Advances in Knowledge-Based Systems, Data Science, and Cybersecurity; Research 1 (1) 78-107 Received 25-06-2024; Accepted 24-08-2024; Published 31-08-2024

Zero-Trust Security Model Applied to Smart Shipping: Towards a Feasible Architecture

S. Bargh, Mortaza m.shoae.bargh@wodc.nl
Research and Data Centre
Koningskade 4, 2596 AA The Hague, The Netherlands
0000-0001-5395-456X

Omar, Ahmad a.omar@hr.nl
Rotterdam University of Applied Science
Wijnhaven 107, 3011WN Rotterdam, The Netherlands
0000-0002-7726-5141

Choenni, Sunil r.choenni@wodc.nl
Research and Data Centre
Koningskade 4, 2596 AA The Hague, The Netherlands
0000-0003-2772-6330

Corresponding Author: Mortaza S. Bargh

Abstract

Securing information systems and assets within smart shipping environments is of utmost importance. In practice, however, securing smart shipping is a difficult and tedious task because smart shipping environments are highly dynamic, distributed, and loosely coupled, which cause having large threat/attack vectors without having all security measures under own control. The Zero Trust Security Model (ZTSM) has been suggested by security experts and many national cybersecurity centers as a promising approach for addressing the shortcomings of the traditional perimeter-based security architecture. However, a scalable ZTSM architecture which is applicable to large networks, like those of smart shipping, is missing. In this contribution we aim at investigating how the ZTSM can be made suitable for securing smart shipping. We study smart shipping security requirements and describe three off-the-shelf security services that can contribute to the realization of the ZTSM in such environments. Investigating these example security services inspired us to propose a ZTSM architecture for smart shipping environments, which relies on metadata exchange for trust establishment at various levels among federations of organizations, human or business controlled context and content transfer, and monitoring and controlling data and service usage. The proposed architecture can embody the ZTSM deployment within large networks of cooperating organizations (like those within smart environments). Although this architecture is proposed for and based on the security requirements of smart shipping, we conjecture that it can be applicable to other forms of smart environments as well.

Keywords: Architecture, Federated, Smart shipping, Security, Zero trust security model

Citation: Mortaza Bargh, et. al . Zero-Trust Security Model Applied to Smart Shipping. Advances in Knowledge-Based Systems, Data Science, and Cybersecurity; Research.2024;1(1):5.

1. INTRODUCTION

Information technology advances are increasingly impacting our lives and transform our society on every scale. For the last three decades, the concept of smart environments in its various forms (like smart transport, smart shipping, smart city, smart healthcare, smart logistics, and smart government) has emerged as a promising direction to take full advantage of information technology in different domains. Information and Communication Technology (ICT) is a key element of smart environments that enables collecting data from various data sources, integrating the collected data into useful information, exchanging integrated information, and supporting decision makers with collective intelligence that is based on the exchanged information [1].

Despite the success that data-driven smart environments are experiencing, there are still many key stumbling blocks in their large-scale and real-life deployments. Realizing smart environments, on the one hand, entails several technological challenges like establishing efficient mechanisms for integration, storage, and retrieval of (large volumes of) data, and processing (different types of) data in real-time. On the other hand, there are many non-functional or so-called soft challenges for sharing and using data in practice, like mitigating the security issues of largely distributed data-reliant systems, managing the data quality issues of loosely coupled data sources, and dealing with unjustified discrimination of individuals and groups (i.e., unfairness) as embedded in collected data or induced due to inattentive data processing. Not handling these soft challenges appropriately and adequately would harm individuals, groups, and society; adversely affecting public safety and basic human rights like privacy, liberty, autonomy, and dignity. Therefore, all societal, environmental, technological transformations affected by or derived from smart systems must be attentive and respectful of, among others, safety and security principles [1].

In this contribution, we consider the special case of smart shipping [2], where the integration of new technologies – like (industrial) Internet of Things (IoT), cloud services, Artificial Intelligence (AI) and Machine Learning (ML) – enables ships and some port services to (co)operate at various levels of autonomy [3] [4]. Smart environments, in general, and smart shipping, in particular, can be characterized as being highly dynamic (i.e., participating individuals, devices, and resources may join and leave at any time), distributed (i.e., the physical boundaries of the environment may span globally over many locations, organizations, administration domains), and loosely coupled (i.e., there might be no established business, institutional, and personal relationships; in other words, there might be no trust relationships at business/organizational, technical, and operational levels). These characteristics require establishing ad-hoc service level agreements and trust relationships at various levels to provision services and share data in such environments.

Increasing data communication and information processing capabilities of maritime objects and allowing these systems to interact autonomously can, however, lead to increased cybersecurity risks. Therefore, securing information systems and assets within such environments is important and necessary. In practice, securing smart (environments and) shipping is a difficult and tedious task because of having a large threat/attack vector [5], and not having all security measures under own control. In this setting, as a result, the traditional solutions with perimeter-based security architecture, i.e., giving access to assets based on network location or being connected via a Virtual Private Network (VPN) to the own network is not suitable.

The security model of zero trust has been recommended by security experts and national cybersecurity centers to address the shortcomings of the traditional perimeter-based security architecture [6]. However, it is unclear how to apply the Zero-Trust Security Model (ZTSM) to smart environments such as maritime. Further research is needed about how the ZTSM can be applied to various organizational settings, such as a single organization and across-organizations, where ships communicate and share data with ships or services of own or other organizations, respectively. Particularly, it is needed to investigate the scalability of the ZTSM architecture to large networks, the ease of the ZTSM applicability to proprietary settings (like for shipping and transportation), and enhancing the ZTSM user friendliness and organizational acceptance[7].

In this contribution, we aim at investigating how the ZTSM can be made suitable for securing smart environments, i.e., to share data and provision services across organizations securely. To this end, we consider smart shipping as a use case representing a typical smart environment. Our research questions can be formulated as:

1. What are the implications of smart shipping (or alike smart environments) imposed on the ZTSM?
2. How can the ZTSM be realized structurally in smart shipping (or similar) environments?
3. What are the challenges in applying the ZTSM to smart shipping (and similar) environments and what are the solution directions?

As our contributions in this paper, we will argue that in the context of secure smart shipping, there is a need for having trust establishment *at various levels* as well as putting users and organizations in control of sharing their data, credentials and sensitive information. Subsequently, we suggest adopting a federated architecture for ZTSM deployment in smart shipping settings, which is based on metadata exchange at various levels (e.g., at the business, personal, and physical levels) among (federations of) organizations. *The proposed architecture fills in the existing gap for structuring the ZTSM deployment within large networks of cooperating organizations (like those within smart environments)*. To motivate the proposed architecture, we argue that the ZTSM can be seen as rebranding the already existing (security) concepts such as federated identity management, putting users in control of their credentials, and having a continuous access control. Thus, a federated architecture that supports these concepts can structure the ZTSM deployment within smart shipping (and alike) environments. Through giving insight in some limitations of the ZTSM, we will also address the third research questions by calling for further research that aims at integrating (and/or enhancing) the ZTSM with, among others, ad-hoc trust establishment models and risk based trust establishment methods.

For this study we have conducted a critical literature review [8], where several selected papers are analyzed and a reflection done on the existing concepts, models and approaches. Our results, although being positioned within the context of smart shipping, can be applicable to other smart environments like smart city, smart logistics, smart healthcare, smart industry, and smart disaster management.

In the remainder of the paper, we present the background information that comprises the related work in Section 2 and review the relevant characteristics of smart shipping in Section 3. Subsequently, in Section 4, we provide a short description of three security mechanisms which can be regarded

as important building blocks of the ZTSM in smart shipping (and similar) settings. We propose an architecture in Section 5 for applying the ZTSM to large networks like those of smart shipping. We discuss the implications of the proposed architecture and the limitations of applying the ZTSM to smart environments, and suggest a few research directions for addressing these limitations in Section 6. Finally, we draw some conclusions in Section 7.

2. BACKGROUND

In this section, we shortly present the theoretical background of the study in Subsection 2.1 and discuss the related work in Subsection 2.2.

2.1 Relevant Concepts and Principles

Trust, trust establishment and trust management are key enablers of the vision of secure smart environments. Further, the ZTSM represents a specific view on (some aspects of) these concepts. In this section, therefore, we start with explaining a view on trust and trust management that is relevant for our scope in Sections 2.1.1 and 2.1.2, and give a review of the ZTSM in Section 2.1.3.

2.1.1 Trust and trust establishment

Despite the existing efforts to define trust in a very specific way, for example by relating it to authentication, authorization or the ability to pay for a purchase [9], trust is a complex concept that also relates to belief in, among others, honesty, trustfulness, competence and reliability. Some argue that trust is a subjective decision based on perceived (thus, may be not real) vulnerability, which makes trust decisions not necessarily rational [10]. Nevertheless, for practical reasons, many bodies have defined or conceptualized trust, like the ITU's X.509 recommendation that defines trust as: "Generally, an entity can be said to trust a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects" [11]. Without loss of generality, let's adopt a similar definition to the ITU definition as "[t]rust of a party A in a party B for a service X is the measurable belief of A in that B will behave dependably for a specified period within a specified context" [12]. In this case, party A is called the relying party and party B is the trusted party.

There are various ways for establishing such a trust. For example, the trust relation can be established via policies, contracts, recommendations, reputations, and predictions [13]. In this paper we are concerned with those mechanisms that are based on metadata (like certificates, recommendations, and contracts) and exchanging this metadata. These are common mechanisms for trust establishment in distributed settings (like smart shipping). The metadata (exchange) should, in turn, be done trustfully. This suggests the need for establishing levels of trust between a relying party and a trusted party. For example, these levels in a business transaction could be [14]: *Trust on the business level* (e.g., to ensure the organization/company is trusted as a business partner), *trust on service Level* (e.g., to ensure that the service provided by the trusted party is according to the service standards), *trust on personal level* (to ensure the person behind shipment of goods or money

is trustworthy), and *trust on the physical level* (e.g., to ensure that physical or digital objects and goods are transferred trustfully). The depth and nature of the trust levels depend on, among others, the type of the business activity, the actors involved, and the context in which the activity takes place. Having all these levels of trust, so-called *horizontal trusts*, is necessary to establish the trust relationship from the relying party to the trusted party.

Further, we note that, for establishing horizontal trust relations, there must be vertical trusts established between these levels. As an example of a vertical trust relationship, an enterprise trusts its employee for making a business transaction. In this contribution, we are interested in establishing cross organizational trusts, which means that we are concerned with horizontal trusts. Thus, from this point on, we assume that vertical trust relationships hold between levels of horizontal trusts.

2.1.2 Trust management models

In a smart environment, trust must be established and managed between the involved entities (e.g., persons, devices, organizations, etc.). Trust management can be achieved by exploiting the properties of trust: being context dependent, being directed from a relying party to a trusted party, being a measurable belief, existing in time, evolving in time, and being transferable. Note that being transferable is not exactly the same as having relational transitivity (as mentioned in [12], ”transferability in our case corresponds to influencing the level of trust rather than relational transitivity”). Considering the properties of trust, one can identify various forms of trust relations such as [15]:

- *Peer-to-Peer Trust,* where trust is established between individual entities directly (i.e., without involvement of another party). An example is the trust in two tiered system between a client machine and a server.
- *Transitive (or transferable) Trust,* where trust is established via an intermediary party, meaning that A trusts B and B trusts C, then A trusts C. An example is multi-tiered systems where trust is propagated through interconnected entities.
- *Web of Trust,* where trust in a party is established through endorsements from multiple peers. Examples are the PGP (Pretty Good Privacy) model for cryptographic key verification and the consensus mechanism in the blockchain.

For managing the above-mentioned trust relationships, one can identify the following structural models or architectures:

- *Centralized Trust Model,* where a central entity acts as intermediary to establish trust with the other entities or between any couple of the other entities. For example, in traditional client-server architecture, a central server manages authentication of all clients.
- *Distributed Trust Model,* where trust is established via multiple entities without having any central entity. An example is the trust established in a blockchain network [16].
- *Hybrid Trust model,* which combines elements of centralized and distributed trust models. Here, one can further identify

– *Hierarchical Trust Model,* where trust between entities A and B is established through those entities on the hierarchical path between nodes A and B.
– *Federated Trust Model,* where trust is established between entities from multiple domains. Each of these domains my have its own hierarchical structure. An example of this model will be discussed in Section 4.1.

In this contribution, we investigate and motivate the applicability of the Federated Trust Model to establish trust at multiple levels in smart shipping settings. Moreover, adopting the federated trust model leads to or prescribes a system architecture for large-scale smart environments. In this way, as we will argue, the designed system preserves and makes use of the structure of the vast number of organizations that collectively form the ecosystem of smart environments.

2.1.3 Zero-trust security model

The ZTSM is a paradigm, mentality, or mindset according to which trust is not assumed beforehand, and it should be re-established every time that an entity tries to access or use resources. For example, according to ZTSM, end-users must be authenticated and authorized every time that they access resources. As such, the term zero-trust does not equate to distrust, but to trust after a fresh verification. The ZTSM ”is built on the notions of least privilege, granular access control and dynamic and strict policy enforcement wherein no user or device is implicitly trusted–irrespective of stature or location” [6]. As such, ZTSM is an approach (not concrete guidelines or security measures) that is based on the following main tenants:

- *Resource:* Every digital asset is a resource. Examples are: hardware, datasets, applications, and services.
- *Communication security:* Communication channels, irrespective of the location and by default, are secured by using encryption as much as possible.
- *Session security:* Granting access to resources should be per session and according to the need-to-know principle.
- *Dynamic access control:* Determine access to resources dynamically by continuous authentication, authorization, and observation of the access state.
- *Information logging:* Every possible access information should be collected and used to improve the security posture.

The logical architecture of the ZTSM, as illustrated in FIGURE 1, consists of three core components: the Policy Enforcement Point (PEP), the policy administrator and the policy engine. The policy engine is responsible for deciding whether to grant, deny, or revoke access to resources based on enterprise policies and external inputs. It logs these decisions, which the policy administrator then executes by establishing or shutting down communication paths between users and resources. The policy administrator also manages session-specific authentication, relying on the policy engine’s decisions. The PEP implements these decisions, controlling and monitoring the connections. Together, these components ensure secure access within the system. As part of the control plane,

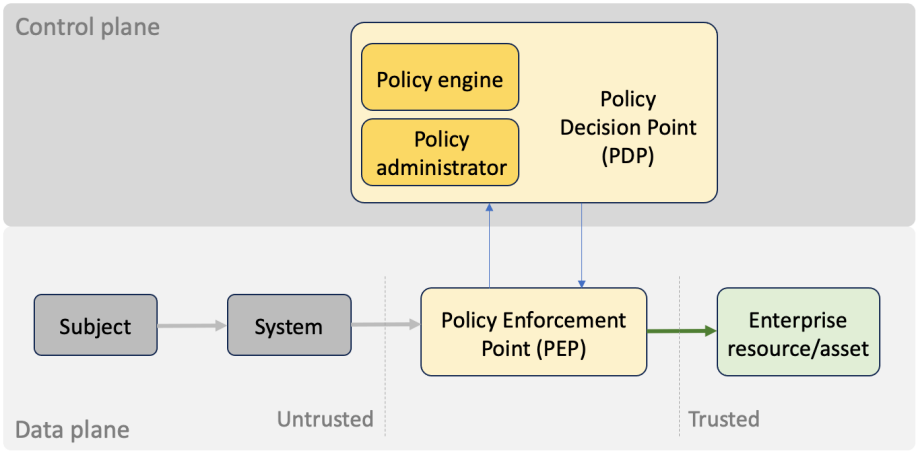

Figure 1: An illustration of the ZTSM logical architecture, see also [6]

policy administrator and policy engine constitute the Policy Decision Point (PDP), which in large part rely on contextual information to make security related decisions based on some policies [6].

In summary, the ZTSM characterizes the time-line and contextualization of the trust establishment process and does not specify the organizational aspects of trust establishment. This organizational aspect of the ZTSM is the one that we want to elaborate upon in this contribution. More specifically, we will elaborate on the structuring of the PEPs and PDPs (i.e., their structural architecture) in smart shipping settings.

2.2 Related Work

A number of efforts has been devoted to the technical feasibility, security and safety requirements, and challenges of autonomous vessels. For example, the MUNIM project [17] carried out a feasibility study for autonomous operation of an unmanned vessel during deep-sea voyage (thus, not in congested or restricted waters). In addition to technical and operational security (like safety, security and reliability of integrated ship data networks and infrastructure), the project investigated legislation, liability, insurance and contractual issues. The Autoship project [18], developed a framework for assessing the safety, security and cybersecurity of autonomous shipping. The resulting framework, called Safety, Security and Cyber-Security Assessment Framework (SSCSAF), can help eliciting the requirements to which the autonomous shipping operation must comply, identifying the hazards and unwanted events, and determining the ways to mitigate the risks (i.e., reduce either the probability or impact) of those hazards and events. The framework can be applied to various technical components of Maritime Autonomous Surface Ships systems (MASS) that enable autonomous and unmanned ship operations such as Situational Awareness (SA) system, Remote Control Centre (RCC), Connectivity and Cyber-Security System (CCSS), and Autonomous Navigation System (ANS). The Advanced Autonomous Waterborne Applications (AAWA) project [19], aims at realizing the ANS. The project requires having oversight on cybersecurity needs dynamically and proactively. To this end, taking various cybersecurity measures are needed such

as data classification, data encryption, user identification, authentication and authorization, data protection against unauthorized use, data integrity protection, connectivity protection, and activity logging and auditing. In addition to automatic measures, it is needed to have a sufficient amount of human resources, as the level of cybersecurity depends on education and the organizational culture for guiding the people involved. The use of blockchain technology within the maritime industry is considered as a forward-looking approach to protect autonomous vessels and operation centers against cybersecurity threats [16]. In general, the use of blockchain technology is advantageous due to its inherent decentralized, transparent, and tamper resistant features[20]. None of the efforts mentioned above, have elaborated on applying and using the ZTSM in smart shipping settings with continuous monitoring, having access and usage control, and putting users in control.

The paradigm of smart shipping consists of ”networks of connected ships and shore-based facilities equipped with digital entities” [21]. This paradigm is therefore referred to as ”the Internet of Ship (IoS)” [21]. The authors of [22], introduce a layered approach to cybersecurity, and integrate those layers in their network architecture of smart shipping for autonomous ships. The introduced layers are: off-ship layer, general ship layer, integrated ship control (ISC) layer, process layer, and instrument layer. Using the layers introduced, the authors discuss security threats and countermeasures. We adopt also a similar layered approach within our proposed architecture for establishing trust at multiple levels via using and exchanging metadata.

In [7], several architectural propositions for ZTSM based systems have been reviewed. The authors report that the existing works mostly focus on small networks, such as those for organizations and private homes, and conclude that the works proposing ZTSM architectures for large-scale networks, such as those for smart cities, are missing. ”While researchers suggest that following zero-trust principles results in a highly scalable infrastructure, an architecture for such large-scale networks has not yet been proposed, demonstrated, or tested” [7]. In this contribution, we propose an architecture which advocates a federated approach for applying the ZTSM to large scale networks as in smart shipping settings (and to smart environments). Using a federated approach together with the ZTSM is already proposed in [23], for realizing (cross organizational) identity management. Similarly, a NIST report [6], proposes adopting the federated identity management model as a use case to control access to resources across organizations. The proposed identity management in [23], is context based and allows context exchange under user control to protect user privacy. In this work, we propose and argue about extending the applicability range of the federated approach beyond identity management and consider it as a promising architecture of the ZTSM for large scale networks. To this end, we focus on explaining the applicability of the federated architecture to establish trust at multiple levels in smart shipping settings. This choice stems from the need for the system design to preserve and utilize the organizational structures of numerous organizations that collectively shape the ecosystem of smart environments. We believe that adopting the federated model can facilitate the adoption and scalability of the envisioned smart environments in general, and more specifically in smart shipping, because the federated model aligns well with existing organizational structures. Furthermore, the architecture supports continuous monitoring, having proper access and usage control, and putting users in control when necessary as envisioned within the ZTSM.

3. CHARACTERISTICS OF SMART SHIPPING

Here we provide an overview of the smart shipping ecosystem and review its cybersecurity requirements in Subsections 3.1 and 3.2, respectively.

3.1 Cyber-Physical Ecosystem

Following the industry 4.0 trend that intended to leverage digital technologies such as the IoT, AI, and Big Data Analytics for automated manufacturing and manufacturing processes, the term Shipping 4.0 was coined in 2016 to describe the new developments in digitalization of shipping [24]. Nowadays, almost all ships are equipped with digital instruments and make use of automated services to some level. As a result, various levels of autonomy have been identified in smart shipping. For example, van Dijk et al. [25] identify the following 7 levels: manual (level 0), decision support on board (level 1), on-board or shore-based decision support (level 2), system based overall navigation/operation calculations (level 3), execution with human supervision and intervention (level 4), monitored system-based decision-making (level 5), and full autonomy (level 6). Without loss of generality, we describe the structural setting of remotely operated vessels and autonomous vessels; which coincide with the higher levels of shipping autonomy in [25]. Such an ecosystem of so-called cyber-enabled ships (C-ES) [24], represents the most challenging setting from the viewpoint of cybersecurity and trust establishment.

A typical C-ES ecosystem consists of the vessel itself, other ships in the vicinity, a Shore Control Center (SCC) that controls the vessel, and the communication links between the vessel and the SCC [24]. For a secure and safe operation of smart ships, both Information Technology (IT) and Operational Technology (OT) systems are crucial. The communication link for vessel-shore communications is often established via satellite networks; unless the vessel is close to shore, where 3G, 4G and 5G mobile networks can be used. For the scope of this paper, we abstract from the communication link as it transparently transports data between the vessel, the SCC and the other ships. Further, we note that the sketched smart shipping ecosystem can be extended with components that enable the vision of smart ports [26], where one tracks vessels and containers in order to manage port traffic, allocate priorities, stack containers optimally at the port terminals, facilitate the transition from manual to automated ports/terminals, and optimize existing port processes.

The bridge and engine systems within ships communicates with SCC and other ships. The former communicates navigation, voyage and safety related data; and the latter communicate engine related data. Further, one can identify the following subsystems within the C-ES ecosystem that enable smart shipping (and smart ports) [24]:

- *Automatic Identification System (AIS),* which provides information needed for traffic monitoring to ensure ship's safety and enhance the situational awareness. In addition to internal navigational subsystems, AIS shares (voyage and safety-related) data with two external entities, namely: the SCC and the other ships in the vicinity.
- *Electronic Chart Display Information System (ECDIS),* which provides information about the ship's voyage. In addition to internal navigational subsystems, ECDIS shares (voyage and safety-related) data with the SCC and the ship controller.

- *Global Maritime Distress and Safety System (GMDSS),* which alerts (on)shore authorities in the event of emergency. In addition to internal subsystems, the GMDSS shares the emergency related data with the SCC.

The authors in [27], introduce the Maritime Architecture Framework (MAF) as an architectural methodology for developing new maritime systems. There are two viewpoints in the MAF that are interesting for us, namely topological and interoperability viewpoints. The topological view captures the same structural entities as those described above, namely, the vessel, other vessels, those in the shore. The interoperability view captures various layers for smart shipping systems, namely: Regulation and governance, functions and (elemental) services, data and information exchange, communication protocols, and system components like human agents, applications, devices and network infrastructure. In our view, these levels of the interoperability views can be related to the trust levels to be discussed in the following sections.

Finally, we note that various systems generate (enhanced) data in a smart ship and share it with other entities. For example, an onboard Situational Awareness (SA) system fuses sensory information from different sensory sources to map local obstacles for enabling reactive collision avoidance. The SA information is then communicated with a RCC for remote human interaction and control in situations where the ship autonomy cannot resolve or is not allowed to handle by itself. Further, the Autonomous Navigation System (ANS), enables ship navigation by using the vessels' SA system in combination with AIS data received from other vessels. All the data and information exchanged between a vessel and other vessels or an RCC, which may traverse organizational boundaries, should be exchanged securely and reliably across those organizations (i.e., to be protected against intentional tampering and unintentional hazards), as will be described in the following section.

3.2 Security Requirements

As mentioned, the operational setting of smart shipping is highly dynamic, distributed, and loosely coupled. Ships equipped with digital technology, specially C-ESs which are controlled and monitored remotely, have increased attack surface (i.e., having an increased number of vulnerabilities). This makes them more vulnerable to cyber-attacks, as revealed by various researches [24]. Further, lack of already established trust relationships (at business/organizational, technical, and operational levels) asks for establishing, among others, ad-hoc business collaborations, service level agreements, and trust relationships.

Protecting these C-ESs and vessels against cyber-threats is not only about safeguarding assets but also about maintaining maritime safety, environmental protection, and the security of global supply chains [24]. Several publications have elaborated on cybersecurity related threats and requirements for (smart) shipping including autonomous shipping. For example, for conventional vessels, [28], describes the security requirements of the components of the vessel control system, derived from relevant standards. One of these standards is the IEC 61162-460 standard [29], that describes the security requirements of onboard maritime navigation and radio communication equipment and systems. In [24], the authors use a systematic approach to elicit security requirements of the cyber-physical systems of the C-ES.

In the following, we group the security requirements for smart shipping that we have encountered in a few categories relevant for our study (i.e., highlighting the needs for trust establishment at multiple levels, context transfer, and continuous service/data usage monitoring). Note that it is not our intention in this paper to be exhaustive and cover all cybersecurity requirements for smart shipping. First, we recapture the typical data content that should be transferred from a smart ship, namely:

- *Navigation, voyage, engine and safety data,* which is transferred between onboard navigation and control systems and the Human Machine Interface (HMI) of the SCC exchanges.
- *Voyage and navigation data,* which is transferred between onboard navigation and control systems and other ships. This data is relevant to, for example, the e-navigation concept of the International Maritime Organization (IMO) safety and security standards. The e-navigation concept denotes ”the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment” [30].

In some situations, there should be a mechanism or an authority to adjust the content and authorize the content transfer. For example, the system administrator should be able to command locking the Human Machine Interface (HMI) of the AIS system. Or, the ECDIS must control the flows of voyage data sent to other ships and the SCC.

Based on security threats that exist in smart shipping (and alike) environments, there are numerous security requirements identified in literature, as mentioned above. These requirements ask for establishing trust relationships at various levels and with arbitrary entities (i.e., those who are encountered on an ad-hoc basis). For example,

- *At the physical level,* the voyage data transferred between AIS and SSC should be protected against tempering and damage (data integrity), and the safety signals sent by ECDIS and the data sent by GMDSS signals to SCC should be authenticated. The AIS system should be authenticated. The stress signals sent by the GMDSS should be encrypted.
- *At the personal level,*, the actors reading, modifying and transmitting AIS data should uniquely be identified. The use of ECDIS is only for authorized personnel.
- *At the service level,* the audit of the data sent/received by the ECDIS should be possible.
- *At the business level*, onboard and shore based systems must be maintained regularly by a third party. The involved parties must rely on established trust relationships to monitor those systems and be able to maintain it in time by, for example, conducting necessary system updates.

In Table 1 we provide some security requirements relevant to our study together with links to the corresponding references. Considering these selected requirements, we conclude that it is necessary to establish trust at multiple levels in smart shipping (and alike) environments, and possibly among those who have not already established a peer-to-peer trust relationship (on an ad-hoc basis).

Aspects	Type	References
Service integration	Physical level	”Reliable authentication mechanisms must be in place in order to uniquely identify the actors reading, modifying, and transmitting AIS data, as well as to authenticate the system itself and its services” [24].
Service integration	Personal level	”System maintenance must be performed only by well-trained personnel” [24].
Service integration	Service level	”real-time cargo tracking” [21]
Content transfer	Physical level	”The authenticity of the transmitted GMDSS signals and data in transit to the Autonomous Ship Controller (ASC), to other subsystems, and to the SCC must be ensured” [24].
Content transfer	Personal level	”The GMDSS must be able to detect whether the signal/data comes from a legitimate user/system or from a malicious user” [24].
Content transfer	Service level	”The ECDIS must be able to control the flows of voyage-related data sent to other ships and to the SCC” [24].
Continuous monitoring	Business level	”Appropriate mechanisms must be employed to validate hardware, software, and data from the suppliers” [24].
Continuous monitoring	Service level	”Integration of information from multiple stakeholders in intrusion detection systems can be a challenging task” [31].

Table 1: A selection of the security requirements for smart shipping that are relevant to our proposed architecture for realizing the ZTSM in smart shipping settings.

The trust at the personal level requires communicating parties in smart shipping to be, among others, authenticated and authorized according to the ZTSM for exchanging data and information. For example, an agent or an end-user onboard on a ship wants to continuously know about (or monitor) the locations and trajectories of nearby vessels, which can be seen as a service provided by a local SCC. In smart shipping settings, such an Service Provider (SP) and such a Service Requester (SR, like end-users, agents or devices) may belong to different organizations (or administrative domains) without a prior business, service, personal and/or physical level trust relationships. Such a personal level trust can be established via Identity Federation in a scalable manner, which is practically proven effective in cooperative cross organizational settings. Such a federated identity management, however, requires or relies on establishing trust at higher levels. For example at the service level one must assure that the Identity Provider (IdP) of the SR and the SP have a trustful communication (i.e., have a technical trust for delivering authenticated, authorised, and encrypted data communication) and have a trustful business relationship (i.e., have a behavioural trust in delivering desired business transactions). While the former can be established via exchanging public-key information trustfully (e.g., via a Public Key Infrastructure (PKI), the latter can be established via, for example, establishing trade contracts and service level agreements. Both of technical and behavioral trusts are established by exchanging appropriate metadata (i.e., public-key certificates and contracts) trustfully. In the following section, we describe a federated identity management service as the key component of realizing ZTSM at a personal level together with its higher level metadata exchange ingredients.

4. REPRESENTATIVE SECURITY SERVICES

In this section, we explain three representative security services that deliver those aspects of the ZTSM that inspire and substantiate our proposed ZTSM architecture for smart shipping (and alike) environments. We envision federated trust establishment at various levels to be a key aspect of the ZTSM for smart shipping. In Section 4.1 we describe a typical federated identity management to illustrate the concept. In addition to establishing trust, two important aspects of the ZTSM are user controlled data transfer across organizational boundaries and monitoring/controlling the usages of assets and resources. For each of these aspects, we describe one typical security service in Sections 4.2 and 4.3, respectively.

4.1 Federated Identity Management

To illustrate the concept of a federated identity management service, we review a typical federated identity management service that has been used widely for authenticating and authorizing individuals who are members of different organizations. These organizations collaborate with each other by sharing their resources with authenticated and authorized users from these collaborating organizations. These authentication and authorization of users are enabled by Identity Federation (IdF) service, which is based on trustfully sharing user identities and credentials among organizations. A user's identity here is the set of information about her, such as her ID and affiliations (i.e., the organization to which she belongs, like a university or workplace).

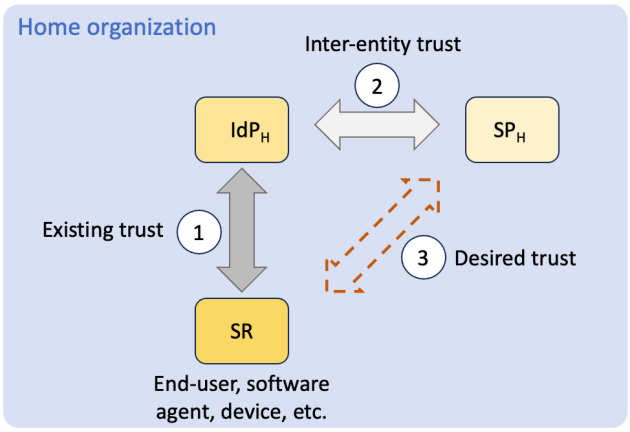

Figure 2: Trust fabric of service provisioning

An example of an inter-university IdF is SURFcontext [32], through which users associated with Dutch universities and research institutions can seamlessly access some services provided by other Dutch universities without having to register as a new user with these other universities. For example, a student of Dutch university A can connect to the WiFi network of Dutch university B, without being affiliated with the latter. "SURFcontext connects your institution (identity provider) with a single link to various service providers. Authentication, authorization, group management and agreements on privacy and security are partly handled centrally for you by SURFcontext" [32]. Via its dashboard, the SURFcontext federation enables provisioning about 1082 services to its members currently [33].

One can apply the concept of federation hierarchically among several cooperating federations. For example, eduGAIN [34], is an international inter-federation that interconnects research and education identity federations from various countries, most of which are Europeans. It enables the secure exchange of information related to identity, authentication and authorization between organizations from the participating federations. The dashboard of the SURFcontext federation enables provisioning about 261 services to eduGAIN members currently [33].

4.1.1 Establishing inter-entity trust in home setting

In a generic identity management setting, an SR wants to use services wherever they are and SPs want to offer their services to as many users and devices as possible. FIGURE 2 shows the trust fabric of such a typical service provisioning. These SRs establish trust relationships with their own organizations via Identity Providers (IdPs). Link 1 in FIGURE 2 represents the trust between the SR and IdP, where both of which are co-located in one organization (i.e., within so-called home organization) and the SP resides in the organization (that is why the suffix H appears). Whenever there is a trust relationship between SPs and IdPs in place, see link 2 in FIGURE 2, SRs and SPs can establish a transitive trust relationship with each others, as indicated by link 3 in FIGURE 2, based on which they can trust each other to offer or use services, respectively.

The trust relationship between SPs and IdPs in FIGURE 2, or so-called the inter-entity trust, entails SP trusting the IdP in its assertions concerning the SR's identity and related attributes. Accordingly, the IdP trusts the SP in being a legitimate service provider to deal with user identity information. For establishing the inter-entity trust it is required that:

(a) The communication channel between the SP and the IdP is secure in the sense that both endpoints' identity can be verified, the affiliations of the entities with their federations can be approved, the authenticity of the data exchanged can be verified, and the privacy of the data exchanged can be preserved (since the exchanged data includes user identity information).

(b) Both entities behave as expected by, for example, abiding to the real-world contracts, laws, policies, conventions, etc. Here the subjective trust aspects play a role as well. Subjective trust can be based on, for example, previous behaviour and reputation of the other entity, situational context, authenticity of attribute values, and quality of identity management.

The trust relation defined in item (a) is called "technical trust" in [35], and it implies having trust in each other's identity. The trust relation defined in item (b) is called "behaviour trust" in [35], and it implies having trust in each other's intention. Note that both trusts are needed to produce the inter-entity trust relationship.

4.1.2 Establishing inter-entity trust in federated setting

The inter-entity trust between SPs and IdPs is a key enabler of trust establishment for service provisioning and data sharing. This inter-entity trust exists (or can be hard-coded) when both IdPs and SPs are within one organization (see FIGURE 2). In smart environments, however, users (or devices) are highly mobile and may desire to use the services of other organizations when visiting those organizations, as indicated in FIGURE 3. Often there is no already established inter-entity trust between visited SP (SP_V) and home IdP (IdP_H), and it should be established at run-time (in an ad-hoc way). A solution would be to have a central IdP across all organizations that a user (or device) might visit. This solution is, however, not scalable and, moreover, the central IdP would become a single point of failure.

Practically, the inter-entity trust can be established in various ways like by signing contracts, taking procedural measures and exchanging metadata [36]. The former two are suitable within one organizational settings and are too slow or not scalable for ad-hoc trust establishment across organizations. In establishing inter-entity trust via exchanging metadata, as indicated in FIGURE 3, the metadata may include (a) the data-items required for establishing the inter-entity technical trust (e.g., entity descriptor, service endpoints, embedded certificate, expiration time of metadata, contact information) and (b) some data items required for establishing part of the inter-entity behavioural trust (e.g., scopes/list of requested attributes, tags from trusted third parties). Metadata exchange is technically realizable and it plays a key role in establishing inter-entity trust relationships within and among identity federations (like the SURFcontext federation within Dutch universities and the eduGAIN cross federation within, among others, European higher education institutions). Metadata exchange in such federated identity management involves the exchange of information that enables trustful and Security Assertion Markup Language (SAML) based identity management. It

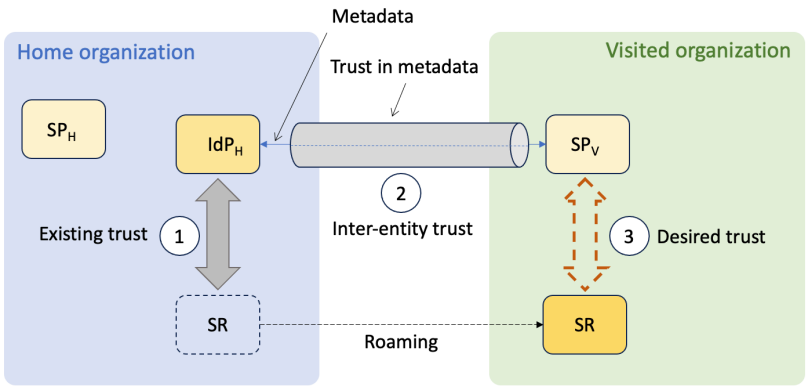

Figure 3: Establishing trust when a SR vising another organization

bootstraps a secure transaction between an IdP and a SP, which previously used to be encoded into the implementation in a proprietary way.

An intriguing aspect of metadata exchange is that the metadata itself must be exchanged trustfully, as shown also in FIGURE 3. The entity receiving the metadata of the other entity must be assured about the authenticity of the metadata as endorsed by the underlying federated collaboration. Distribution of metadata in a trustful way across organizations which may reside in different federations can be done by technical solutions such as PKI (based on public key certificates and attribute certificates), directory services such as DNSSEC, and exchanging an XML file that is signed by a trusted metadata publisher and that can be authenticated by a metadata consumer [36]. These trusted metadata publisher and metadata consumer are represented by Metadata Aggregator (MA) per organization in FIGURE 4. The XML exchange approach is recommended for all Shibboleth deployments and is adopted by Europe's higher education federations for the eduGAIN confederation. We also adopt exchanging signed XML files in this paper as it is technically convenient and can easily be tailored to, for example, smart environment settings.

4.1.3 Summary

To summarize the concept behind trust establishment within federated identity management, we sketch three service provisioning scenarios in FIGURE 5. The objective in all three scenarios is to exchange service related data between a SP and a SR. However,

- In Scenario 1 and for Service_1, both SR and SP are co-located within the home organization (i.e., the organization with which the SR is affiliated). Here the metadata at level 1 is exchanged between SP_H and IdP_H.
- In Scenario 2 and for Service_2, the SR and SP are located at two different organizations, which are co-located within the same home federation. Here the metadata at level 1 is exchanged between SP_{VH} and IdP_H, which is enabled by exchanging metadata at level 2 between metadata aggregators MA_H and MA_{VH}.

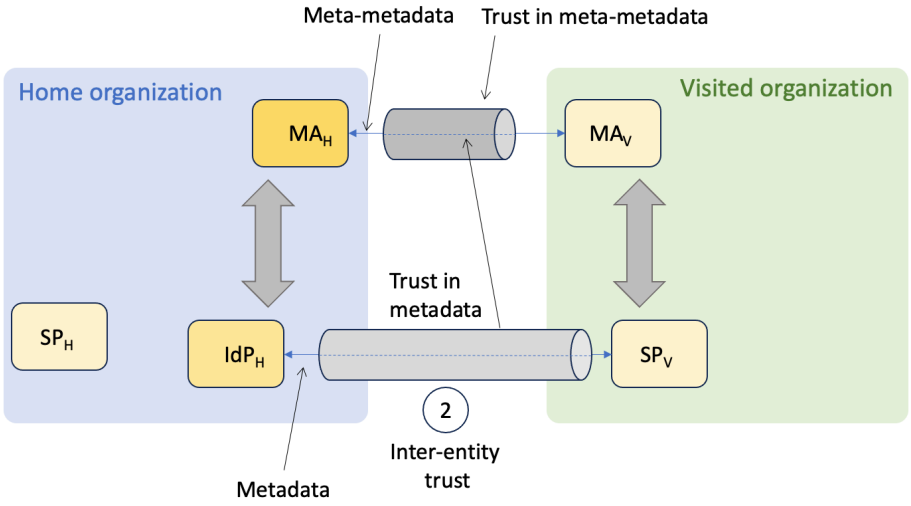

Figure 4: Establishing inter-entity trust between IdP_H and SP_V

- In Scenario 3 and for Service_3, the organizations of the SR and SP are located at two different federations. Here the metadata at level 1 is exchanged between SP_{VF} and IdP_H, which is enabled by exchanging metadata at level 2 between metadata aggregators MA_H and MA_{VF}, which is in turn enabled by exchanging metadata at level 3 between federation metadata aggregators F-MA_H and F-MA_V.

In FIGURE 5 the metadata exchanged at one level enables establishing trust at one level below. Due to the hierarchical structure of data and metadata exchange entities in FIGURE 5, the federated scheme offers a scalable mechanism for trust establishment from the viewpoint of the number of trust relationships needed. Further, the structural architecture of these components is superimposed on the existing organizational structure and, as such, the architecture does not impose drastic changes on the real-world organizational structures. Note that our intention here is to illustrate how trust is established in these settings by exchanging metadata and, as such, we do not intend to specify the exact content of the (meta)data exchanged and the type of the inter-party trust they induce/establish. These aspects are context dependent and must be chosen within the design space.

4.2 Putting Users in Control

In realizing identity management, it is necessary to exchange some contextual information relevant to an access request between a SR and a SP. For example, the ZTSM based federated identity management architecture proposed in [23], introduces a so-called Context Attribute Provider (CAP) to collect, manage and share contextual information about an SR. Hereby, an SP (a relying party) can control access using assertions from IdP and contexts from CAP. Sharing a user's contextual information may contain personal information. For example, Gakunin (the SURFcontext-like service in Japan) can share user attributes such as email addresses or employment/university affiliations, and their pseudonymous IDs [23]. Therefore, sharing contextual information must be under the control of users. Another example for using contextual information is proposed in [37], where the

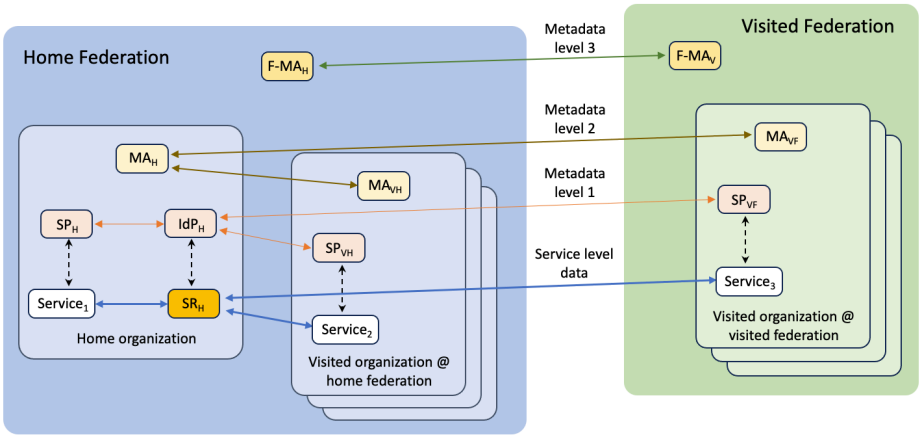

Figure 5: Data and metadata exchange levels for service provisioning in three different settings

contextual information is about the way that personal data is used at the data consumer side (i.e., it is a feedback about personal data usage). In this case, contextual information empowers users for controlling the usage of their personal information.

Enabling users to control which information they want to share with a SP (especially within a visited organization) concerns not only identity management related information (related to the metadata exchange at level 1 in FIGURE 5) but also any service level data sharing between entities (related to the service data exchange in FIGURE 5). Enabling users to control the content of the shared data or metadata is a key aspect of privacy and business sensitive information protection due to, for example, liability or privacy concerns [23].

An interesting protocol for enabling users to decide on sharing their (privacy sensitive) information is the myIdP service introduced in [38]. The myIdP is originally designed as a complimentary service to identity management. Nevertheless, it can be explored further for putting users in control of sharing any personal and business information whenever a SP (at a visited organization) asks for that. FIGURE 6 presents the steps of the myIdP protocol with minor adaption to the context of this paper, where we specifically indicate how users can be put in control of sharing their personal and contextual data. In step one, the user requests an e-form from the SP. After authenticating the user, in step 6 the SP requests some extra information/attribute about the user from the myIdP service (asking for, e.g., the address, the email and contextual information about the user). Steps 7 and 8 in FIGURE 6 provide users with a means to specify which extra information and in how much detail they want to share with the SP. In addition, as we envision, the myIdP component can apply other content adaptation like personal data minimization [39] [40], which aims at adjusting the amount of personal or business-sensitive data to the level desired by the user/business and needed by the SP. As such, the myIdP protocol is capable of providing more than identification related information, as we envision. Further, as indicated in FIGURE 6, the IdP and myIdP services can be located in the home organization and/or home federation of the SR, considering the discussions in Sections 4.1 and 4.1.3.

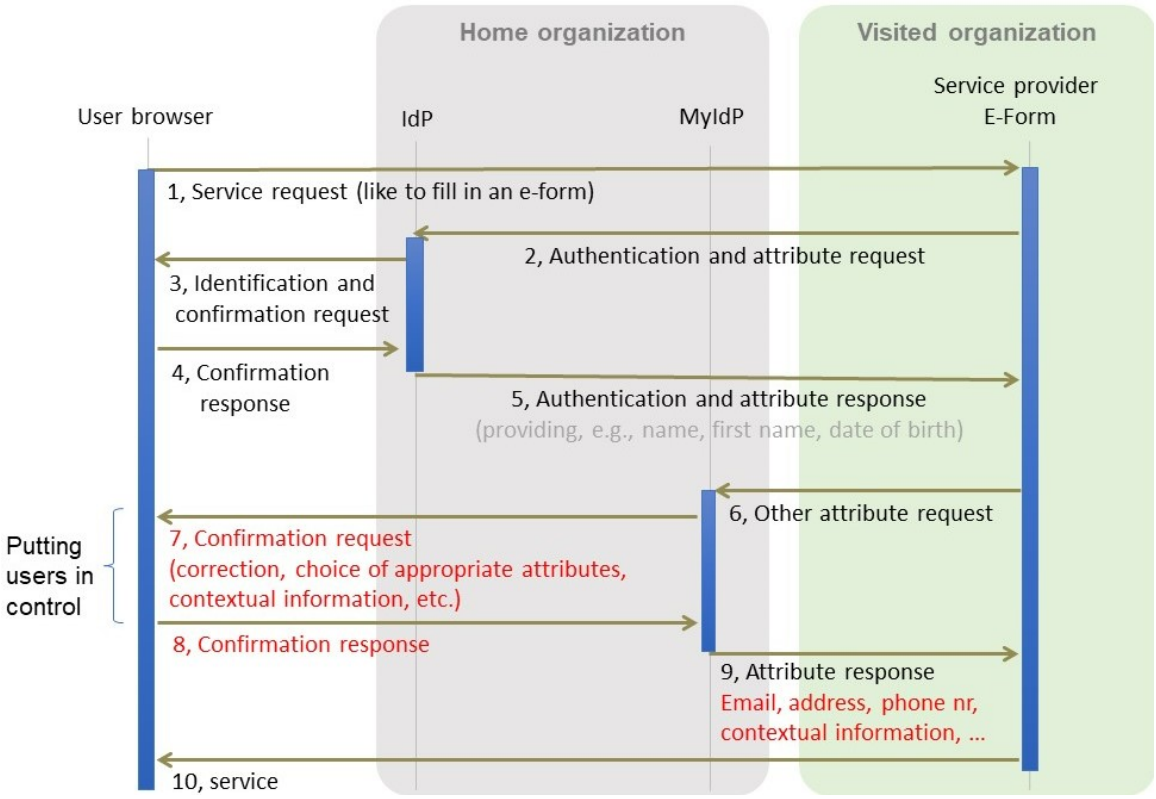

Figure 6: Adapted MyIdP protocol

4.3 Usage Control

Usage control is widely mentioned within the context of the ZTSM. We envision its relevance in cross federation settings such as smart shipping as well. There are nowadays compelling incentives for businesses and organizations to analyze all collected data available by data analytics tools and apply the results to their practice for, for example, improving their services and processes. As a result of this trend, the collected data may be used in another context, possibly for another purpose than the one they are collected for [41] [42]. Any inconsistency between the data collection/access context and the data usage context may cause harms on individuals and businesses. Further, use of personal data for a secondary purpose can conflict with privacy principles of transparency and intended purpose usage. Consequently, even when data is collected and accessed legitimately, one should still use it appropriately according to policies, guidelines, rules, laws, or the (current) preferences of data subjects.

There are many examples of usage control in practice. For example, Google's Continuous Access Evaluation Protocol (CAEP) is an event-sharing protocol that is used for continuous authentication in IdF [23]. An SP (being a relying party) can use the CAEP to share internally generated events about users with the IdP for context based authentication of users (events like a change of the network used or a vulnerability discovered in the user's device). Herewith the IdP can monitor the user's contexts in the SP environment and enforce continuous authentication based on notified contexts. As another example, in [41] [42], the authors motivate adopting a usage control mechanism for joining vertically-separated relational datasets and characterize it as obligations within a so-called Usage Control (UCON) model, described below.

Traditionally via access control a Subject seeks access to an Object (a resource) based on some access Rights, which determine whether and how the subject is allowed to access the object. For digital objects, for example, these access rights may include being able to do actions like reading, writing and deleting those objects. A so-called Reference Monitor uses the access Rights to grant or prohibit actions requested by a Subject on an Object. The traditional Access Control is static and is established once at the beginning of an access request. As mentioned, the ZTSM pleas for continuous monitoring of an access control, for which the traditional access control is not suitable.

The UCON model is introduced to cope with the shortcomings of the traditional access control models in [43] [44] [45]. The UCON model extends the traditional models to include also access decision continuity (for controlling the access decisions during the object's usage interval) and attribute mutability (for allowing also adapting the access criteria before, during and after object usage interval). Both continuity of decisions and mutability of attributes in UCON allow adapting to the changes of Subject, Object and environmental attributes before, during or after the data usage period. For example, the number of subjects that concurrently may access the object can change depending on the number of simultaneous requests (i.e., consumption intensity).

The reference monitor of the UCON model uses three types of decision-making factors. The first type is called Authorizations. These authorizations include those predicates that put constraints on Subject and Object attributes. Example attributes of the Subject are the name, age, role, and nationality; and those of the Object are document type, content sensitivity, and data ownership. The other two types of decision-making factors in the UCON model are Conditions and Obligations, which are not uniquely defined in literature [46]. The authors in [43], consider for conditions

the environmental or system-oriented constraints that should hold before or during the Object's usage interval. Example conditions are those related to the time of the day, room temperature, and disastrous situation. As such, conditions are not dependent of the Subject and the Object (i.e., the data) directly. Obligations are generally defined as those requirements that must be fulfilled before, during and after accessing a resource (so-called pre-obligations, on-going-obligations and post-obligations). Examples of obligations are: Give contact information before accessing a web-content, watch a short advertisement during watching a YouTube video, and notify the Object owner about the access within a number of days.

Exchanging trusted contextual information (metadata) is essential for realizing the UCON model in provisioning services within and across organizations in smart shipping settings.

5. PROPOSED ARCHITECTURE

Based on the insights gained from investigating the ZTSM in Section 2.2, characteristics of smart shipping in Section 3, and three representative services for the ZTSM in Section 4, we sketch a generic architecture for applying the ZTSM to smart shipping like environments in Section 5.1. Subsequently, we mention example use cases in Section 5.2, and review the scalability and performance considerations of the proposed architecture in Section 5.3.

5.1 A Generic Architecture

Smart environments, in general, and smart shipping, in particular, consist of many entities (e.g., physical objects, humans and software agents) that are able to move in the physical space by changing their spatial coordinates and/or in cyberspace by exploring the web-space. As such, a (web) space exploring entity may encounter new entities with whom it may need to exchange data for receiving or enabling a data driven service, without having an already established trustful relationship.

As mentioned in Section 4.1, metadata and trustful exchange of metadata at various levels are key enablers of trust establishment between interacting entities in smart environments. Structuring such a metadata exchange platform can be done in various ways, like central, hierarchical and peer-to-peer. A promising structure, as we foresee, is to rely on the existing organizational structures where (a) every organization manages its personnel and (digital) equipment based on its internal policies and systems, (b) some partner organizations join forces and collaborate on matters in common or on in common interests - in our vocabulary, they form a federation - and (c) alliances of organizations (i.e., federations) may also collaborate on various issues of common interest - i.e., they form federation among federations (or, in other words, confederations). Practice has shown that the sketched hierarchical structure among organizations (i.e., among members of every organization, organizations within federations, and confederation of federations) works well and can scale up organically. The well established and developed eduGAIN confederation [34], is an evidence of such an organic growth.

We observe that in practice, this extendable structure can become hierarchical downwards (i.e., towards individuals/entities within an organization) and become peer-to-peer upwards (i.e., towards

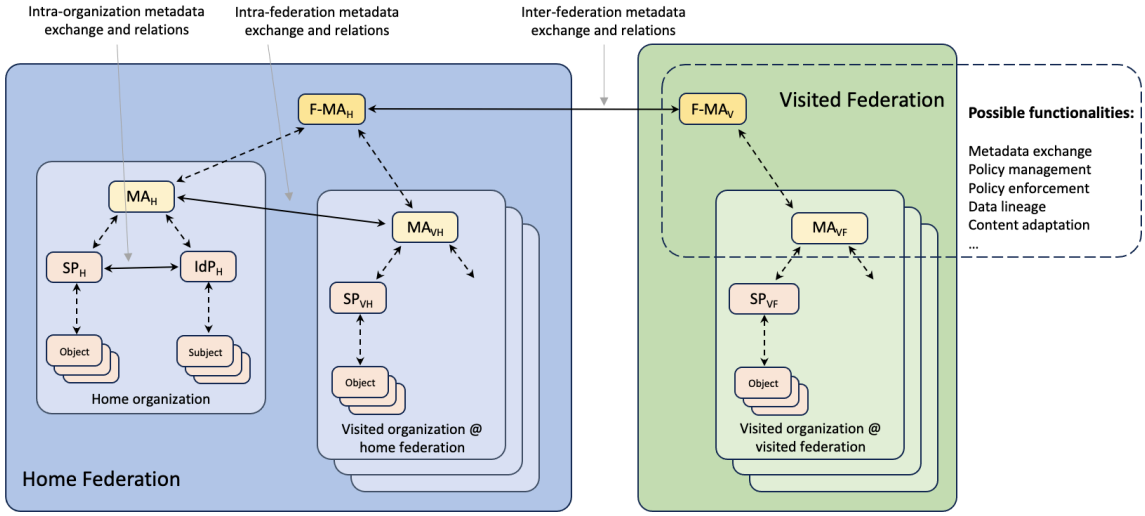

Figure 7: An illustration of proposed architecture for smart shipping

federations). This is because the number of the relations established at higher levels is not many, and the metadata of the higher level entities is at a high level of abstraction. This structure of hierarchical-downwards peer-to-peer upwards is illustrated in FIGURE 7, which we propose as a promising architecture for applying the ZTSM to smart shipping (and alike) environments. The proposed architecture can be related to that of edge computing [47], in the sense that (semi)autonomous domains are connected via gateways at the boundaries of those domains. A gateway is an entry/exit point to/from a domain, which is responsible for, among others, access control to the domain, content adaption towards outside the domain, service and data discovery within and across domains.

The Metadata Aggregators (MAs) in the proposed architecture can not only store and exchange per organization/federation ZTSM related metadata, but also host other ZTSM related functionalities like PEP, PDP and context transfer, content adaption; should the underlying components/parts of an organization or federation be unable to do so. As indicated in FIGURE 7, the MAs can also host other (i.e., non ZTSM related) functionalities that are based on metadata (exchange) needed for data sharing, data management, and data governance. These functionalities include per domain Service Discovery, Data Discovery, Data Catalog, and Data Lineage. Further, we note that the realization of the higher levels in FIGURE 7, e.g., that of confederation, can be centralized (e.g., via a trusted third party) or be made peer-to-peer (e.g., by using a blockchain). As an example of the latter, Matsubara et al. [48], propose an architecture for data lineage among collaborating organizations. The proposed architecture manages metadata related to data lineage hierarchically within organizations and uses a blockchain for exchanging metadata between organizations.

5.2 Two Use Cases

The authors of [23], propose and realize a federated identity management with context exchange possibility. The identity related context is shared across federations under the control of users to protect user privacy. This work can be seen as a use-case of the proposed architecture for federated

ZTSM approach whose scope is limited to identity management functionality. As explained in Section 5.1, we propose and argue about extending the functionality range of the federated approach beyond identity management by using it to establish trust between various entities at higher levels (e.g., establishing service level agreements and business level contracts). We note that these higher level trust relationships are also necessary for realizing the ZTSM. Like for identity management, in the proposed architecture these higher level trusts are based on the associations of the higher level entities (e.g., services and businesses) with collaborating federations (i.e., without having peer-to-peer trust relationships between these entities). Therefore, one may consider the proposed federated architecture as a promising architecture of the ZTSM for large scale networks. Adopting the proposed architecture, can lead to establishing federations at regional, national, and international scales (like The Netherlands, EU and IMO). Eventually, every entity would belong to and be managed by at least one organization which is a member of at least one federation. Such an structure does not only improve trust establishment processes (see the following section), but also makes tracing and/or discovering malicious activities manageable.

Other use-cases that showcase the practicality of the proposed architecture are the SURFcontext [32] and eduGAIN systems [34], being the federated identity management infrastructure for Dutch and European universities, respectively. As mentioned above, we suspect that the same level of practicality can be achieved when the federated architecture is adopted and used for also establishing higher levels of trusts as needed for (and suggested by us for) the ZTSM.

5.3 Scalability and Performance Considerations

Establishing trust in metadata requires that the metadata-publishing and consuming entities share meta metadata (or secrets, see FIGURE 3) for signing and validating (i.e, trusting) the metadata. Trusting metadata constitute the trust-fabric of the metadata exchange process, whose scalability with respect to the number of trust relationships can be considered within a federation or across federations. Without loss of generality, we consider the cross federation case where the involved SP and IdP entities belong to different federations. Most of the arguments below also hold for intra-federation cases with minor modifications.

Let's consider two example cases. In the first case, federation A likes to establish trust in metadata relationships between its IdPs and the SPs of the other federations. How many of such relationships are needed? (let's assume $n \approx 50$), where every federation has m IdPs and l SPs (let's assume $m \approx 200$ and $l \approx 2000$). Then, federation A in this case has to establish $m \times (n-1) \times l$ (in our example, $19,600,000$) relationships between its IdPs and all SPs of the other federations! However, in the proposed solution, federation A needs to establish m relations with its own IdPs and $0.5 \times n \times (n-1)$ peer-to-peer trust relationships among n federations (i.e., their local-MAs). Thus, the number of required relationships reduced to $m + 0.5 \times n \times (n-1)$ (in our example, 2652, which is a factor of 73991 difference). Instead of peer-to-peer relations among n federations, one may opt for another level of centralized meta-metadata aggregation for these n federations. In this case, there are n trust relationships needed to be established between the meta-MA and the local-MAs. Thus, the centralised meta-metadata aggregation protocol is more scalable compared to the distributed peer-to-peer meta-metadata aggregation protocol by another factor of $n-1$ (in our example, 49).

In the second case a new SP joins federation A. How many of the above mentioned trust relationships must the SP establish with the IdPs of the other federations? In this case the SP must establish $m \times (n-1)$ (in our example, $9,800$) relationships! However, in the proposed solution the SP needs to join one federation, i.e., establish one trust relation with the local-MA of its federation. This case, indicates a factor of $m \times (n-1)$ difference (in our example, $9,800$).

Other performance aspects (e.g., increased security complexity, increased local complexity and increased latency) are elaborated upon in the following section.

6. DISCUSSION

In this section, we discuss the limitations of the proposed architecture and identify a few avenues for future research.

Security complexity (and costs). Compared to the traditional approach to information system security, the ZTSM can lead to increased complexity and consequently can increase the costs associated with system design, implementation and maintenance. For example, developing dynamic and granular policies, as required within the ZTSM, for millions of distributed (IoT) devices and users is a complex task. Realizing the ZTSM (or any security solution) may not be justifiable economically whenever its marginal benefit becomes less than its marginal costs [49]. Lack of economical justification may hinder adoption of ZTSM technology. Therefore, it is necessary to adopt an incremental and iterative approach for a transition to the ZTSM, guided by cost–benefit considerations. The federated approach can facilitate such an incremental approach by (a) allowing organizations to join whenever they are ready to adopt the ZTSM, and (b) relying on the exiting organizational structure and thereby not imposing drastic changes to the current structures of organizations.

Local complexity. The proposed federated architecture offers a way to reduce complexity by reducing the number of trust relationships, reducing the burden of trust establishment and maintenance - as mentioned in Section 5.3 - and keeping sensitive information in the own domain. Nevertheless, it may, to some level, introduce new complexity and scalability issues. For example, the offered services within a federation of organizations and the need for specific services may vary in time. It is necessary to maintain a metadata set (like a data catalog) about available services in a federation so that discovery of these services becomes possible. There are costs associated with maintaining such metadata and data catalogs. There could be a point where maintaining the information about all services in a federation can become too expensive as the federation size increases. At some point, having perfect information about the entire federation becomes increasingly difficult and ultimately impossible. At this point, a federated system should be able to cope with using stale or incomplete information [15]. One way to mitigate this problem of too many services and entities in a federation is to distribute services and/or data catalog and use a search engine to find services/data of a desired type [15]. This metadata distribution, in our opinion, can follow the underlying organizational structure, as supported by the proposed architecture in Section 5. Another approach would be to keep track of only those services/data that are really used in practice, i.e., to make the service/data discovery business driven. How to achieve this objective is a subject of our future research.

Context-dependent discoverability. According to the ZTSM, the monitoring, discovery and protection of sensitive information and services should be categorized to mitigate potential risks and

threats. This categorization can be based on various factors such as importance, business sensitivity and privacy sensitivity of shared (meta)data and provisioned services. One can imagine that many services/datasets will be provided/shared in smart shipping environments. Further, the level of service provisioning and data sharing may depend on the context and the level of the trust established. Realizing service and data discovery in smart shipping environments, therefore, may need to be done at various classification levels, depending on the context and the level of trust established. In this way, moreover, access control can be done at finer granularity. Realization of a service and data discovery at various classification levels can increase the complexity of the discovery functionality in federated settings. To alleviate this, a Federation Broker Deployments (FBD) [50], can be used. Via subscribing to and using an FBD, organizations can subscribe to a catalog of discoverable services/data within a federation (or across federations) and find and access relevant services/data according to their classification levels. Using such an FBD can facilitate multilevel service discoverability within a federation or across federations.

Latency and priorities. Establishing trust using a remote or centralized policy engine can introduce unnecessary delays. In some settings (like emergency occasions and for maintaining safety), there is a need for real-time communication in an ad-hoc way. Often in such occasions, the communicating parties need to consider different priorities that determine how data are processed for ensuring quick decisions on emergency and safety matters. Communicating with a centralized or remote policy engine, as may be required by the ZTSM, can introduce unnecessary delays. A possible direction to reduce such delays is to adopt a graceful degradation of the ZTSM service, should safety and emergency situations arise. This degradation of security level, however, might not be acceptable in some situations. Another possible approach would be to adopt a hybrid approach for the ZTSM, where one allows part of the security policy to be executed locally, for example by delegating the PDP functionality residing at the visited edges/gateways or to the smart ship. For monitoring ship activities and for being situation aware, as required by the ZTSM as well as autonomous shipping, ships and ports are being enhanced with maritime IoT technologies. Adopting IoT technology would worsen the overall latency problem [51], as real-time processing of large volume data in the suggested approach for delegation of policy execution may not be affordable in IoT devices with limited processing and communication resources. Reducing latency of the ZTSM for IoT devices with limited resources is a challenging task [52]. How to apply the hybrid approach to smart shipping setting is a subject for our future research.

Flexibility and extensibility. One of the metadata type that the MA of a federation can provide (see FIGURE 7) is public key certificates (i.e., MA being part of a PKI, fulfilling a Certificate Authority task). Being part of a federation means that each member organisation complies with a minimum standard set by the federation. Such a federation can select several preferred CA [53], and suppliers to reduce the risk of possible attacks using untrusted authorities. In addition, each federation can establish its own security policy regarding to, among others, the availability of certain services, the security level of a public-key encryption when establishing trust among organizations and end-to-end communication. Further, the proposed architecture would simplify and reduce the complexity of adopting new Quantum-Resistant Algorithms (QRAs) or Post-Quantum Algorithms (PQAs) [54]. Current cryptography systems use relatively small key size in comparison to quantum-safe algorithms. Note that larger key size that quantum-safe algorithms use will impact the performance and security level when establishing trust relationships within federations and end to end communication. Therefore, there would be a need for future research on designing and implementing energy-efficient quantum-safe cryptography systems.

The realization of the ZTSM in smart shipping encounters additional challenges, including a shortage of skilled human resources, issues of accountability and liability, the reliability of IoT devices, and the compatibility and interoperability of IoT hardware and software from different manufacturers. There are many strategies for organizations to adopt ZTSM in general and in federation settings. The Zero Trust Maturity Model (ZTMM) is one of these strategies that can provide a road-map to adopt and comply with a targeted federation [55]. Using third party services, as also done in federated version, might be attacked through weakness in systems of third parties. Who is liable in such cases is another issue. The lesson learned from liability issues and cases within cloud federation services could be applied here [56][57]. Investigating these issues as well as how to resolve them in practice is for future research.

7. CONCLUSION

Smart shipping integrates new technologies such as (industrial) IoT, cloud services, AI and ML to allow ships and port services to (co)operate at various levels of autonomy. Increasing the data sharing and information processing capabilities of maritime objects and allowing these systems to interact autonomously can lead to increased cybersecurity risks. Therefore, securing information systems and assets within such environments is of utmost importance. In practice, however, securing smart (environments and) shipping is a difficult and tedious task because such environments are highly dynamic, distributed, and loosely coupled. These characteristics cause smart shipping environments to face large threat/attack vectors without having all security measures under own control. To deal with the shortcomings of the traditional perimeter-based security architecture, security experts and national cybersecurity centres have recommended the ZTSM. However, it has been unclear how to apply the ZTSM to smart environments such as maritime. Particularly, a scalable ZTSM architecture which is applicable to large networks, i.e. like those of smart shipping, is missing.

In this contribution we started with studying the implications of smart shipping (or alike smart environments) imposed on the ZTSM. To this end, we argued that there is a need for establishing (ad-hoc) trust relationships at various levels among abundant entities and actors (like end-users, agents and devices) involved in smart shipping. Further, as other implications, we argued about the necessity of putting users and organizations in control of sharing their sensitive data, credentials and contextual information as well as monitoring how data and services are used.

Considering these security requirements, we chose and described three off-the-shelf security services that can contribute to the realization of the ZTSM in smart shipping environments. To this end, we built on the fact that the ZTSM can be seen as re-branding the already existing (security) concepts. We gave an overview of a well-known federated identity management system called SURFcontext, a method/service for putting users in control of their credentials (the myIdP service), and a continuous access control model called UCON. The combinations of these example security services inspired us to propose a federated architecture for deploying the ZTSM in smart shipping environments, which relies on metadata exchange for trust establishment at various levels among (federations of) organizations, human/business controlled context and content transfer, and monitoring and controlling data and service usage. The proposed architecture can embody the ZTSM deployment within large networks of cooperating organizations (like those within smart environments). Although this architecture is proposed for and based on the security requirements

of smart shipping, we conjecture that it can be applicable to other forms of smart environments as well as to any other cooperating (semi-)autonomous organizations.

We elaborated on a number of challenges in applying the ZTSM to smart shipping (and similar environments) and sketched a few avenues for future research. There are costs associated with creating, distributing and maintaining the metadata in the federated architecture proposed. Distributing metadata, which, in our proposal, follows the underlying organizational structure, requires employing a powerful metadata discovery mechanism. An approach would be to keep track of only those metadata that are really used in practice, which implies making service/data discovery business driven. How to achieve a balance for metadata management is a subject of our future research. Further, in some emergency situations it might be too costly to rely on communicating with a centralized or remote policy engine, as required by the ZTSM. A possible direction to reduce such delays is to adopt a graceful degradation of the ZTSM service, should safety and emergency situations arise. This degradation of security level, however, might not be acceptable in some situations. Another possible approach would be to adopt a hybrid approach where one allows part of the security policy to be executed locally, for example at the ship. How to apply the hybrid approach to smart (shipping) settings is a subject for our future research. The reliability issue when using third party services is another issue for future research.

References

[1] Choenni S, Bargh MS, Busker T, Netten N. Data Governance in Smart Cities: Challenges and Solution Directions. J Smart Cities Soc. 2022;1:31-51.

[2] Sepúlveda Estay DA, Guerra P. The Wave Analogy of Cyber-Resilience as Applied to Shipping Operations. Cybersecurity Resil Arct. 2020:265-273.

[3] Felski A, Zwolak K. The Ocean-Going Autonomous Ship—Challenges and Threats. J Mar Sci Eng. 2020;8:41.

[4] MSC. IMO. Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships. London, UK: IMO, 2021.

[5] Silverajan B, Ocak M, Nagel B. Cybersecurity Attacks and Defences for Unmanned Smart Ships. In: IEEE International Conference on Internet of Things (Ithings) and IEEE Green Computing and Communications (Greencom) and IEEE Cyber, Physical and Social Computing (Cpscom) and IEEE Smart Data (SmartData); 2018:15-20.

[6] Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. National Institute of Standards and Technology. Gaithersburg, MD;2020:800-207.

[7] Buck C, Olenberger C, Schweizer A, Völter F, Eymann T. Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust. Comput Sec. 2021;110:102436.

[8] Paré G, Trudel MC, Jaana M, Kitsiou S. Synthesizing Information Systems Knowledge: A Typology of Literature Reviews. Inf Manag. 2015;52:183-199.

[9] Grandison T, Sloman M. A Survey of Trust in Internet Applications. IEEE Commun Surv Tutorials. 2000;3:2-16.

[10] Ølnes J. A Taxonomy for Trusted Services. In: Towards the E-society: E-Commerce, E-Business, and E-government. Springer.2002:31-44.

[11] Moses T. Trust Management in the Public-Key Infrastructure. Entrust seucring Digit. identities Inf.; 1999:5-20.

[12] Dimitrakos T. Systems Models, E-Rists and E-trust, Towards Bridging the Gap? Intowards the E-society: E-Commerce, E-Business, and E-government. Switzerland. Zurich; 2001;13: 45-58.

[13] Noor TH, Sheng QZ, Zeadally S, Yu J. Trust Management of Services in Cloud Environments: Obstacles and Solutions. ACM Comput Surv (CSUR). 2013;46:1-30.

[14] Bargh MS, Janssen W, Alko Smit. Trust and Security in E-business Transactions. GigaTS Project, Telemática Instituut, Enschede, The Netherlands; 2002.

[15] Lee CA, Bohn RB, Michel M. The Nist Cloud Federation Reference Architecture. 2020;500:332.

[16] Wang Y, Chen P, Wu B, Wan C, Yang Z. A Trustable Architecture Over Blockchain to Facilitate Maritime Administration for Mass Systems. Reliab Eng Syst Saf. 2022;219:108246.

[17] MUNIN. Munin Final Brochure: Research in Maritime Autonomous Systems Project Results and Technology Potentials; 2016.

[18] Bolbot V, Theotokatos G, Wennersberg LA, Faivre J, Nesheim DA. Autoship Deliverable d2.6. A Holistic Framework for Autonomous Shipping Safety, 2021.

[19] Jokioinen E. Advanced Autonomous Waterborne Applications Position Paper, Remote and Autonomous Ships: The Next Steps. rolls-royce .2016.

[20] Yaga D, Mell P, Roby N, Scarfone K. Blockchain Technology Overview. arXiv preprint arXiv:1906.11078, 2019.

[21] Bouhlal A, Aitabdelouahid R, Marzak A. The Internet of Things for Smart Ports. Procedia Comput Sci. January 2022;203:819-824.

[22] Cho S, Orye E, Visky G, Prates V. Cybersecurity Considerations in Autonomous Ships. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence; 2022.

[23] Hatakeyama K, Kotani D, Okabe Y. Zero Trust Federation: Sharing Context Under User Control Towards Zero Trust in Identity Federation. In: IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events .2021.

[24] Kavallieratos G, Diamantopoulou V, Katsikas SK. Shipping 4.0: Security Requirements for the Cyber-Enabled Ship. IEEE Trans Ind Inform. 2020;16:6617-6625.

[25] Dijk T, Dorsser H, Berg R, Moonen H, Negenborn R. Smart Ships and the Changing Maritime Ecosystem. 2018;6.

[26] Bouhlal A, Aitabdelouahid R, Marzak A. The Internet of Things for Smart Ports. Procedia Comput Sci. 2022;203:819-824.

[27] Weinert B, Hahn A, Norkus O. A Domain-Specific Architecture Framework for the Maritime Domain. 2016.

[28] DNVGL. Cyber Security Capabilities of Control System Components. tech. rep. 2018.

[29] International Electrotechnical Commission. Iec. Maritime Navigation and Radiocommunication Equipment and Systems. NEK IEC. 2018;2018:61162-460:152.

[30] International Maritime Organization (IMO) website. E-Navigation .2024 . Available from: https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx.

[31] Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M. Developments and Research Directions in Maritime Cybersecurity: A Systematic Literature Review and Bibliometric Analysis. Int J Crit Infrastruct Prot. December 2022;39:100571.

[32] Surfconext, Secure Access Everywhere With One Set of Credentials .2024. Available from: https://www.surf.nl/en/services/surfconext.

[33] Srufcontext id dashboard website .2024. Available from: http://surfconext.nl/apps/all.

[34] Edugain's Technical Site.2024. Available from: https://technical.edugain.org.

[35] Young IA, La Joie C. Interfederation and Metadata Exchange: Concepts and Methods.2024.

[36] Bargh MS, Hulsebosch B, Zandbelt H. Scalability of Trust and Metadata Exchange Across Federations; 2010.

[37] Bargh MS, Meijer R, Choenni S, Conradie P. Privacy Protection in Data Sharing: Towards Feedback Based Solutions. In: Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance, ICEGOV'14. New York. Association for Computing Machinery; 2014:28-36.

[38] Laube A, Hauser S. Myidp-the Personal Attribute Hub. Fifth Int Conf Adv Serv Comput. 2013:1-5.

[39] Bargh MS, Vlietinck H, Amighi A, Omar A, Yang S, Daniels N et al. Directions for Enhancing the Use of Personal Data Minimization Technology in Public Organizations. In: Proceedings of the 25th Annual International Conference on Digital Government Research. Association for Computing Machinery. 2024:232-240.

[40] Bargh MS, Latenko A, van den Braak S, Vink M, Meijer R. Personal Data Protection in the Justice Domain: Guidelines for Statistical Disclosure Control Reeks Cahier Technical Report, reeks Cahier. 2021-10: PU-Tools 2.0 project.

[41] Bargh MS, Vink M, Choenni S. On Usage Control in Relational Database Management Systems: Obligations and Their Enforcement in Joining Datasets. In: International Conference on Information Systems Security and Privacy. SciTePress Digital Library. 2017;2:190-201.

[42] Bargh MS, Vink M, Choenni S. On Using Obligations for Usage Control in Joining of Datasets. Commun Comput Inf Sci, Information Systems Security and Privacy (ICISSP 2017). 2018;867:173-196.

[43] Park J, Sandhu R. The Uconabc Usage Control Model. ACM Trans Inf Syst Secur. 2004;7:128-174.

[44] Sandhu R, Park J. Usage Control: A Vision for Next Generation Access Control. In: Gorodetsky V, Popyack L, Skormin V, editors. Proceedings: Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2003, St. Petersburg, Russia, Security: Computer Network; Springer .2003;2:17-31.

[45] Zhang X, Parisi-Presicce F, Sandhu R, Park J. Formal Model and Policy Specification of Usage Control. ACM Trans Inf Syst Secur. 2005;8:351-387.

[46] Colombo P, Ferrari E. Enforcing Obligations Within Relational Database Management Systems. Depend Secur Comput IEEE, translator. 2014;11:1-14.

[47] Qiu T, Chi J, Zhou X, Ning Z, Atiquzzaman M, et. Al,. Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges. IEEE Commun Surv Tutorials. 2020;22:2462-88.

[48] Matsubara M, Miyamae T, Ito A, Kamakura K. Improving Reliability of Data Distribution Across Categories of Business and Industries With Chain Data Lineage. Fujitsu Sci Tech J. 2020;56:52-59.

[49] Collier ZA, Sarkis J. The Zero Trust Supply Chain: Managing Supply Chain Risk in the Absence of Trust. Int J Prod Res. 2021;59:3430-3445.

[50] Lee CA, Bohn RB, Michel M. The Nist Cloud Federation Reference Architecture. NIST Spec Publ. 2020:500-332.

[51] Liu RW, Nie J, Garg S, Xiong Z, Zhang Y, et al,. Data-Driven Trajectory Quality Improvement for Promoting Intelligent Vessel Traffic Services in 6G-Enabled Maritime IOT Systems. IEEE Internet Things J. 2021;8:5374-5385.

[52] Liu C, Tan R, Wu Y, Feng Y, Jin Z, et al. Dissecting Zero Trust: Research Landscape and Its Implementation in IOT Cybersecurity. 2024;7:20 .

[53] Chuat L, Krähenbühl C, Mittal P, Perrig A. F-Pki: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure. arXiv preprint arXiv:2108.08581, 2021.

[54] Abuarqoub A, Abuarqoub S, Alzu'bi A, Muthanna A. The Impact of Quantum Computing on Security in Emerging Technologies. In: Proceedings of the 5th International Conference on Future Networks and Distributed Systems, ICFNDS'21. New York. Association for Computing Machinery; 2021:171-176.

[55] Cybersecurity and Infrastructure Security Agency Cybersecurity Division. Zero Trust Maturity Model; April 2023.

[56] Levite AE, Kalwani G. Cloud Governance Challenges: A Survey of Policy Andregulatory Issues. Washington, DC: Carnegie Endowment for International Peace; 2020.

[57] Nekit K, Kolodin D, Fedorov V. Personal Data Protection and Liability for Damage in the Field of the Internet of Things. Jur Tribune J= Tribuna Juridica. 2020;10:80-93.