22, no. 21, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/21/8188

[43] F. d. F. Rosa, R. Bonacin, and M. Jino, "The security assessment domain: a survey of taxonomies and ontologies," *arXiv preprint arXiv:1706.09772*, 2017.

[44] T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," *Electronics*, vol. 9, no. 11, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/11/1864

[45] Z. Liao, S. Nazir, H. U. Khan, and M. Shafiq, "Assessing security of software components for internet of things: a systematic review and future directions," *Security and Communication Networks*, vol. 2021, no. 1, p. 6677867, 2021.

[46] S. Hollerer, T. Sauter, and W. Kastner, "A survey of ontologies considering general safety, security, and operation aspects in ot," *IEEE Open Journal of the Industrial Electronics Society*, vol. 5, pp. 861–885, 2024.

[47] T. R. Gadekallu, P. K. R. Maddikunta, P. Boopathy, N. Deepa, R. Chengoden, N. Victor, W. Wang, W. Wang, Y. Zhu, and K. Dev, "Xai for industry 5.0-concepts, opportunities, challenges and future directions," *IEEE Open Journal of the Communications Society*, 2024.

[48] H. Wang, G. Wang, H. Li, J. Leng, L. Lv, V. Thomson, Y. Zhang, L. Li, and L. Chen, "An automatic unsafe states reasoning approach towards industry 5.0's human-centered manufacturing via digital twin," *Advanced Engineering Informatics*, vol. 62, p. 102792, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1474034624004403

[49] M. Arazzi, A. Nocera, and E. Storti, "The semioe ontology: A semantic model solution for an ioe-based industry," *IEEE Internet of Things Journal*, pp. 1–1, 2024.

[50] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," *Health information & libraries journal*, vol. 26, no. 2, pp. 91–108, 2009.

[51] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, "The prisma 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021. [Online]. Available: https://www.bmj.com/content/372/bmj.n71

[52] R. T. Watson and J. Webster, "Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0," *Journal of Decision Systems*, vol. 29, no. 3, pp. 129–147, 2020.

[53] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*, pp. xiii–xxiii, 2002.

[54] J. H. Elliott, A. Synnot, T. Turner, M. Simmonds, E. A. Akl, S. McDonald, G. Salanti, J. Meerpohl, H. MacLehose, J. Hilton, D. Tovey, I. Shemilt, J. Thomas, T. Agoritsas, J. Hilton, C. Perron, E. Akl, R. Hodder, C. Pestridge, L. Albrecht, T. Horsley, J. Platt, R. Armstrong, P. H. Nguyen, R. Plovnick, A. Arno, N. Ivers, G. Quinn, A. Au, R. Johnston, G. Rada, M. Bagg, A. Jones, P. Ravaud, C. Boden, L. Kahale, B. Richter, I. Boisvert, H. Keshavarz, R. Ryan, L. Brandt, S. A. Kolakowsky-Hayner, D. Salama, A. Brazinova, S. K. Nagraj, G. Salanti, R. Buchbinder, T. Lasserson, L. Santaguida, C. Champion, R. Lawrence, N. Santesso, J. Chandler, Z. Les, H. J. Schünemann, A. Charidimou, S. Leucht, I. Shemilt, R. Chou, N. Low, D. Sherifali, R. Churchill, A. Maas, R. Siemieniuk, M. C. Cnossen, H. MacLehose, M. Simmonds, M.-J. Cossi, M. Macleod, N. Skoetz, M. Counotte, I. Marshall, K. Soares-Weiser, S. Craigie, R. Marshall, V. Srikanth, P. Dahm,

N. Martin, K. Sullivan, A. Danilkewich, L. Martínez García, A. Synnot, K. Danko, C. Mavergames, M. Taylor, E. Donoghue, L. J. Maxwell, K. Thayer, C. Dressler, J. McAuley, J. Thomas, C. Egan, S. McDonald, R. Tritton, J. Elliott, J. McKenzie, G. Tsafnat, S. A. Elliott, J. Meerpohl, P. Tugwell, I. Etxeandia, B. Merner, A. Turgeon, R. Featherstone, S. Mondello, T. Turner, R. Foxlee, R. Morley, G. van Valkenhoef, P. Garner, M. Munafo, P. Vandvik, M. Gerrity, Z. Munn, B. Wallace, P. Glasziou, M. Murano, S. A. Wallace, S. Green, K. Newman, C. Watts, J. Grimshaw, R. Nieuwlaat, L. Weeks, K. Gurusamy, A. Nikolakopoulou, A. Weigl, N. Haddaway, A. Noel-Storr, G. Wells, L. Hartling, A. O'Connor, W. Wiercioch, J. Hayden, M. Page, L. Wolfenden, M. Helfand, M. Pahwa, J. J. Yepes Nuñez, J. Higgins, J. P. Pardo, J. Yost, S. Hill, and L. Pearson, "Living systematic review: 1. introduction—the why, what, when, and how," *Journal of Clinical Epidemiology*, vol. 91, pp. 23–30, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0895435617306364

[55] B. B. Penning de Vries, M. van Smeden, F. R. Rosendaal, and R. H. Groenwold, "Title, abstract, and keyword searching resulted in poor recovery of articles in systematic reviews of epidemiologic practice," *Journal of Clinical Epidemiology*, vol. 121, pp. 55–61, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0895435619306018

[56] B. Franco Martins Souza, "A framework for conceptual characterization of ontologies and its application in the cybersecurity domain," Ph.D. dissertation, Universitat Politècnica de València, 2024.

[57] R. Syed, "Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system," *Information & Management*, vol. 57, no. 6, p. 103334, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378720620302718

[58] S. Wilson, J. S. Goonetillake, A. Ginige, and W. Indika, "A conceptual model for ontology quality assessment — www.semantic-web-journal.net," https://www.semantic-web-journal.net/content/conceptual-model-ontology-quality-assessment-1, Feb 2023, (Accessed on 04/02/2023).

[59] A. Duque-Ramos, J. T. Fernández-Breis, R. Stevens, and N. Aussenac-Gilles, "Oquare: A square-based approach for evaluating the quality of ontologies," *Journal of research and practice in information technology*, vol. 43, no. 2, pp. 159–176, 2011.

[60] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network security situation awareness based on semantic ontology and user-defined rules for internet of things," *IEEE Access*, vol. 5, pp. 21 046–21 056, 2017.

[61] A. Duque-Ramos, J. T. Fernández-Breis, M. Iniesta, M. Dumontier, M. E. Aranguren, S. Schulz, N. Aussenac-Gilles, and R. Stevens, "Evaluation of the oquare framework for ontology quality," *Expert Systems with Applications*, vol. 40, no. 7, pp. 2696–2703, 2013.

[62] Y. He, Z. Xiang, J. Zheng, Y. Lin, J. A. Overton, and E. Ong, "The extensible ontology development (xod) principles and tool implementation to support ontology interoperability," *Journal of biomedical semantics*, vol. 9, pp. 1–10, 2018.

[63] "Code of Practice: Cyber Security in the Built Environment – revised second edition." [Online]. Available: https://bit.ly/3YlhWJP

[64] S. Schrecker, H. Soroush, J. Molina, J. Caldwell, D. Meltzer, F. Hirsch, J. Pierre Leblanc, and M. Buchheit, "Industrial Internet of Things Volume G4: Security Framework," 2016.

[65] L. Wüstrich, M.-O. Pahl, and S. Liebald, "Towards an extensible iot security taxonomy," in *2020 IEEE Symposium on Computers and Communications (ISCC)*, 2020, pp. 1–6.

[66] J. Alanen, J. Linnosmaa, T. Malm, N. Papakonstantinou, T. Ahonen, E. Heikkilä, and R. Tiusanen, "Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (sta) method for industrial control systems," *Reliability Engineering & System Safety*, vol. 220, p. 108270, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832021007444

[67] H. Booth and C. Turner, "NIST- Vulnerability Description Ontology (VDO)," http://csrc.nist.gov/publications, accessed on :2024-04-03.

[68] "Web of Things (WoT) Security Ontology," Mar. 2023, [Online; accessed 1. Apr. 2023]. [Online]. Available: https://www.w3.org/2019/wot/security

[69] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the internet of things," in *2015 IEEE International Workshop on Measurements Networking (M N)*, 2015, pp. 1–6.

[70] P. Bowen, P. Bowen, J. Hash, and M. Wilson, "Information Security Handbook: A Guide for Managers," *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*, pp. 178—-800, 2007. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.697.168

[71] V. Y. P. Michael Nieles, Kelley Dempsey, "Draft nist sp 800-12 rev. 1, an introduction to information security," https://csrc.nist.gov/CSRC/media/Publications/sp/800-12/rev-1/draft/documents/sp800_12_r1_draft.pdf, January 2017, (Accessed on 04/02/2023).

[72] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, and R. Jardim-Goncalves, "An ontology-based cybersecurity framework for the internet of things," *Sensors*, vol. 18, no. 9, p. 3053, 2018.

[73] A. Gyrard, C. Bonnet, and K. Boudaoud, "An Ontology-Based Approach for Helping to Secure the ETSI Machine-to-Machine Architecture," in *2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*, 2014, pp. 109–116.

[74] R. A. Amélie Gyrard, Elsaleh Tarek, "Linked open vocabularies," https://lov.linkeddata.es/dataset/lov/vocabs/m3lite, Sep 2017, (Accessed on 04/02/2023).

[75] K. B. Amelie Gyrard, Christian Bonnet, "Linked open vocabularies for internet of things (lov4iot)," http://lov4iot.appspot.com/?p=lov4iot-security, Jan 2014, (Accessed on 04/02/2023).

[76] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*, 2009, pp. 183–194.

[77] S. Zhang, G. Bai, H. Li, P. Liu, M. Zhang, and S. Li, "Multi-source knowledge reasoning for data-driven iot security," *Sensors*, vol. 21, no. 22, p. 7579, 2021.

[78] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21 046–21 056, 2017.

[79] A. García-Crespo, J. Chamizo, I. Rivera, M. Mencke, R. Colomo-Palacios, and J. M. Gómez-Berbís, "SPETA: Social pervasive e-Tourism advisor," *Telematics and Informatics*, vol. 26, no. 3, pp. 306–315, aug 2009.

[80] Z. Syed, A. Padia, T. Finin, L. Mathews, and A. Joshi, "Uco: A unified cybersecurity ontology," in *Workshops at the thirtieth AAAI conference on artificial intelligence*, 2016.

[81] S. Barnum, "About stix — stix project documentation," https://stixproject.github.io/about/, Feb 2014, (Accessed on 04/02/2023).

[82] "Github - ebiquity/unified-cybersecurity-ontology: Unified cybersecurity ontology," https://github.com/Ebiquity/Unified-Cybersecurity-Ontology, (Accessed on 04/02/2023).

[83] G. Bakirtzis, T. Sherburne, S. Adams, B. M. Horowitz, P. A. Beling, and C. H. Fleming, "An ontological metamodel for cyber-physical system safety, security, and resilience coengineering," *Software and Systems Modeling*, vol. 21, no. 1, pp. 113–137, 2022.

[84] "ontologicalmetamodel for cyber-physical system safety, security. cps-metamodel/cps-metamodel.graphql at master · coordinated-systems-lab/cps-metamodel · github," https://github.com/coordinated-systems-lab/cps-metamodel/blob/master/cps-metamodel.graphql, May 2020, (Accessed on 04/02/2023).

[85] "Web of Things (WoT) Security Ontology," accessed 2024-10-31. [Online]. Available: https://www.w3.org/2019/wot/security

[86] "IoT Security Ontology ," accessed 2024-10-31. [Online]. Available: https://github.com/brunomozza/IoTSecurityOntology/blob/master/iotsec.owl

[87] "STAC ," accessed 2024-10-31. [Online]. Available: https://databus.dbpedia.org/ontologies/securitytoolbox.appspot.com/stac

[88] "ebiquity ," accessed 2024-09-23. [Online]. Available: https://ebiquity.github.io/Unified-Cybersecurity-Ontology/uco_1_5.owl

[89] "GraphQL schema ," accessed 2024-09-23. [Online]. Available: https://github.com/coordinated-systems-lab/cps-metamodel

[90] P. Gonzalez-Gil, J. A. Martinez, and A. F. Skarmeta, "Lightweight data-security ontology for iot," *Sensors*, vol. 20, no. 3, p. 801, 2020.

[91] "ds4iot ," accessed 2024-10-31. [Online]. Available: https://github.com/mainakae/ds4iot

[92] P. Gonzalez-Gil, J. A. Martinez, and A. F. Skarmeta, "Github - mainakae/ds4iot: Data security for iot ontology (ds4iot)," https://github.com/mainakae/ds4iot, 2020, (Accessed on 04/02/2023).

[93] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for iot networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022.

[94] "Isagca quick start guide final.pdf," https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf, (Accessed on 04/02/2023).

[95] S. Cariell, M. Eble, F. Hirsch, E. Rudina, and R. Zahavi, "Security maturity model - industry iot consortium," https://www.iiconsortium.org/smm/, (Accessed on 04/02/2023).

[96] M. Al-Hawawreh, F. Den Hartog, and E. Sitnikova, "Targeted ransomware: A new cyber threat to edge system of brownfield industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7137–7151, 2019.

[97] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156–168, 2017.

[98] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "NIST Special Publication 800-12 Revision 1 An Introduction to Information Security," https://doi.org/10.6028/NIST.SP.800-12r1.

[99] "Nvd - home," https://nvd.nist.gov/, (Accessed on 04/02/2023).

[100] "Common vulnerability scoring system version 3.1 specification," https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf, (Accessed on 04/02/2023).

[101] F. Song, Y.-T. Zhou, Y. Wang, T.-M. Zhao, I. You, and H.-K. Zhang, "Smart collaborative distribution for privacy enhancement in moving target defense," *Information Sciences*, vol. 479, pp. 593–606, 2019.

[102] A. Shah, K. A. Farris, R. Ganesan, and S. Jajodia, "Vulnerability selection for remediation: An empirical analysis," *The Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 13–22, 2022.

[103] "Cvss v3.1 specification document," https://www.first.org/cvss/specification-document, (Accessed on 04/02/2023).

[104] L. Zhu, Z. Zhang, G. Xia, and C. Jiang, "Research on vulnerability ontology model," in *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*. IEEE, 2019, pp. 657–661.

[105] S. Munirathinam, "Industry 4.0: Industrial internet of things (iiot)," in *Advances in computers*. Elsevier, 2020, vol. 117, no. 1, pp. 129–164.

[106] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2011.

[107] "Industrial iot: Threats and countermeasures - rambus," https://www.rambus.com/iot/industrial-iot/, (Accessed on 04/02/2023).

[108] B. Sangchoolie, P. Folkesson, P. Kleberger, and J. Vinter, "Analysis of cybersecurity mechanisms with respect to dependability and security attributes," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2020, pp. 94–101.

[109] "Wifi suspended at big uk train stations after 'cybersecurity incident' — uk news — the guardian," https://www.theguardian.com/uk-news/2024/sep/26/wifi-suspended-big-uk-train-stations-cybersecurity-incident, (Accessed on 09/26/2024).

[110] H. Xu, W. Yu, X. Liu, D. Griffith, and N. Golmie, "On data integrity attacks against industrial internet of things," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2020, pp. 21–28.

[111] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.

[112] "Building functional safety and security into modern iiot enterprises," https://resources.sw.siemens.com/en-US/white-paper-safety-and-security-modern-iiot-enterprises, (Accessed on 04/02/2023).

[113] "Data protection best practices," https://www.iiconsortium.org/pdf/Data_Protection_Best_Practices_Whitepaper_2019-07-22.pdf, Jul 2019, (Accessed on 04/02/2023).

[114] T. N. Nguyen, Q.-D. Ngo, H.-T. Nguyen, and G. L. Nguyen, "An advanced computing approach for iot-botnet detection in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8298–8306, 2022.

[115] M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Computer Networks*, vol. 165, p. 106946, 2019.

[116] D. Kshirsagar and S. Kumar, "An ontology approach for proactive detection of http flood dos attack," *International Journal of System Assurance Engineering and Management*, pp. 1–8, 2021.

[117] "Mitre - security mechanism detection methods," https://cwe.mitre.org/community/swa/detection_methods.html, (Accessed on 04/02/2023).

[118] "Networking and security in industrial automation environments." https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.pdf, (Accessed on 04/02/2023).

[119] S. L. Kwast, "Is cyber deterrence possible?" https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF, (Accessed on 04/02/2023).

[120] M. Guerar, L. Verderame, A. Merlo, F. Palmieri, M. Migliardi, and L. Vallerini, "Circlepin: a novel authentication mechanism for smartwatches to prevent unauthorized access to iot devices," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, pp. 1–19, 2020.

[121] "The cyber security body of knowledge," https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf, 2019, (Accessed on 04/02/2023).

[122] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, pp. 1–44, 2022.

[123] P. Radanliev, D. De Roure, M. Van Kleek, U. Ani, P. Burnap, E. Anthi, J. R. Nurse, O. Santos, R. M. Montalvo, and L. Maddox, "Dynamic real-time risk analytics of uncontrollable states in complex internet of things systems: cyber risk at the edge," *Environment Systems and Decisions*, vol. 41, pp. 236–247, 2021.

[124] M. Fagan, J. Marron, K. G. Brady Jr, B. B. Cuthill, K. N. Megas, R. Herold, D. Lemire, and B. Hoehn, "Sp 800-213, iot device cybersecurity guidance for the federal government — csrc," https://csrc.nist.gov/publications/detail/sp/800-213/final, (Accessed on 04/02/2023).

[125] H. N. Noura, R. Melki, and A. Chehab, "Secure and lightweight mutual multi-factor authentication for iot communication systems," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–7.

[126] C. L. Maines, D. Llewellyn-Jones, S. Tang, and B. Zhou, "A cyber security ontology for bpmn-security extensions," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. IEEE, 2015, pp. 1756–1763.

[127] "W3c - asset description metadata schema (adms)," https://www.w3.org/TR/vocab-adms/, (Accessed on 04/02/2023).

[128] S. Bergner and U. Lechner, "Cybersecurity ontology for critical infrastructures." in *KEOD*, 2017, pp. 80–85.

[129] M. Jbair, B. Ahmad, C. Maple, and R. Harrison, "Threat modelling for industrial cyber physical systems in the era of smart manufacturing," *Computers in Industry*, vol. 137, p. 103611, 2022.

[130] W. Liu, M. Wu, G. Wan, and M. Xu, "Digital twin of space environment: Development, challenges, applications, and future outlook," *Remote Sensing*, vol. 16, no. 16, 2024. [Online]. Available: https://www.mdpi.com/2072-4292/16/16/3023

[131] X. Li, C. Zhou, Y.-C. Tian, N. Xiong, and Y. Qin, "Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 608–618, 2017.

[132] S. Acharya, A. A. Khan, and T. Päivärinta, "Interoperability levels and challenges of digital twins in cyber–physical systems," *Journal of Industrial Information Integration*, vol. 42, p. 100714, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X24001572

[133] P. Ochieng and S. Kyanda, "Large-scale ontology matching: State-of-the-art analysis," *ACM Comput. Surv.*, vol. 51, no. 4, jul 2018. [Online]. Available: https://doi.org/10.1145/3211871

[134] K. Alshammari, T. Beach, and Y. Rezgui, "Cybersecurity for digital twins in the built environment: Current research and future directions," *Journal of Information Technology in Construction*, vol. 26, pp. 159–173, 2021.

[135] K. S. Bughio, D. M. Cook, and S. A. A. Shah, "Developing a novel ontology for cybersecurity in internet of medical things-enabled remote patient monitoring," *Sensors*, vol. 24, no. 9, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/9/2804

[136] J. Akroyd, S. Mosbach, A. Bhave, and M. Kraft, "Universal digital twin-a dynamic knowledge graph," *Data-Centric Engineering*, vol. 2, p. e14, 2021.

[137] T. Wang, "Aligning the large-scale ontologies on schema-level for weaving chinese linked open data," *Cluster Computing*, vol. 22, no. 2, pp. 5099–5114, 2019.

[138] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security considerations for internet of things: A survey," *SN Computer Science*, vol. 1, pp. 1–19, 2020.

[139] S. Vetrivel, R. Maheswari, and T. Saravanan, "Industrial iot: Security threats and counter measures," in *Communication Technologies and Security Challenges in IoT: Present and Future*. Springer, 2024, pp. 403–425.

[140] P. Smart, M. Boniface, M. A. Jarwar, and J. Watson, "Secure ontologies for the internet of things: representing risk and security concepts using basic formal ontology," UCL, Project Report, July 2023. [Online]. Available: https://github.com/ps02v/SOfIoTS/blob/main/Documentation/SOfIoTS%20Ontology%20Documentation.pdf

[141] D. Canavese, L. Mannella, L. Regano, and C. Basile, "Security at the edge for resource-limited iot devices," *Sensors*, vol. 24, no. 2, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/2/590

[142] Y. Badr, X. Zhu, and M. N. Alraja, "Security and privacy in the internet of things: threats and challenges," *Service Oriented Computing and Applications*, vol. 15, no. 4, pp. 257–271, 2021.

[143] L. Mauri and E. Damiani, "Modeling threats to ai-ml systems using stride," *Sensors*, vol. 22, no. 17, p. 6662, 2022.

[144] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2021.

[145] A. Sánchez-Zumba and D. Avila-Pesantez, "Cybersecurity for industrial iot, threats, vulnerabilities, and solutions: A brief review," in *International Congress on Information and Communication Technology*. Springer, 2023, pp. 1101–1112.

[146]

[147] S. Ramanauskaitė, D. Olifer, N. Goranin, and A. Čenys, "Security ontology for adaptive mapping of security standards," *International Journal of Computers, Communications & Control (IJCCC)*, vol. 8, no. 6, pp. 813–825, 2013.

[148] S. Zhang, Y. Dong, Y. Zhang, T. R. Payne, and J. Zhang, "Large language model assisted multi-agent dialogue for ontology alignment," in *The 23rd International Conference on Autonomous Agents and Multi-Agent Systems*, 2024.

[149] M. B. Alaya, S. Medjiah, T. Monteil, and K. Drira, "Toward semantic interoperability in onem2m architecture," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 35–41, 2015.

[150] I. Berges, J. Bermudez, and A. Illarramendi, "Toward semantic interoperability of electronic health records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 3, pp. 424–431, 2012.

[151] H. Rahman and M. I. Hussain, "A comprehensive survey on semantic interoperability for internet of things: State-of-the-art and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3902, 2020.

[152] R. Confalonieri, T. Weyde, T. R. Besold, and F. Moscoso del Prado Martín, "Using ontologies to enhance human understandability of global post-hoc explanations of black-box models," *Artificial Intelligence*, vol. 296, p. 103471, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0004370221000229

[153] A.-L. Wozniak, R. Mazo, and S. Segura, "Rationale: A security and safety testing ontology for machine learning-based systems."

[154] D. Sacha, M. Kraus, D. A. Keim, and M. Chen, "Vis4ml: An ontology for visual analytics assisted machine learning," *IEEE Transactions on Visualization and Computer Graphics*, vol. 25, no. 1, pp. 385–395, 2019.

[155] P. Buitelaar, P. Cimiano, and B. Magnini, *Ontology learning from text: methods, evaluation and applications*. IOS press, 2005, vol. 123.

[156] G. Petasis, V. Karkaletsis, G. Paliouras, A. Krithara, and E. Zavitsanos, "Ontology population and enrichment: State of the art," *Knowledge-driven multimedia information extraction and ontology evolution*, pp. 134–166, 2011.

[157] P. Mateiu and A. Groza, "Ontology engineering with large language models," 2023. [Online]. Available: https://arxiv.org/abs/2307.16699

[158] L. M. Sanagavarapu, V. Iyer, and Y. R. Reddy, "Ontoenricher: a deep learning approach for ontology enrichment from unstructured text," in *Cybersecurity and High-Performance Computing Environments*. Chapman and Hall/CRC, 2021, pp. 261–284.

[159] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access control for iot: A survey of existing research, dynamic policies and future directions," *Sensors*, vol. 23, no. 4, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1805

[160] L. Urquhart, "An argumentation and ontology based legal support system for ai vehicle design," 2022.

[161] O. Ishmilh, M. A. Jarwar, and Y. Javed, "A novel iot middleware for secure pharmaceuticals condition monitoring in supply chain," in *2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2024, pp. 342–347.

[162] X. Xie, N. Moretti, J. Merino, J. Chang, P. Pieter, and A. Parlikad, "Enabling building digital twin: Ontology-based information management framework for multi-source data integration," 2022.

[163] X. Hu, Q. Chen, and M. Du, "Ontology-based multi-sensor information integration model for urban gardens and green spaces," in *IOP Conference Series: Earth and Environmental Science*, vol. 615, no. 1. IOP Publishing, 2020, p. 012023.

[164] T. S. Sobh, "A secure and integrated ontology-based fusion using multi-agent system," *International Journal of Information and Communication Technology*, vol. 25, no. 1, pp. 48–73, 2024.

[165] S. Ali, M. G. Kibria, M. A. Jarwar, H. K. Lee, I. Chong, and N. Mitton, "A model of socially connected web objects for iot applications," *Wirel. Commun. Mob. Comput.*, vol. 2018, Jan. 2018. [Online]. Available: https://doi.org/10.1155/2018/6309509

[166] S. Peldszus, J. Bürger, T. Kehrer, and J. Jürjens, "Ontology-driven evolution of software security," *Data & Knowledge Engineering*, vol. 134, p. 101907, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0169023X21000343

Muhammad Aslam Jarwar (Senior Member, IEEE) is a Senior Lecturer with the Department of Computing, Sheffield Hallam University, U.K. He served as a co-investigator for the Secure Ontologies for IoT Systems (SOfIoTS) project. His academic credentials include the distinction of being Fellow of the Higher Education Academy, U.K., and a private member of the 4D Special Interest Group (4DSIG) Network. Before his current role, he garnered invaluable experience as a research fellow specializing in industrial and cyber-physical system security modelling with the esteemed University College London (UCL), U.K., and as a research associate with the University of Manchester, U.K. Currently, he is the lead guest editor for a special issue within Sustainable Energy Technologies and Assessments Journal. He served as a Technical Program Committee (TPC) member for the 4th International Conference on Sustainable Technologies for Industry 4.0, showcasing his active engagement in the academic community. His impressive body of work includes authorship of numerous peer-reviewed articles and technical reports for the ITU-T. He is also recognized as a discerning peer reviewer for various esteemed journals and flagship conferences, including but not limited to IEEE Transactions on Industrial Informatics, IEEE Transactions on Network Science and Engineering, IEEE Internet of Things Journal, Springer Neural Computing and Applications, Elsevier Future Generation Computer Systems, IEEE Global Communications Conference (GLOBECOM), and IEEE International Conference on Distributed Computing Systems (ICDCS). His research interests include a wide spectrum, with a particular focus on areas such as the Internet of Things, cybersecurity, digital twins, ontologies, and applied AI.

Jeremy Watson is Emeritus Professor of Engineering Systems in the Faculty of Engineering Sciences, based in the Department of Science Technology, Engineering and Public Policy (STEaPP). Until August 2021 he was also Chief Scientist and Engineer at the Building Research Establishment (BRE).Between 2009 and 2012, Jeremy was Chief Scientific Advisor for the Department of Communities & Local Government (now DLUHC). He was Arup's Global Research Director between 2006 and 2013, and was awarded a CBE in the Queen's 2013 Birthday honours for services to Engineering. Jeremy was PI and Director of the eight-year (2016 - 24) £50m PETRAS National Centre of Excellence for Cybersecurity of IoT Systems - a collaboration of 24 universities - and co-creator of the UKRI SDTaP programme (Securing Digital Technologies at the Periphery of the Internet), which includes EPSRC PETRAS and Innovate UK Demonstrator initiatives. An electronics engineer by training, Jeremy has experience as a practitioner and director of pure and applied research and development in industry (BOC and Arup), the public sector and academia. He has held research, technical management and director roles in industry and universities plus voluntary service with DTI and BIS. Jeremy is a Chartered Engineer and a Fellow and past Trustee of the Royal Academy of Engineering. At the RAEng, Jeremy was founding chair of the National Engineering Policy Centre Committee. He is a Fellow of the Institution of Engineering Technology, and was President of the IET between October 2016 and October 2017. Jeremy is a member of the UK Committee on Research Integrity (UKCORI), leading on AI, and recently served on the NPL Science and Technology Advisory Council (STAC) with specific interests in digital metrology and quantum technologies. He was a founding Board member of the Technology Strategy Board (now Innovate UK), and was Chair of the Institute for Sustainability and of Building SMART UK. He also chaired the NERC Innovation Advisory Board, and served on Council of the Engineering & Physical Sciences Research Council (EPSRC).

Sajjad Ali (Senior Member, IEEE) is a Research Associate at the School of Computing, Engineering, and Intelligent Systems, Ulster University, U.K. He earned his Ph.D. in Information and Communication Engineering from Hankuk University of Foreign Studies, South Korea, and a Master's degree in Computer Science from the National University of Computer and Emerging Sciences, Pakistan. He has contributed to the research and development of several national and international projects in collaboration with academia and industry. He has authored numerous peer-reviewed articles in esteemed journals and conferences and has developed technical reports for the ITU-T, FGDPM Section on smart cities and communities. Additionally, he has served as a peer reviewer for various renowned journals and conferences, including Elsevier's Future Generation Computer Systems (FGCS), IEEE Access, International Journal of Intelligent Automation and Soft Computing (IASC), Elsevier's Sustainable Energy Technologies and Assessments, International Journal of Flow Visualization and Image Processing, and the International Bhurban Conference on Applied Sciences and Technology (IBCAST). His research interests include the Internet of Things (IoT), Artificial Intelligence (AI), predictive analytics, digital twins, and knowledge graphs.