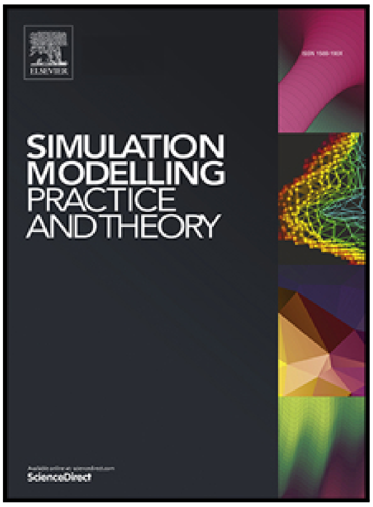


CAAVI-RICS Model for Observing the Security of Distributed IoT and Edge Computing Systems

Saša Pešić, Mirjana Ivanović, Miloš Radovanović, Costin Bădică

PII: S1569-190X(20)30064-2
DOI: https://doi.org/10.1016/j.simpat.2020.102125
Reference: SIMPAT 102125

To appear in: *Simulation Modelling Practice and Theory*

Please cite this article as: Saša Pešić, Mirjana Ivanović, Miloš Radovanović, Costin Bădică, CAAVI-RICS Model for Observing the Security of Distributed IoT and Edge Computing Systems, *Simulation Modelling Practice and Theory* (2020), doi: https://doi.org/10.1016/j.simpat.2020.102125

CAAVI-RICS Model for Observing the Security of Distributed IoT and Edge Computing Systems

Saša Pešić[a], Mirjana Ivanović[a], Miloš Radovanović[a], Costin Bădică[b]

[a] University of Novi Sad, Faculty of Sciences, Trg Dositeja Obradovića 4, Novi Sad, Serbia
[b] University of Craiova, Craiova, Romania

Abstract

The pervasive integration of 'things' in the Internet of Things together with state-of-the-art computer systems provide a stimulating environment for creativity and business opportunities, but also a large range of security challenges. Engineering the security of such systems must acknowledge the peculiar conditions under which such systems operate: low computational capacity, distributed decision-making, significant node churn, etc. These conditions must, therefore, be supported by the techniques and methodologies for building secure and robust IoT systems. With CAAVI-RICS methodology we explore credibility, authentication, authorization, verification, and integrity of IoT and edge computing systems, through explaining the rationale, influence, concerns, and security solutions that accompany them. Our contribution is a complete and detailed systematic categorization and streamlining of security problems, covering the security environment of IoT and edge computing systems. Besides, we contribute to the debate on key aspects of edge computing security and state-of-the-art solutions.

Keywords: Edge computing, IoT, cyber-security, distributed security

1. Introduction

Since its appearance, cloud computing has provided the easiest way to remotely store and access data and services. Cloud computing has rapidly brought about a revolution in how we develop our services and applications by providing on-demand self-service, multi-tenant processing resources, broad network access, pooling of resources, fast provisioning, and rapid elasticity. Despite its capacity, the cloud-based application building model does not extend to use-cases where disrupting time-sensitive functionalities and inducing

Email addresses: sasa.pesic@dmi.uns.ac.rs (Saša Pešić), mira@dmi.uns.ac.rs (Mirjana Ivanović), radacha@dmi.uns.ac.rs (Miloš Radovanović), cbadica@software.ucv.ro (Costin Bădică)

higher latency can result in catastrophic events (e.g. vehicle-to-vehicle communication). Even though the cloud offers a range of advantages, it introduces new concerns about security, privacy, availability of data and services, reliability, and performance.

Hence the concepts of the Internet of Things (IoT) and Edge Computing (ECP) systems. IoT cyber-physical systems are enabled through a multitude of technological innovations: on-demand adaptive resource management frameworks, lightweight communication, and data protection protocols, etc. ECP is a computational framework/deployment methodology where data analytics and decision-making processes are moved from cloud closer to data sources, i.e. to the edge of the network. ECP vastly reduces the volume of data that is sent through the network, improves overall system security, responsiveness, and latency.

Security problems and attack points for IoT/ECP systems are not so different from centralized systems. Nonetheless, addressing protection at the edge is considerably more difficult, since IoT systems are deployed in areas that are usually out of rigorously managed environments (i.e. data centers). Besides, ECP systems should use distributed protection mechanisms (protection steps and activities that are carried out collectively by a subset of nodes) since a central decision-making body imposes a single point of failure. Besides, these mechanisms need to be computationally light and undemanding to be deployed on IoT devices such as smartwatches, single-board computers, microchips, sensor devices, and embedded software [64].

There are several ways to look at the security aspect of the system: layers, application scope, resource usage, location, etc. Without a proper model for assessing the protection of these layers, it is difficult to decide what needs to be protected, at which layers, and how.

For this purpose, we propose a novel methodological framework i.e. the CAAVI-RICS categorization methodology for IoT and edge-computing systems' security. CAAVI is an acronym for Credibility, Authentication, Authorization, Verification, and Integrity principles, while RICS is an acronym for Rationale, Influence, Concerns, and Solutions aspects. So far, in our previous articles we particularly focused on the Authentication [48] and Credibility [47] principles. In this paper, through discussing RICS we intend to systematically explain each of the CAAVI principles for IoT/ECP systems, focusing on real-world security concerns and solutions. CAAVI-RICS model provides an overview of the security landscape in IoT/ECP systems and contributes to the discussion on the aspects of ECP security challenges and state-of-the-art (SoTA) solutions. The interconnection of CAAVI principles is discussed as well. This paper aims to contribute to the acceptance of the IoT/ECP paradigm, as required by the emergence of 5G, by explaining its technological and resource-management advantages as well as unique security challenges and practical flaws.

The rest of the paper is structured as follows: Section 2 presents related work; Section 3 discusses each of the CAAVI principles through RICS;

Section 4 offers a unifying perspective on the CAAVI principles; Finally, Section 5 presents the concluding remarks.

2. Related Work

The related work is focused on papers creating distinct categorizations and/or overviews of security solutions and/or concerns in IoT/ECP systems.

Mahmoud et al. address countermeasures to protect IoT systems through authentication, trust-building, federated architectures, and security-awareness [34]. In their IoT security and threat taxonomy, Babar et al. address solutions in detection, communication, physical threats, embedded security, and storage management [4]. An algorithmic overview of solutions is provided by Cirani et al., where solutions are divided into the following chapters: security protocols, lightweight cryptographic algorithms, key distribution and management, safe data aggregation, and authorization [9]. Kumar et al. are dividing ECP security into network, data, access control, privacy, and attackers Interest in private data [26], while Khan et al. have defined 12 security categories for systematic analysis, some of which are: Advanced Persistent Threats, Data and information Loss, Insecure APIs, Insufficient Due Diligence, Abuse, and Nefarious Use [24]. It is currently the most thorough systematic study of security problems and possible solutions for ECP systems. Yi et al. discuss security across six chapters: trust and authentication, network security, secure data storage, secure and private data processing, privacy, access control, and intrusion detection [81].

Although the papers listed in this section provide a detailed overview of the security of IoT and ECP systems, they neither examine the abstractions above the proposed security categories nor provide an overview methodology that may be compatible not only with their categorization but also with others. Furthermore, the above papers generally address IoT systems as a mixture of cloud and ECP paradigms. Our paper focuses on the edge, thereby distinguishing our research from the papers mentioned in this section. Also, the security taxonomy described in this research may be extended to other types of computer systems.

We have published two papers on the CAAVI-RICS methodology analyzing Credibility and Authentication principles in-depth [46, 48]. Since each of the CAAVI principles is complex and valuable for the methodology and could be published individually, we focused our previous papers on deepening the discussion on the two principles. The contribution of this paper is, thus, connecting credibility and authentication principles to authorization, verification, and integrity principles completing the CAAVI-RICS methodological overview. The result is a design-and-implementation dependency analysis between the principles that also illustrates their inseparability. This thoroughly-described and extensively discussed bridge of principles, i.e. the CAAVI-RICS model applies to a wide range of computer systems.

3. Methodological Security Overview Framework for ECP Architectures – CAAVI

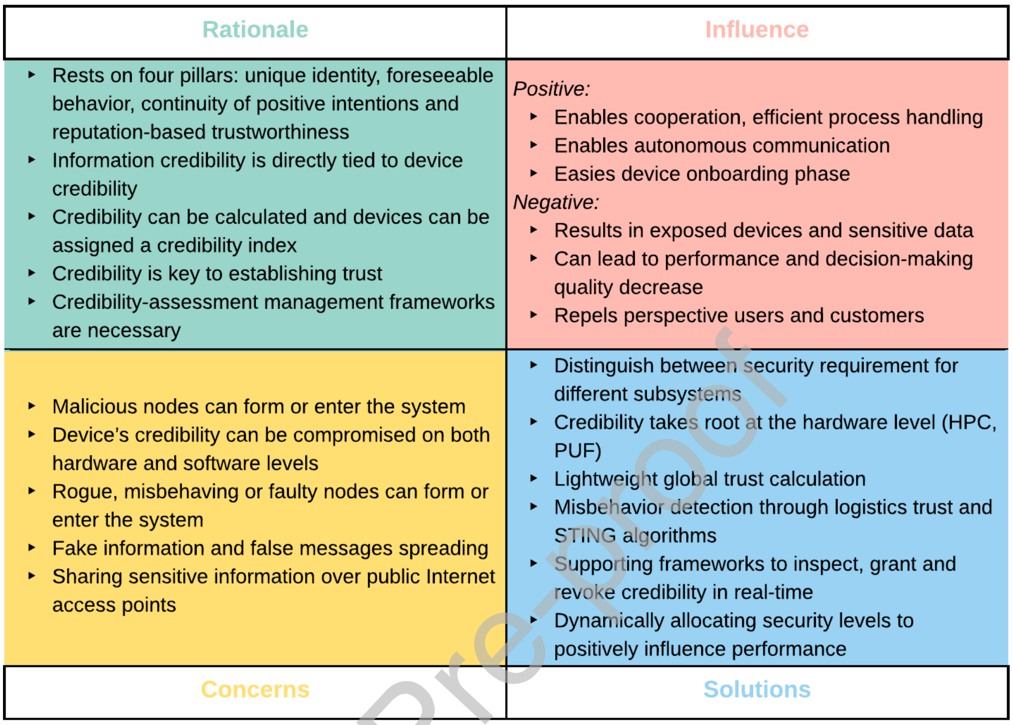
In the rest of this section, we will elaborate on CAAVI-RICS, our proposed methodological framework for discussing security aspects of computer systems, focused on IoT/ECP. CAAVI is an acronym for Credibility, Authentication, Authorization, Verification, and Integrity. Credibility refers to whether the edge node is not malicious, i.e. it is trustworthy and thus legitimized to function inside the system. Authentication manages the identity of the nodes, so that the nodes may access or modify data. An authenticated node is the one that can unquestionably prove its unique identity. Authorization refers to obtaining official privileges to conduct system-wide activities. Verification is the process of determining the truth, accuracy, or validity of a system action and its results (we are focused on data). Integrity is the guarantee that data has not changed during transmission (we concentrate on detecting malicious behavior leading to corruption of system integrity). The CAAVI will be discussed through considering 4 aspects (RICS): (1) Rationale (what is it and why is it important?), (2) Influence (how does it affect the overall system well-being if (not) implemented correctly), (3) Concerns (what problems does it bring?) and (4) Solutions (review of current SoTA solutions).

There are three essential rules for the design of ECP security solutions: (1) be efficient, responsive, and resource preserving; (2) act at the edge layer in collaboration with peers; (3) dynamically adapt and advance through feedback. In discussing CAAVI SoTA solutions, we pay particular attention to complying with these rules. Security solutions for all following CAAVI principles will be discussed from two standpoints: (I GROUP) solutions that bring new or improved algorithms, techniques and schemes for security enhancement; (II GROUP) solutions that propose new or improved security management frameworks, architectures, and middlewares, methods, and methodologies. Original authors' comments on presented security solutions are written in *italic*.

3.1. Credibility

This section applies RICS on the credibility principle of CAAVI. The credibility principle of the CAAVI model has been presented in detail in our previous paper [48]. The summary of the results of RICS applied to the credibility principle is given in Figure 1.

Rationale – Credibility is the process of creating trustworthy relationships between devices. It is invaluable in decision-making processes and allows for the establishment of autonomous communication channels between resource-constrained edge nodes. The credibility of ECP nodes must be founded on four pillars: Identity, Behavior, Continuity, and Reputation. Firstly, each node must have its own unique identity and at any time be able to authenticate itself to the entire network. If the identity is compromised, the node must be immediately blacklisted. Second, the actions of



Rationale

- Rests on four pillars: unique identity, foreseeable behavior, continuity of positive intentions and reputation-based trustworthiness
- Information credibility is directly tied to device credibility
- Credibility can be calculated and devices can be assigned a credibility index
- Credibility is key to establishing trust
- Credibility-assessment management frameworks are necessary

Influence

Positive:

- Enables cooperation, efficient process handling
- Enables autonomous communication
- Easies device onboarding phase

Negative:

- Results in exposed devices and sensitive data
- Can lead to performance and decision-making quality decrease
- Repels perspective users and customers

- Malicious nodes can form or enter the system
- Device's credibility can be compromised on both hardware and software levels
- Rogue, misbehaving or faulty nodes can form or enter the system
- Fake information and false messages spreading
- Sharing sensitive information over public Internet access points

Concerns

- Distinguish between security requirement for different subsystems
- Credibility takes root at the hardware level (HPC, PUF)
- Lightweight global trust calculation
- Misbehavior detection through logistics trust and STING algorithms
- Supporting frameworks to inspect, grant and revoke credibility in real-time
- Dynamically allocating security levels to positively influence performance

Solutions

Figure 1: Credibility summary.

all devices must be predictable. All system actions must be established and recognized by the network [15]. Third, the credibility of the system should not be assumed upon a single honest action, but instead the consistency i.e continuity of actions with good intentions. Furthermore, reputation-based trustworthiness audit is an option [13]. The credibility of each node should be assessed, thereby giving it a reputation in the system. If credibility is maintained over some time, the node will earn rewards and, as a result, its reputation will increase, and vice versa. The credibility of a certain node can be quantified, and then calculated through a method called credibility calculation. Calculation of credibility is the process of determining the reputation of a system's node, taking into account a particular collection of considerations (all or subset of which we have already listed in this section) [42]. This credibility information can be processed and computed locally (at the edge) on a subset of nodes, based on various factors (node reputation, credibility score), thus outsourcing the credibility calculation to the edge.

Influence – A distributed system is positively affected by a well-established structure of action legitimacy (i.e. credibility) as it facilitates straightforward, mutual collaboration between devices and allows for more effective management functions. As a consequence, autonomous communication is permitted

– the establishment of communication channels between devices without prior knowledge of each other. When a system lacks metrics of the trustworthiness of its devices, components, or actions, the probability of negative consequences of its operation can be quite high. The system can not guarantee the well-being of its devices and users unless there are a comprehensive credibility evaluation and management framework in place. This can result in nodes being exposed to attacks and sensitive data theft that can be fatal in operation-critical systems (e.g. treatment control for patients suffering from cancer). Low system credibility can lead to a reduction in the quality and efficiency of decision-making processes. It can also harm the ability of the system to attract users and customers – users must trust the privacy and security of the ECP system.

Concerns – Concerns about violation and malformation of credibility in ECP systems can be observed at two aspects: hardware and software. At the hardware level, by tampering with peripherals, sensors, etc. the system can be led to provide false information feedback without knowing it. Many hardware-layer security risks can be triggered by the misbehavior of nodes that deviate from their usual actions, probably due to the malfunction of parts, various errors that trigger incorrect operation, etc. At the software level, credibility can be undermined by tampering with system functionalities, e.g. malicious code injection, identity theft, etc. The credibility of a device may be compromised by a 3rd party, external devices, or equipment. Such devices are referred to as malicious. They can impact the credibility of IoT systems on two layers: by disseminating malicious information or by performing malicious actions. This is often made possible by working under poorly secured internet access points. Malicious nodes affect basic system functionalities by violating the system's confidence in its nodes, and negatively impacting its credibility by attacks such as self-promoting, bad-mouthing, and good-mouthing [42]. Finally, in ECP systems there must always be in place a distributed (preferably autonomous and self-triggered) mechanism that performs regular device security and health checks.

Solutions – Although there is a need for a higher degree of reliability in some systems where trust is very important (e.g. patient support/care systems), other systems (e.g. home automation systems) might trade-off the complexity of safety and security procedures to improve the efficiency of their functionalities. In terms of credibility, we will address different hardware solutions, lightweight trust management, and computational frameworks and sacrifice and remote attestation approaches.

I GROUP – Credibility roots must be established starting from a hardware level that gives the system credibility, e.g. by the use of hardware performance counters (HPCs). HPCs are present in all commodity processors and can be used to detect firmware tampering [76], kernel control-flow modifying rootkits [75], etc. Also, if a sensor is tampered with to report false data at the hardware level, this issue can be solved using PUFs-Physical Unclonable Functions [52]. *This is a good method for addressing anti-hardware* *tampering from an ECP point of view that also recognizes firmware and software tampering. Since all devices implement HPCs, it is a good security technique to begin with.*

Sacrifice attacks present another scheme for misbehavior identification based on an honest majority and are referred to as the STING algorithm [40]. The purpose of this strategy is to make the risk of potential involvement expensive, to deter false claims, i.e.: if one node suspects that another node might have been compromised, it will send a warning that will bar both of them from the network. *The STING algorithm is successful in quickly expelling the misbehaving nodes, but at the expense of expelling the node that detected it as well. While authors argue that false allegations and misbehavior may be prevented, some ECP systems are unable to overcome these high-risk involvement constraints, especially in critical systems.*

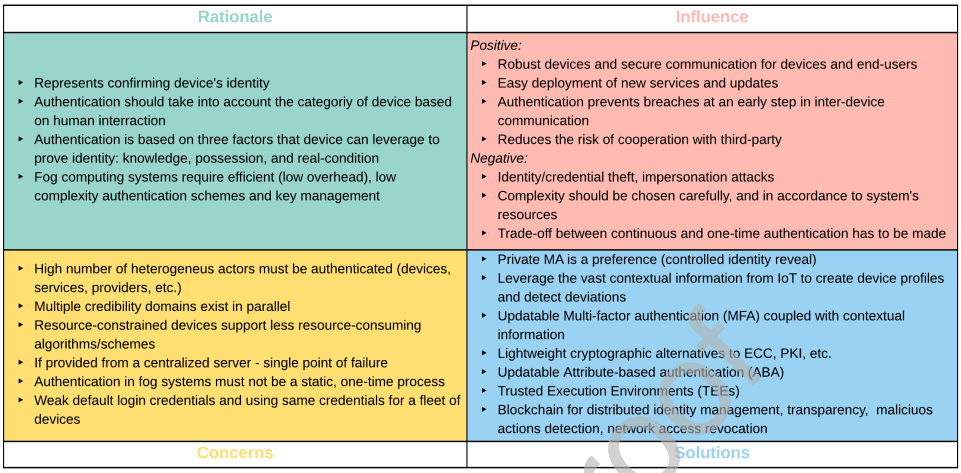
II GROUP – Credibility and Distributed Trust-Management Frameworks are relevant in edge systems and must have the means to audit, grant, and revoke trust in near-real-time [40]. Guo et al. provided a comprehensive survey of current trust-computing techniques in service-oriented IoT, classifying them into five aspects: trust composition, trust propagation, trust update, trust formation, and trust aggregation [15]. *This paper is relevant to the topic of our paper: (1) it summarizes the pros and cons of each aspect's and highlights the efficacy of the security mechanisms against malicious attacks; (2) it summarizes the most, and least-visited trust-computation techniques in the literature and offers insight into their efficacy and application to IoT systems; (3) it identifies gaps in IoT trust-computation research.*

Razouk et al. proposed a middleware-based architecture for protecting an ECP system where IoT-constrained devices communicate through a middleware agent. The agent can get access to more computing resources to improve secure communications, if necessary, and makes decisions when that is necessary [49]. *Middleware-based systems are as trustworthy as the middleware used in the credibility decision-making process. By dynamically assigning network credibility, as well as security strictness, ECP systems are more reliable and scalable.*

Credibility can be checked and audited with a remote-attestation approach. Two major classes of remote-attestation techniques can be distinguished: hardware-based (heavyweight), and software-based (lightweight). There are several hybrid schemes between these two classes, e.g. the TCM-RAA (Trusted Cryptographic Module-based Remote Anonymous Attestation) [8]. *Remote attestation can appear in three forms: centralized; semi-decentralized, when a subset of all nodes handles attestation; and completely decentralized. A semi-to fully decentralized solution is ideal for ECP systems. It is the consequence of the fact that in some environments there are many nodes unable to take part in the attestation.*

3.2. Authentication

This section explains the application of RICS on the authentication principle of CAAVI. The Authentication principle of the CAAVI model has been



Rationale	Influence
- Represents confirming device's identity - Authentication should take into account the categoriy of device based on human interraction - Authentication is based on three factors that device can leverage to prove identity: knowledge, possession, and real-condition - Fog computing systems require efficient (low overhead), low complexity authentication schemes and key management	*Positive:* - Robust devices and secure communication for devices and end-users - Easy deployment of new services and updates - Authentication prevents breaches at an early step in inter-device communication - Reduces the risk of cooperation with third-party *Negative:* - Identity/credential theft, impersonation attacks - Complexity should be chosen carefully, and in accordance to system's resources - Trade-off between continuous and one-time authentication has to be made
- High number of heterogeneous actors must be authenticated (devices, services, providers, etc.) - Multiple credibility domains exist in parallel - Resource-constrained devices support less resource-consuming algorithms/schemes - If provided from a centralized server - single point of failure - Authentication in fog systems must not be a static, one-time process - Weak default login credentials and using same credentials for a fleet of devices	- Private MA is a preference (controlled identity reveal) - Leverage the vast contextual information from IoT to create device profiles and detect deviations - Updatable Multi-factor authentication (MFA) coupled with contextual information - Lightweight cryptographic alternatives to ECC, PKI, etc. - Updatable Attribute-based authentication (ABA) - Trusted Execution Environments (TEEs) - Blockchain for distributed identity management, transparency, maliciuos actions detection, network access revocation
Concerns	Solutions

Figure 2: Authentication summary.

presented in detail in our paper [48]. The summary of the results of RICS applied to the authentication principle is given in Figure 2.

Rationale – ECP systems must distinguish between two authentication steps: (1) identification and (2) authentication. Identification provides a node‘s identity to the security system. For rights and permissions to be given, a node must provide proof of its identity to the system. The method of determining the claimed identity of the node by verifying the evidence provided is called authentication and the evidence provided is called an authentication credential. There are three key pieces of information that authentication schemes are typically based on, and that are expected from the nodes: knowledge, possession, and condition [19]. Knowledge refers to something known to the node (e.g. password, PIN), possession refers to something owned (e.g. certificate) and condition refers to something issued (e.g. MAC address, serial ID). According to Shahzad et al., there are two distinct types of IoT devices that humans communicate with, so different authentication approaches must be considered [60]. There are devices, such as insulin pumps, that maintain continuous physical contact with the user and devices that do not (e.g. household appliances). The use of continuous human-computer interaction in authentication approaches is highly important.

Influence – Authentication is regarded as a critical security concern for ECP systems [65]. Proper authentication enables more robust devices and secure communication for system components and end-users. Deployment of new services and updates to existing systems can be effortless if the devices are already authenticated. Authenticated devices can be used to distribute commands, firmware, and software updates to other devices while performing system authentication in parallel. Data breaches are avoided by removing unauthenticated users and activities, whilst the anti-tampering capabilities of the network are improved. Fragile authentication schemes, on the other hand, can lead to identity/credential theft or impersonation attacks. The effect of the use of complex authentication schemes depends on various criteria and requested level of data and actions sensitivity and security. Complex mechanisms provide stronger security, but they induce lower system performance and higher network latency. Based on how robust authentication is, the level of decision-making is often affected.

Concerns – In an ECP environment, multiple actors and infrastructures collaborate through an ecosystem where multiple domains of credibility coexist. Unlike most enterprise networks where authentication processes require a person entering a credential, many IoT/ECP authentication scenarios (e.g. embedded sensors) are M2M-based. On one hand, the human error coefficient is minimized while, on the other hand, M2M authentication has to be strong. Non-existent or weak authentication mechanisms may be used by an attacker to access data or to execute an operation by impersonating a real user, potentially leading to a disastrous outcome (i.e. the reset of an insulin pump). Usually, IoT devices go through a one-time authentication process, making them a perfect source of penetration into private enterprise networks. Furthermore, many consumer IoT devices are still being dispatched with weak default login credentials (such as "admin/admin") that many end-users do not update. Many service advertisements are not authenticated in today's IoT systems, thereby allowing malicious devices to easily spoof service broadcasts [15]. The situation can be leveraged to extract data from users, overwhelm the system with junk data that triggers Denial-of-Service (DoS), etc. When a remote authentication scheme is in operation, the network latency must be accounted for. Besides, a device needs to have reliable attributes, i.e. sufficient proof of its identity, without contacting a central server. Furthermore, most IoT applications lack conventional user interfaces (keyboards, touchscreen). Consequently, the lack of easily accessible interfaces raises two critical security issues: (1) How are IoT users/devices authenticated when there are no standardized, easily accessible methods? (2) How to provide continuous authentication for users/devices with non-typical interfaces?

Solutions – Authentication schemes are evolving from single to multi-authentication, peer-to-peer solutions are available, and the importance of developing authentication schemes and algorithms to meet the abundance of contextual information (physical and logical context of system operation) is recognized. The remainder of the section will discuss such security strategies for ECP systems.

I GROUP – Unlike single-factor authentication (SFA), multi-factor authentication (MFA) has become increasingly common and essential [35]. *MFA is superior to SFA in ECP systems. As edge devices function in a certain context (physical, logical), environmental information can be used to create a multi-factor credential that is unique to each device. Not only does it satisfy*

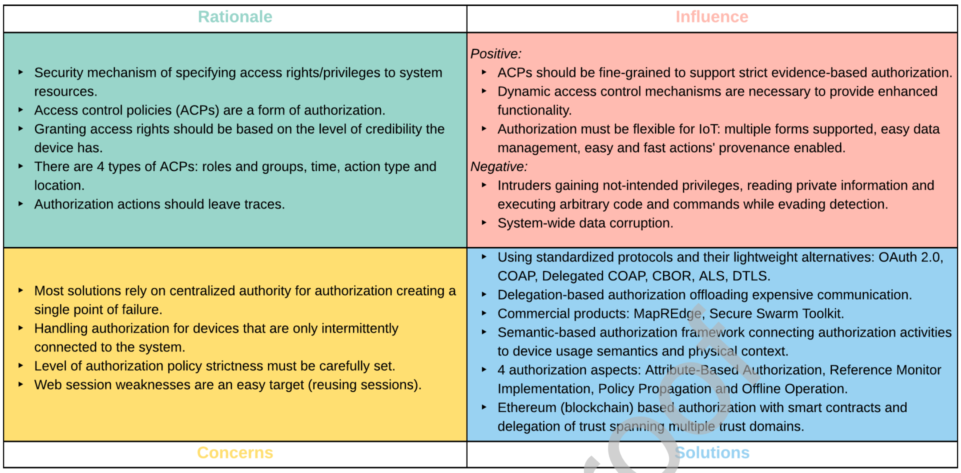
MFA, but it can also be changed regularly, always using contextual information, to provide a more reliable authentication framework. To create a context-based authentication framework, devices, sensors, node/user habits, and data must be observed. *User-worn devices should frequently authenticate the legitimacy of users themselves, before authorizing them to act.* Nevertheless, it is more difficult to develop authentication schemes for devices that seldom or never communicate with human users. Shahzad et al. suggest a Radio Frequency-based approach that uses information about how wireless signals change in the environment (channel state information-CSI and received signal strength-RSS) depending on user behavior (e.g. movement) to perform authentication [60]. *Users/devices can be correlated with normal behavioral trends by analyzing wireless signal metrics, while their behavioral anomalies can also be identified. Light can also be leveraged in this manner, enabling light-based authentication. Contextual data can be used to create machine-learning models that would be able to tell whether the current usage pattern indicates that the system or user should be re-authenticated.* Hardware-related approaches using Trusted Execution Environments (TEEs) in MFA are described by Rijswijk-Deij et al. [50]. Marforio et al. suggested using smartphones as TEE in the form of secure location authentication tokens to fix the issue of fraudulent purchases at points of sale made with fake or duplicated payment cards [36]. *TEEs present a good option for systems with compatible hardware many IoT deployments use common devices (simple ARM processing boards, wireless sensors, etc.) that are not pre-equipped with special TEEs.*

IoT and ECP are here to stay in the 5G era and beyond, and developing lightweight cryptographic schemes suitable for this kind of deployments remain a research challenge. Wu et al. offer a lightweight and efficient authentication and key agreement scheme for multi-gateway wireless sensor networks with a focus on IoT/ECP deployments and low-constraint devices [78]. Similarly, Li et al. propose a lightweight MFA protocol based on public-key encryption [30]. The authentication approach proposed by Ye et al. uses a lightweight encryption mechanism by defining attribute-based authentication, improving MFA between user and system nodes [80]. Shivraj et al. leverage the lightweight identity-based Elliptic Curve Cryptography (ECC) scheme and Lamport's OTP algorithm to construct a novel authentication scheme for IoT [61]. *Lightweight cryptographic schemes are required and should adopt implementation strategies that are compatible with low-constraint devices. More importantly, not all devices have to perform all the calculations (e.g. low-constraint nodes can perform only symmetric cryptography operations).* Attribute-based authentication (ABA) is a concept developed by referring to two subjects: attribute-based cryptography (ABC) and attribute-based encryption (ABE). ABC ensures the fine-grained regulation of access control. ABE is a one-to-many cryptography technique that defines identity not as atomic but as a collection of attributes (e.g. roles, private device-specific data, location, etc.). Stojmenovic et al. proposed a possible solution by embracing the idea of stand-alone authentication (SAA) and providing it with ABE for its protection in distributed information systems [65]. *ABA, ABE, and its variations are critical for ECP systems and can be easily implemented for the same purpose as MFA–the richness of contextual information.*

II GROUP – The privacy-preserving MFA architecture is proposed by Liu et al. Passwords are combined with user activity profiles to provide authentication credentials and fuzzy hashing and fully-homomorphic encryption are implemented to further secure user profiles [33]. Turkanović et al. suggest a low-complex user-authentication and key-agreement scheme for heterogeneous ad-hoc wireless sensor networks for resource-constrained architectures. The complexity of the calculations is minimized by using only simple hash and XOR computation [71]. Huang et al. propose a secure data access control framework for ECP systems based on CP-ABE and ABA signature schemes [18]. ABA is suggested by Dsouza et al. in a policy-driven security management framework, which demonstrates that near-real-time policy compliance can be implemented into an ECP system inducing a minor delay in communication [11].

OCTOPUS allows mutual, M2M authentication while performing minimal hash invocations and symmetric key operations, making it ideal for ECP [21]. *Efficient mutual MFA schemes can be used for ECP architectures. Instead of computationally expensive public-key cryptography, symmetric-key cryptography should be used. This applies, in particular, to edge devices with restricted CPU power.* Since MFA is required for the IoT, a solution based on blockchain, a decentralized authentication scheme with multiple levels of authentication, is potentially a good solution. The digital ID of the device would be used to identify the device on the network and function as a digital watermark to follow all steps of the device's activity on the blockchain network (e.g. signing transactions). *The malicious transactions are identified immediately and the node is marked as untrusted. Blockchain can be used mainly to authenticate behavior rather than devices themselves.* Lei et al. suggest a blockchain framework to simplify distributed key-management in heterogeneous vehicular communication systems [29]. *While public blockchains like Ethereum are not suitable for IoT because of the hash calculations complexity in the Proof of Work algorithm for consensus establishment, private blockchain networks, i.e. one of the Hyperledger blockchain projects [73], for resource-richer ECP systems, may be used.*

Public-Key Infrastructure (PKI) is a well-established framework for authentication. With an emphasis on wide-area measurement systems in smart grids, Law et al. explored and presented a PKI-based solution involving multicast authentication for IoT [28]. He et al. present an enhanced PKI to protect smart grid wireless networks that effectively withstands DoS attacks [16]. It is used in vehicle networks [43], ZigBee networks [39], and blockchains [73]. *PKI can provide a full X.509 digital certificate for an ECP system, along*



Rationale	Influence
‣ Security mechanism of specifying access rights/privileges to system resources. ‣ Access control policies (ACPs) are a form of authorization. ‣ Granting access rights should be based on the level of credibility the device has. ‣ There are 4 types of ACPs: roles and groups, time, action type and location. ‣ Authorization actions should leave traces.	*Positive:* ‣ ACPs should be fine-grained to support strict evidence-based authorization. ‣ Dynamic access control mechanisms are necessary to provide enhanced functionality. ‣ Authorization must be flexible for IoT: multiple forms supported, easy data management, easy and fast actions' provenance enabled. *Negative:* ‣ Intruders gaining not-intended privileges, reading private information and executing arbitrary code and commands while evading detection. ‣ System-wide data corruption.
‣ Most solutions rely on centralized authority for authorization creating a single point of failure. ‣ Handling authorization for devices that are only intermittently connected to the system. ‣ Level of authorization policy strictness must be carefully set. ‣ Web session weaknesses are an easy target (reusing sessions).	‣ Using standardized protocols and their lightweight alternatives: OAuth 2.0, COAP, Delegated COAP, CBOR, ALS, DTLS. ‣ Delegation-based authorization offloading expensive communication. ‣ Commercial products: MapREdge, Secure Swarm Toolkit. ‣ Semantic-based authorization framework connecting authorization activities to device usage semantics and physical context. ‣ 4 authorization aspects: Attribute-Based Authorization, Reference Monitor Implementation, Policy Propagation and Offline Operation. ‣ Ethereum (blockchain) based authorization with smart contracts and delegation of trust spanning multiple trust domains.
Concerns	Solutions

Figure 3: Authorization summary.

with cryptographic keys life-cycle management functionalities, including generation, delivery, management, and revocation. Nonetheless, more challenging algorithms, such as ECC or Rivest-Shamir-Adleman (RSA), may induce a greater computational overhead.

3.3. Authorization

This section explains the application of RICS on the authorization principle of CAAVI. The authorization will be examined by discussing access control policies, dynamic access control, and leveraging contextual information for both. The summary of the results of RICS applied to the authorization principle is given in Figure 3.

Rationale – Authorization is a security mechanism of specifying access rights/privileges to system resources. Access control policies (ACPs) are a form of authorization and are used to determine user/client privileges or access levels related to different system resources. Authentication protects the system from uncharted malicious entities whereas authorization provides an authenticated device or user to safely access the systems services. The set of actions that an authenticated entity can perform is determined by ACPs. These policies have fine granularity when it comes to governing what an entity can/cannot do to an object, service, or resource. Granting access rights and roles to entities should be based on the level of credibility the device has in the system. There are several types of ACPs: roles and groups, time, action type, and location [55]. Roles refer to the type of the entity and are usually based on a function of the entity, while groups are used for organizing entities with the same type of access to resources and information. Temporal isolation is a mechanism that can be used in access control as well. Activity type refers to controlling what data is accessed during certain types of actions, also which commands can be used on the data. The physical/logical location of the entity can be leveraged to grant/restrict access to services. Authorization actions should leave traces for a tracing function to perform regular checks on whether the device is performing inside its privilege boundaries or is trying to elevate its privileges through malicious activities.

Influence – ACPs are appropriate when they are sufficiently fine-grained to support strict evidence-based authorization. In latency-relevant ECP use-cases, quick authorization brings efficiency in decision-making and resource access management. Furthermore, dynamic access control mechanisms provide greater value, enhanced functionality, and new levels of convenience and utility. For a positive impact, authorization needs to be flexible enough in IoT: multiple forms of access control must be supported; authorization data must have the potential to be easily migrated and aggregated; provenance must be enabled at all times. If access control is not applied properly or fails, intruders can compromise the security of the software by gaining not-intended privileges, reading private information, executing commands, etc. while evading detection. Errors in SCPs can be leveraged to cause system-wide data corruption. When access control checks are not applied consistently, users/devices can perform illegal activities leading to information exposure, DoS, arbitrary code execution, etc.

Concerns – Most existing authorization systems rely on a trusted central authority [63]. If the central authority is compromised, attackers can corrupt the authorization policies system-wide. Network unavailability, node, and link failure is an issue for many highly distributed systems. Authorization and access control should be able to provide a level of functionality even in case of network unavailability. Handling authorization for devices that are only intermittently connected to the underlying system could present a problem and should be handled carefully. Often, it is necessary to determine the required security levels for different parts of a system as some data flows or actions could require stricter authorization policies. Websites are sometimes used to provide an interface to edge devices and in some cases of mishandled authorization, they will permit access to sensitive content or functionality that should require increased access control. Web session weaknesses are an easy target – permitting an attacker to reuse old session credentials for authorization must be denied.

Solutions – Solutions will be presented through aspects such as the granularity of authorization, peer-level delegation, decentralized identity management, and blockchain-based solutions for enabling provenance for all of these aspects. Existing standards will be examined and their usage will be highlighted.

I GROUP – It is always relevant to be aware of existing standards. According to Seitz et al. a proper IoT authorization framework could be built on the following standards: OAuth 2.0, CoAP, CBOR, and ALS [58]. OAuth 2.0 is an industry-standard protocol for authorization. It is well-researched for distributed IoT systems. CoAP (Constrained Application Protocol) is designed for the needs of constrained devices. DTLS (Datagram TLS) capable CoAP devices will support RSA and Advanced Encryption Standard (AES) or ECC and AES. CBOR, the Concise Binary Object Representation, is a data format whose design goals include the possibility of serializing extremely small binary code and message size. Application Layer Security (ALS) can be used when TLS is insufficient. *By using CoAP over UDP and CBOR encoded messages, the energy required for transmitting or receiving messages is highly reduced, making it viable for battery operated/low energy IoT devices. This also addresses devices with a low amount of available memory – CoAP should be used instead of HTTP, Symmetric Key Cryptography instead of Public Key Cryptography, and CBOR instead of JSON.* The Internet Engineering Task Force (IETF) is working on a series of efforts under the umbrella of Authentication and Authorization for Constrained Environments (ACE) topic. Their proposal for Delegated CoAP specifies how resource-constrained nodes can delegate authorization tasks to less-constrained devices, thus limiting the hardware requirements of the security solution [59]. *ECP systems should leverage the security controls built into IoT protocols based on standards such as DTLS, CoAP, etc. This allows for interoperability in authorization activities between different vendors devices.*

Hummen et al. propose delegation-based authorization, focused on DTLS, specifically offloading the expensive DTLS connection establishment to a delegation server [20]. *By handing over the established security context to the constrained device, resource requirements of DTLS-protected communication for constrained devices is significantly reduced.* Xiao et al. created a hybrid authorization model spanning user-edge-cloud for fine-grained search and access authorization in ECP environments. They combined index encryption with searchability and data encryption with fine-grained access control ability in one authorization system [79].

As commercial products go, MapREdge is an industry-scale product offering to solve the challenge of porting authentication, authorization, and access control to edge IoT networks with limited bandwidth, supporting real-time processing and low-constraint devices [27]. The system uses several industry-grade protocols: POSIX, HBase, SQL, Apache Kafka, etc. Kim et al. propose SST (Secure Swarm Toolkit), an open-source toolkit for construction and deployment of an authorization service infrastructure for the IoT [25]. *To the best of our knowledge, this paper presents the first working implementation of an Internet-scale authorization infrastructure that covers heterogeneous security requirements from sensor nodes to safety-critical components, with automated, formal security analysis.*

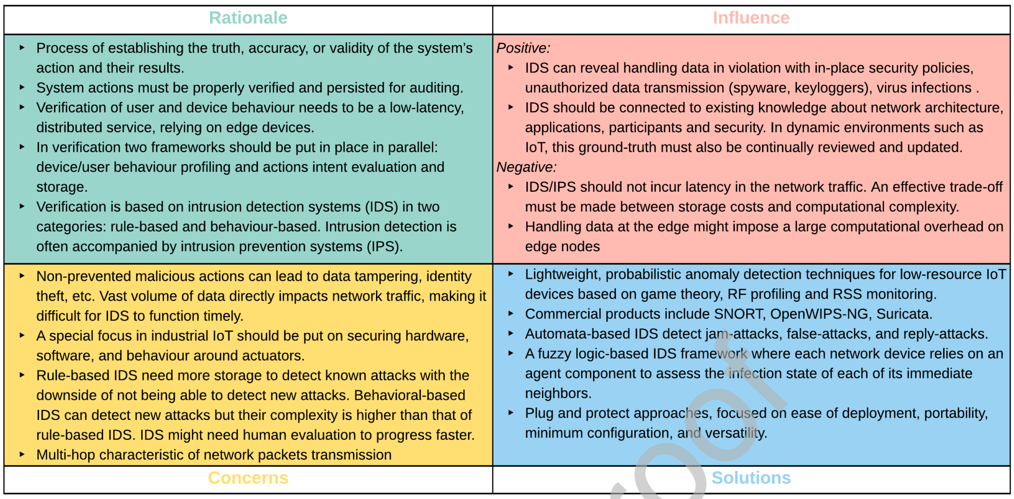
II GROUP – An authentication and authorization solution based on central identity storage of all devices is proposed by Trnka et al. [68]. It is built on top of the current web standards: OpenID Connect, OAuth and JSON Web Token. *Although secure and based on well-established protocols, this is still a remote authorization solution.* Tian et al. propose a user-centered, semantic-based authorization framework for IoT. The approach is based on linking a devices context (e.g. bathroom humidity sensor) to an activitys semantics (e.g. showering) using natural language processing and leveraging that information for authorization [67]. *Compliant to the ECP paradigm, authorization decisions relating to a device are based on local device data. The proposed framework supports fine-grained and flexible access control to constrained devices.* On behalf of structured frameworks, Salonikias et al. presented 4 aspects for a proper authorization framework: Attribute-Based Authorization, Reference Monitor Implementation (distributed reference monitor based on attribute-based access control – ABAC), Policy Propagation (all policy changes are in near real-time propagated to the entire system) and Offline Operation (access control system backup) [54]. *These four aspects underline key features of authorization frameworks.*

Blockchain solutions can be leveraged for authorization. For example, WAVE, a novel decentralized authorization system for IoT uses the Ethereum platform and smart contracts. It is presented by Andersen et al. with significant benchmark tests run on an experimental setup with more than 150 IoT devices [3]. Smart contracts are embedded with the Delegation of Trust mechanism that helps create a global permission graph that spans different trust domains ("work", "home"), where permission delegation can be easily tracked and audited. Each user has unique identity characteristics for signing transactions for every administrative domain. *Alongside identity and trust management, blockchains can also be suitable to audit authorization operations and inspect how access control is performed.*

3.4. Verification

This section explains the application of RICS on the verification principle of CAAVI. Verification will be examined by discussing device/user behavior profiling and actions intent evaluation and storage. The summary of the results of RICS applied to the verification principle is given in Figure 4.

Rationale – Verification is the process of establishing the truth, accuracy, or validity of the system actions and their results. After already considering CAA (Credibility, Authentication, and Authorization) security layers, the fourth layer, verification, must further minimize the probability of a malicious action in the system through rigorous analysis of current system-wide devices' behaviour. All system actions must be properly verified and are remembered for both internal and external audits. Verification of user and device behaviour through consecutive observation is essential for an ECP platform and it needs to be a low-latency, distributed service, relying on edge devices. For complex tasks in action evaluation and action intent prediction, computationally heavier approaches can be put in place, and their computing effort can be shared between resource-richer devices. In verification, two frameworks should be put in place in parallel: device/user behaviour profiling and actions intent evaluation and storage. When discussing verification, our focus will be on intrusion detection approaches falling into two categories: rule-based and behaviour-based intrusion detection systems



Rationale

- Process of establishing the truth, accuracy, or validity of the system's action and their results.
- System actions must be properly verified and persisted for auditing.
- Verification of user and device behaviour needs to be a low-latency, distributed service, relying on edge devices.
- In verification two frameworks should be put in place in parallel: device/user behaviour profiling and actions intent evaluation and storage.
- Verification is based on intrusion detection systems (IDS) in two categories: rule-based and behaviour-based. Intrusion detection is often accompanied by intrusion prevention systems (IPS).

Influence

Positive:

- IDS can reveal handling data in violation with in-place security policies, unauthorized data transmission (spyware, keyloggers), virus infections .
- IDS should be connected to existing knowledge about network architecture, applications, participants and security. In dynamic environments such as IoT, this ground-truth must also be continually reviewed and updated.

Negative:

- IDS/IPS should not incur latency in the network traffic. An effective trade-off must be made between storage costs and computational complexity.
- Handling data at the edge might impose a large computational overhead on edge nodes

- Non-prevented malicious actions can lead to data tampering, identity theft, etc. Vast volume of data directly impacts network traffic, making it difficult for IDS to function timely.
- A special focus in industrial IoT should be put on securing hardware, software, and behaviour around actuators.
- Rule-based IDS need more storage to detect known attacks with the downside of not being able to detect new attacks. Behavioral-based IDS can detect new attacks but their complexity is higher than that of rule-based IDS. IDS might need human evaluation to progress faster.
- Multi-hop characteristic of network packets transmission

Concerns

- Lightweight, probabilistic anomaly detection techniques for low-resource IoT devices based on game theory, RF profiling and RSS monitoring.
- Commercial products include SNORT, OpenWIPS-NG, Suricata.
- Automata-based IDS detect jam-attacks, false-attacks, and reply-attacks.
- A fuzzy logic-based IDS framework where each network device relies on an agent component to assess the infection state of each of its immediate neighbors.
- Plug and protect approaches, focused on ease of deployment, portability, minimum configuration, and versatility.

Solutions

Figure 4: Verification summary.

(IDS). Rule-based (signature-based) IDS rely on a well-established set of attack signatures to detect uncommon network and data access patterns, while the behavior-based IDS look for evidence of compromise rather than the attack itself. Deployment of IDS often includes the deployment of an Intrusion Prevention System (IPS) as well as [7]. An IPS is a software component that can prevent the attack from being successful. For IDS and IPS, M2M and human-computer interaction are important parts of verification for IoT systems where the semantics of actions should be leveraged to verify the intent/origin of the action.

Influence – IDS can reveal a big set of issues: handling data in violation with in-place security policies, unauthorized data transmission outside the network (spyware, keyloggers), viruses, trojans and malware infections that have gained control over systems internal resources, etc. Effects of IDS on the reliability of cyber-physical systems are influenced by both detection and response strength, and their correlation with attacker strength and detected behaviour. In IDS, these trade-offs have to be considered carefully because they will impact both the quality and the responsiveness of the IDS. Typically, an IDS is a passive system – it scans the network and marks any suspicious traffic. Fine-tuning IDS to the characteristics of the underlying network is an important part of its setup. The more elaborate the configurations, the more efficiently will the IDS operate. The IDS should be connected to existing knowledge about network architecture, applications, participants, and security. In dynamic environments such as IoT, this ground-truth must also be continually reviewed and updated. However, a major challenge for IDS/IPS service providers is that they should not incur latency in the network traffic. In ECP systems this is a particularly important challenge since IDS might have to run solely on edge nodes. Also, IDS/IPS has a large influence on storage management in the underlying system. An effective trade-off must be made between storage costs and computational complexity. If all data is handled on the edge level, while enhancing privacy, it might impose a large computational overhead on edge nodes, resulting in a negative impact on the system's quality of service.

Concerns – Non-prevented malicious actions can lead to data tampering, identity theft, etc. Actuator exploitation has not been mentioned so far, however, to exploit an actuator is maybe the most important security concern for an industrial IoT system since they are the connectors in the cyber-physical world. A special focus of IDS, in industrial IoT, should be put on securing hardware, software, and behaviour around actuators. In industrial IoT, the vast volume of data directly impacts network traffic, making it difficult for IDS to function timely. Storage costs are important for ECP devices as well. Rule-based IDS require more storage to detect known attacks with the downside of not being able to detect new attacks. Behavioral-based IDS can detect new attacks but their computational complexity is higher than that of rule-based IDS. The type of IDS must, thus, be chosen carefully, and trade-offs in storage/computation must be included in the decision. By leveraging cloud-based architectures, an IDS can reduce its workload by offloading expensive operations to higher-level computing infrastructures.

In the ECP ecosystem, the underlying system implementing the IDS might not be able to provide a good data analytics response rate, due to lower computational capabilities. Good task-delegation frameworks should exist to answer to this concern when complex IDS are put in place. Also, IDS might need human evaluation to progress faster. Additionally, in traditional network systems, there are specific nodes in charge of forwarding network packets from source to destination. The multi-hop characteristic of network packets transmission introduced with IoT makes it heavier to protect against network attacks. Edge devices (e.g. sensors) usually do not directly connect to a router, but rather to other edge nodes. This kind of network communication architecture, as well as non-standardized network communication protocols using poses a unique challenge to the efficiency of IDSs.

Solutions – Verification solutions are discussed from the standpoint of IDS and IPS approaches. Lightweight anomaly detection approaches powered by various machine-learning algorithms are explored, together with network traffic real-time analysis and profiling, outsourcing IDS, and pluggable solutions.

I GROUP – Sedjelmaci et al. presented a lightweight, probabilistic anomaly detection technique for low-resource IoT devices [57]. To make a balance between accuracy detection and energy consumption, a game theory approach is used to activate the IDS only when a new attack signature is expected to happen. Roux et al. proposed a neural network-based IDS that works with RF profiling and RSS monitoring and can detect attacks by noticing deviations from legitimate communication behavior [53]. Hodo et al. also proposed a neural network-based IDS trained on internet packet traces to detect known DDoS and DoS attacks demonstrating 99.4% accuracy [17].

An extensive machine-learning-based review of existing IDSs is performed by Tsai et al. [69].

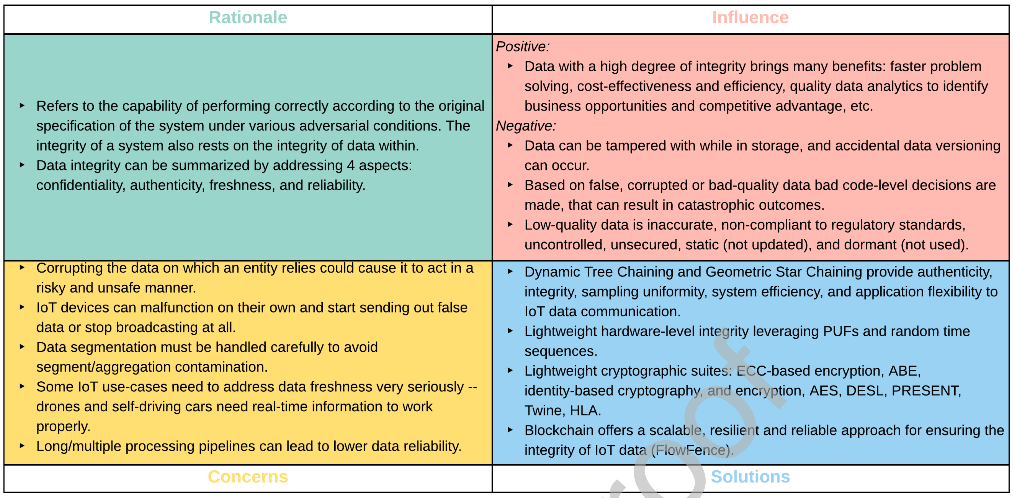
Commercial IDS and IPS solutions are not lacking. SNORT is a lightweight IDS capable of performing real-time traffic analysis and packet logging [51]. Security Onion is a Linux-based IDS used for network monitoring and intrusion detection [6]. OpenWIPS-NG [1] and Suricata [77] are both lightweight IDS/IPS with additional task-delegation extension frameworks included.

II GROUP – Distributed IDS architectures are most commonly set up as an environment where a subset of network is monitoring other nodes, referred to as the "watchdog" method. Misra et al. present an automata-based IDS for IoT that can detect three types of attacks automatically: jam-attack, false-attack, and reply-attack [38]. Sedjelmaci et al. based a distributed IDS on the fact that nodes in the same localities/clusters will behave alike [56]. A fuzzy logic-based IDS framework is proposed by Hendaoui et al. where each network device relies on an agent component to assess the infection state of each of its immediate neighbors. An IDS architecture evaluated on Raspberry Pis running SNORT [51] is presented by Sforzin et al. Authors coined the term Plug and protect, and focused their work on ease of deployment, portability, minimum configuration, and versatility. ProvThings is also a Plug and protects approach [74]. It is positively effective for 26 known IoT attacks. It imposes only 5% network latency and requires only 260 KB of storage to run. *Watchdog method offers an approach to scale the IDS to an ECP system and leveraging contextual information is welcome. Pluggable components and those supporting outsourcing of tasks are viable for ECP.*

3.5. Integrity

This section explores the application of RICS on the integrity principle of CAAVI. Integrity will be examined by discussing system performance according to requirements specification and data integrity. The summary of the results of RICS applied to the integrity principle is given in Figure 5.

Rationale – The integrity of a system refers to the capability of performing correctly according to the original specification of the system under various adversarial conditions. The integrity of a system also rests on the integrity of data within. The integrity of data is unspoiled when data has not been maliciously changed in storage or during transit. Data in IoT can be categorized depending on the type at the highest level to streaming, time-variant data, and event-based data [70]. In IoT, the presence of heterogeneous consumer data like personal information, health data, geographical data with various sensitivity levels calls for secure and scalable transport and storage mechanisms. Data can refer to either information that is entered into a system (through a device, user, 3rd party, etc.) or information created as a result of processing. Data integrity can be summarized through addressing 4 aspects: (1) confidentiality, (2) authenticity, (3) freshness, and (4) reliability. Data confidentiality (1) refers to protecting information from being accessed by unauthorized parties. Confidentiality can also refer to data encryption



Rationale	Influence
‣ Refers to the capability of performing correctly according to the original specification of the system under various adversarial conditions. The integrity of a system also rests on the integrity of data within. ‣ Data integrity can be summarized by addressing 4 aspects: confidentiality, authenticity, freshness, and reliability.	*Positive:* ‣ Data with a high degree of integrity brings many benefits: faster problem solving, cost-effectiveness and efficiency, quality data analytics to identify business opportunities and competitive advantage, etc. *Negative:* ‣ Data can be tampered with while in storage, and accidental data versioning can occur. ‣ Based on false, corrupted or bad-quality data bad code-level decisions are made, that can result in catastrophic outcomes. ‣ Low-quality data is inaccurate, non-compliant to regulatory standards, uncontrolled, unsecured, static (not updated), and dormant (not used).
‣ Corrupting the data on which an entity relies could cause it to act in a risky and unsafe manner. ‣ IoT devices can malfunction on their own and start sending out false data or stop broadcasting at all. ‣ Data segmentation must be handled carefully to avoid segment/aggregation contamination. ‣ Some IoT use-cases need to address data freshness very seriously -- drones and self-driving cars need real-time information to work properly. ‣ Long/multiple processing pipelines can lead to lower data reliability.	‣ Dynamic Tree Chaining and Geometric Star Chaining provide authenticity, integrity, sampling uniformity, system efficiency, and application flexibility to IoT data communication. ‣ Lightweight hardware-level integrity leveraging PUFs and random time sequences. ‣ Lightweight cryptographic suites: ECC-based encryption, ABE, identity-based cryptography, and encryption, AES, DESL, PRESENT, Twine, HLA. ‣ Blockchain offers a scalable, resilient and reliable approach for ensuring the integrity of IoT data (FlowFence).
Concerns	Solutions

Figure 5: Integrity summary.

that prevents access to information to unauthorized entities. Data is considered authentic (2) if it can be proved that it has not been corrupted after its creation or allowed modifications. Data freshness (3) implies that the data is recent. Data reliability (4) is a state that exists when data is sufficiently complete and error-free to be plausible for its purpose and context. Data is considered reliable when it is: complete, accurate, and unaltered [70].

Influence – By 2022, IoT data are expected to constitute 45% traffic in the Internet [22]. Considering that, data in IoT must aim to be error-prone while platforms maintain confidentiality, authenticity, freshness, and reliability. When organizations have confidence in their data integrity, they tend to leverage data more for fueling good business decisions. Data with a high degree of integrity brings many benefits: faster problem solving, cost-effectiveness and efficiency, quality data analytics to identify business opportunities and competitive advantage, etc. Devices at the edge can store and exchange data independently of remote services and that allows for on-demand, actionable, and near-real-time data management. However, data can be tampered with while in storage. Data versioning is a probable side effect of data that is either changed on purpose or has been tampered with. In an IoT/edge system, situations might happen (e.g. network latency) that result in different nodes having access to different versions of data. When acted upon, the same actions from different devices can have different results. A proper data versioning framework should consider extreme use-cases. Based on false, corrupted, or bad-quality data, bad code-level decisions could be made, that can result in catastrophic outcomes. Low-quality data comes in many different forms: inaccurate, non-compliant to regulatory standards, uncontrolled, unsecured, static (not updated), and dormant (not used). Millions of sensors and streams of data drive us towards disregarding the typical data storage policies – in todays IoT systems often only actionable data can be kept while the rest is offloaded and disregarded. Even with the vast number of storage options, keeping all data can result in network bandwidth overflow or latency in data access.

Concerns – In ECP systems, data the devices are generating, processing, sending, and receiving needs protection. ECP brings a new paradigm for computational loading and distributed IoT security. Compromising data integrity is worse than data theft since corrupting the data on which an entity relies could cause it to act in a risky and unsafe manner. IoT devices can malfunction on their own and start sending out faulty data or even stop broadcasting at all. Some low-constraint edge devices might not be able to process large datasets in near-real-time. Instead, services might have to send the data to such devices in a segmented/chunked form, and if one segment is compromised that can lead the device to make a wrong decision. In IoT, it is important that data aggregation schemes reduce power consumption, avoid traffic congestion, and maximize data usability. If one data source in the aggregated data consists of tampered-data, the whole aggregation can be marked as unusable. For IoT systems, it is not only needed to transmit data quickly, but data also needs to be fresh. Some IoT use-cases need to address data freshness very seriously – drones and self-driving cars need real-time information to work properly. Additionally, when processing at the edge level, we can leverage the situation of having fewer stations in the pipeline of data processing. Long and multiple processing pipelines can lead to lower data reliability. Lastly, the clustering of sensors and edge devices can have both advantages and concerns.

Solutions – Presented solutions are focused on data integrity, lightweight encryption and decryption schemes, ABE variants, lightweight existing cryptography algorithm alternatives, and blockchain-based frameworks.

I GROUP – Li et al. have proposed two solutions based on Digital signatures – Dynamic Tree Chaining (DTC) and Geometric Star Chaining (GSC) that provide authenticity, integrity, sampling uniformity, system efficiency, and application flexibility to IoT data communication [31]. *DTC is an extension of Merkle trees, while the GSC is a novice digital signature method, that outperforms DTC in IoT systems.* Aman et al. presented an approach for lightweight data integrity assurance for IoT leveraging PUFs, random time sequences, and aggregation for data integrity in IoT systems, to detect data tampering [2].

Because of resource limitations of IoT/ECP networks and evolving nature of cyber-security, the traditional cryptographic mechanisms such as RSA fail to support many resource-constrained devices in ECP. Thus, investigating lightweight cryptographic suites is of great importance, which is why Diro et al. proposed a lightweight encryption scheme for edge level communication based on ECC. *With extensive experiments, the authors show that the encryption and decryption of multiple message sizes using proxy ECC are faster than its RSA mechanism.* Also, ABE reconsiders the concept of public-key cryptography (PKC) where a message is encrypted for a specific receiver with its public key. A feasible alternative is using identity-based cryptography and identity-based encryption [23], where the public key can be a unique device attribute, such as the MAC address of the receiver. IBE is an important primitive of ID-based cryptography, more flexible and scalable than regular PKC [14].

Other advanced lightweight encryption algorithms for IoT devices are extensively discussed [62]. The authors explain different primitives of lightweight cryptographic algorithms and summarize them based on the key size, block length, number of rounds, and structures (such as AES, DESL, PRESENT, Twine, etc.). Symmetric (e.g. AES, HIGHT, etc.) as well as asymmetric (e.g. RSA, ECC, etc.) lightweight algorithms for IoT are discussed with a focus on possible attacks. Authors also propose a novel Hybrid Lightweight Algorithm (HLA) as a combination of symmetric and asymmetric lightweight encryption algorithms for IoT systems [62]. *HLA aims to bring the best features of both types of algorithms to one hybrid approach with the ultimate aim to minimize computation time, consume less power, be fast and efficient.* An extremely lightweight encryption algorithm was proposed by Usman et al. where authors leveraged 64-bit block ciphers keys for data encryption [72]. The implementation was provided on a low-cost 8-bit microcontroller with an average 10 to 20 encryption rounds. Going further, Noura et al. propose a 1 round cipher algorithm for IoT devices, while maintaining a high level of randomness and security [44]. For more than a decade, many efforts have been spent to make AES into a lightweight block cipher, making it practical for resource-limited edge devices. There is an AES-128 bit hardware implementation with 2400 Gate Equivalents by Moradi et al. [41], and an efficient software AES-8 bit by Osvik et al. [45]. *It is safe to conclude that AES might not be suitable for the most resource-constrained devices but will perform very well on microprocessing boards such as Raspberry Pi. On the other hand, while analyzing the performance of cryptographic techniques, Matsemela et al. have shown that AES performs better in terms of speed and CPU usage than RSA [37].*

II GROUP – As a decentralized distributed ledger, blockchain offers a scalable, resilient and reliable approach for ensuring the integrity of IoT data. One such blockchain-based data integrity service/framework for IoT has been proposed by Liu et al. [32]. In a case study of a smart home use-case, blockchain for IoT security and data privacy has been proposed by Dorri et al. [10]. *With public blockchains, it is necessary to consider the problem of whether they are capable of following the scaling rate of IoT data as well as privacy requirements. However, they require significant computational complexity that is not suitable for most resource-constrained IoT/ devices.* FlowFence protection framework protects sensitive data by asking entities to declare the permitted workflows on that data while undeclared workflows are immediately blocked [12]. *Although authors recognize the increase in software*

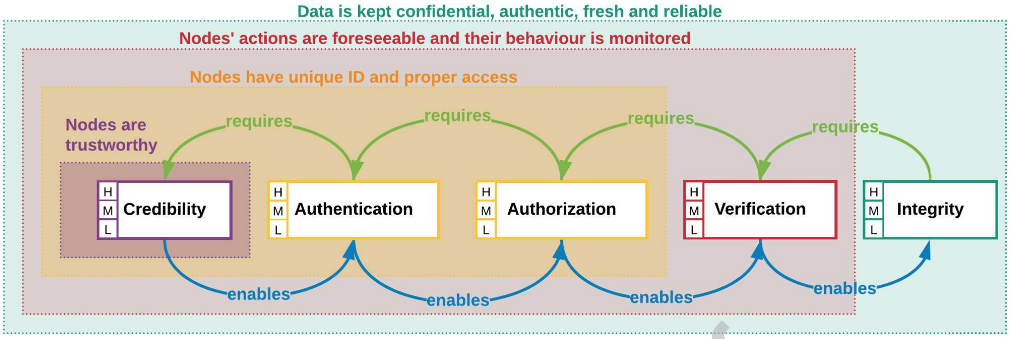


Figure 6: CAAVI principles bridging.

code size and a minor decrease in performance, it is relevant to consider this solution if data is highly sensitive. Regarding IoT/ECP, many authors agree that edge is more appropriate for handling data privacy and security than the cloud, for various use cases: health data [66], geo-spatial data [5], etc. *Distributed data intelligence is a concept that will gain importance in the upcoming years, for several reasons: network resource preservation, scalability, close control, clustering, and resilience.*

4. Bridging CAAVI Principles

The CAAVI principles – Credibility, Authentication, Authorization, Verification, and Integrity have been described in that particular order on purpose, as illustrated in Figure 6. Former principles enable the latter, and the latter requires the former. Nevertheless, engineering considerations for each principle need to be observed separately, and when integrating the principles the specified order should be followed. First, with engineering the mechanisms for ensuring Credibility, we ensure network and node trustworthiness which increases communication efficacy. By tackling Authentication and Authorization, we ensure that each node has unique, verifiable credentials for communicating, accessing data, and system actions. Engineering of the mechanisms behind Verification protects the system from internal misbehaviour and external malicious actions by ensuring system behaviour is foreseeable, consistent and constantly monitored. Lastly, data Integrity is obtained partly from correctly engineering CAAV principles, but also mechanisms at the Integrity layer themselves are assuring data safety, privacy, reliability, completeness, accuracy, and consistency. Designing and bridging CAAVI principles is critical to system security engineering, as the (in)correct design of a former principle significantly impacts the latter.

Furthermore, it is important to highlight that the level of security for each principle can be modeled separately. While for some systems and principles security needs to be tight and more complex, for other systems and principles it could be reduced. This heavily depends on the system and use-case description: criticalness, time sensitivity, and reactiveness requirements,

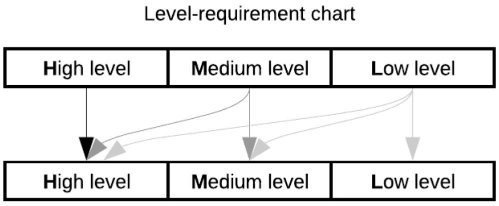


Figure 7: CAAVI levels requirement dependency chart.

data sensitivity and data/user/device privacy requirements, available computational resources, architectural and deployment approach, and the physical and logical operational contextual information availability. It is important to mention that a high level of security at one layer requires a high level of security at the former layer. Such relations are displayed in Figure 7. This was highlighted several times in the paper and illustrated with appropriate examples in Section 3. Lastly, solutions presented in this paper are compatible for adoption in not only IoT/ECP systems but other types of computer systems as well, as long as there is a need or requirement for a distributed security implementation for one of the principles.

5. Conclusion

The main contribution of our efforts is the introduction of a novel security review methodology that we call CAAVI-RICS. This novel review taxonomy aims to explain and discuss the foundational building blocks of an IoT/ECP computing system's security. The presented analysis and systematization framework is also suitable for people with a less technological background, who are interested in evaluating security challenges and deploying secure ECP systems. Besides, we provide an extensive overview of the security in ECP systems through systematic categorization resulting in discussion for more advanced and on-topic readers.

We argue that the CAAVI-RICS review methodology can be applied to modeling the security of all cyber-physical systems. It captures well the security aspects of the IoT/ECP systems through deliberating each of the CAAVI building blocks separately, and then also forces a thorough understanding of each of those building blocks through RICS. Hence, although our focus in this paper was set on IoT/ECP distributed systems, readers are also advised to apply the presented methodology to other real-world security problems. CAAVI-RICS can be applied wherever there is deep architectural knowledge about the system, its features, and expected behavior.

References

[1] Aircrack-NG, 2018. Openwips-ng. https://github.com/aircrack-ng.

[2] Aman, M. N., Sikdar, B., Chua, K. C., Ali, A., 2018. Low power data

integrity in IoT systems. IEEE Internet of Things Journal 5 (4), 3102–3113.

[3] Andersen, M. P., Kolb, J., Chen, K., Fierro, G., Culler, D. E., Popa, R. A., 2017. Wave: A decentralized authorization system for iot via blockchain smart contracts. EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2017-234.

[4] Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R., 2010. Proposed security model and threat taxonomy for the Internet of Things (IoT). In: International Conference on Network Security and Applications. Springer, pp. 420–429.

[5] Barik, R. K., Dubey, H., Samaddar, A. B., Gupta, R. D., Ray, P. K., 2016. Foggis: Fog computing for geospatial big data analytics. In: 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON). IEEE, pp. 613–618.

[6] Burks, D., 2012. Security onion. Securityonion. blogspot. com.

[7] Carter, E., Hogue, J., 2006. Intrusion prevention fundamentals. Pearson Education India.

[8] Chiang, M., Zhang, T., 2016. Fog and IoT: An overview of research opportunities. IEEE Internet of Things Journal 3 (6), 854–864.

[9] Cirani, S., Ferrari, G., Veltri, L., 2013. Enforcing security mechanisms in the ip-based internet of things: An algorithmic overview. Algorithms 6 (2), 197–226.

[10] Dorri, A., Kanhere, S. S., Jurdak, R., Gauravaram, P., 2017. Blockchain for IoT security and privacy: The case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, pp. 618–623.

[11] Dsouza, C., Ahn, G.-J., Taguinod, M., 2014. Policy-driven security management for fog computing: Preliminary framework and a case study. In: Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014). IEEE, pp. 16–23.

[12] Fernandes, E., Paupore, J., Rahmati, A., Simionato, D., Conti, M., Prakash, A., 2016. Flowfence: Practical data protection for emerging iot application frameworks. In: 25th {USENIX} Security Symposium ({USENIX} Security 16). pp. 531–548.

[13] Ganeriwal, S., Balzano, L. K., Srivastava, M. B., 2008. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN) 4 (3), 1–37.

[14] Güneysu, T., Oder, T., 2017. Towards lightweight identity-based encryption for the post-quantum-secure Internet of Things. In: 2017 18th International Symposium on Quality Electronic Design (ISQED). IEEE, pp. 319–324.

[15] Guo, J., Chen, R., Tsai, J. J., 2017. A survey of trust computation models for service management in internet of things systems. Computer Communications 97, 1–14.

[16] He, D., Chan, S., Zhang, Y., Guizani, M., Chen, C., Bu, J., 2014. An enhanced public key infrastructure to secure smart grid wireless communication networks. IEEE Network 28 (1), 10–16.

[17] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C., Atkinson, R., 2016. Threat analysis of IoT networks using artificial neural network intrusion detection system. In: 2016 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, pp. 1–6.

[18] Huang, Q., Yang, Y., Wang, L., 2017. Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. IEEE Access 5, 12941–12950.

[19] Huang, X., Xiang, Y., Chonka, A., Zhou, J., Deng, R. H., 2010. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems 22 (8), 1390–1397.

[20] Hummen, R., Shafagh, H., Raza, S., Voig, T., Wehrle, K., 2014. Delegation-based authentication and authorization for the ip-based Internet of Things. In: 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). Ieee, pp. 284–292.

[21] Ibrahim, M. H., 2016. Octopus: An edge-fog mutual authentication scheme. IJ Network Security 18 (6), 1089–1101.

[22] Index, C. G. C., 2018. Forecast and methodology, 2016–2021 white paper. Updated: February 1.

[23] Joye, M., Neven, G., 2009. Identity-based cryptography. Vol. 2. IOS press.

[24] Khan, S., Parkinson, S., Qin, Y., 2017. Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing 6 (1), 19.

[25] Kim, H., Kang, E., Lee, E. A., Broman, D., 2017. A toolkit for construction of authorization service infrastructure for the internet of things. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. pp. 147–158.

[26] Kumar, P., Zaidi, N., Choudhury, T., 2016. Fog computing: Common security issues and proposed countermeasures. In: 2016 International Conference System Modeling & Advancement in Research Trends (SMART). IEEE, pp. 311–315.

[27] Lalitha, B., et al., 2018. Recover the missing data in IoT by edge analytics. i-Manager's Journal on Software Engineering 13 (2), 25.

[28] Law, Y. W., Palaniswami, M., Kounga, G., Lo, A., 2013. Wake: Key management scheme for wide-area measurement systems in smart grid. IEEE Communications Magazine 51 (1), 34–41.

[29] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., Sun, Z., 2017. Blockchain-based dynamic key management for heterogeneous in-

telligent transportation systems. IEEE Internet of Things Journal 4 (6), 1832–1843.

[30] Li, N., Liu, D., Nepal, S., 2017. Lightweight mutual authentication for IoT and its applications. IEEE Transactions on Sustainable Computing 2 (4), 359–370.

[31] Li, X., Wang, H., Yu, Y., Qian, C., 2017. An IoT data communication framework for authenticity and integrity. In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, pp. 159–170.

[32] Liu, B., Yu, X. L., Chen, S., Xu, X., Zhu, L., 2017. Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services (ICWS). IEEE, pp. 468–475.

[33] Liu, W., Uluagac, A. S., Beyah, R., 2014. Maca: A privacy-preserving multi-factor cloud authentication system utilizing big data. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, pp. 518–523.

[34] Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I., 2015. Internet of things (IoT) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, pp. 336–341.

[35] Manzoor, A., Wahid, A., Shah, M. A., Akhunzada, A., Qureshi, F. F., 2018. Secure login using multi-tier authentication schemes in fog computing.

[36] Marforio, C., Karapanos, N., Soriente, C., Kostiainen, K., Capkun, S., 2014. Smartphones as practical and secure location verification tokens for payments. In: NDSS. Vol. 14. pp. 23–26.

[37] Matsemela, G., Rimer, S., Ouahada, K., Ndjiongue, R., Mngomezulu, Z., 2017. Internet of things data integrity. In: 2017 IST-Africa week conference (IST-Africa). IEEE, pp. 1–9.

[38] Misra, S., Abraham, K. I., Obaidat, M. S., Krishna, P. V., 2009. Laid: a learning automata-based scheme for intrusion detection in wireless sensor networks. Security and Communication Networks 2 (2), 105–115.

[39] Misra, S., Goswami, S., Taneja, C., Mukherjee, A., 2016. Design and implementation analysis of a public key infrastructure-enabled security framework for zigbee sensor networks. International Journal of Communication Systems 29 (13), 1992–2014.

[40] Moore, T., Raya, M., Clulow, J., Papadimitratos, P., Anderson, R., Hubaux, J.-P., 2008. Fast exclusion of errant devices from vehicular networks. In: 2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. IEEE, pp. 135–143.

[41] Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H., 2011. Pushing the limits: A very compact and a threshold implementation of aes.

In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 69–88.

[42] Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G., 2012. A subjective model for trustworthiness evaluation in the social internet of things. In: 2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC). IEEE, pp. 18–23.

[43] Noroozi, H., Khodaei, M., Papadimitratos, P., 2018. Vpkiaas: A highly-available and dynamically-scalable vehicular public-key infrastructure. In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, pp. 302–304.

[44] Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R., Mansour, M. M., 2018. One round cipher algorithm for multimedia IoT devices. Multimedia tools and applications 77 (14), 18383–18413.

[45] Osvik, D. A., Bos, J. W., Stefan, D., Canright, D., 2010. Fast software aes encryption. In: International Workshop on Fast Software Encryption. Springer, pp. 75–93.

[46] Pešić, S., Ivanović, M., Radovanović, M., Costin, B., Tošić, M., Iković, O., Bošković, D., 2019. CAAVI-RICS model for analyzing the security of fog computing systems. In: Proceedings of the 13th International Symposium on Intelligent Distributed Computing. Springer.

[47] Pešić, S., Radovanović, M., Ivanović, M., Badica, C., Tošić, M., Iković, O., Bošković, D., 2019. CAAVI-RICS model for analyzing the security of fog computing systems. In: International Symposium on Intelligent and Distributed Computing. Springer, pp. 23–34.

[48] Pesic, S., Radovanović, M., Ivanović, M., Badica, C., Tošić, M., Iković, O., Bošković, D., 2019. CAAVI-RICS model for analyzing the security of fog computing systems: Authentication. In: 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT). IEEE, pp. 226–231.

[49] Razouk, W., Sgandurra, D., Sakurai, K., 2017. A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. In: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. ACM, p. 35.

[50] Rijswijk-Deij, R. v., Poll, E., 2013. Using trusted execution environments in two-factor authentication: comparing approaches. Open Identity Summit 2013.

[51] Roesch, M., et al., 1999. Snort: Lightweight intrusion detection for networks. In: Lisa. Vol. 99. pp. 229–238.

[52] Rosenfeld, K., Gavas, E., Karri, R., 2010. Sensor physical unclonable functions. In: 2010 IEEE international symposium on hardware-oriented security and trust (HOST). IEEE, pp. 112–117.

[53] Roux, J., Alata, E., Auriol, G., Nicomette, V., Kaâniche, M., 2017. Toward an intrusion detection approach for IoT based on radio communications profiling. In: 2017 13th European Dependable Computing Conference (EDCC). IEEE, pp. 147–150.

[54] Salonikias, S., Mavridis, I., Gritzalis, D., 2015. Access control issues in utilizing fog computing for transport infrastructure. In: International Conference on Critical Information Infrastructures Security. Springer, pp. 15–26.

[55] Samarati, P., de Vimercati, S. C., 2000. Access control: Policies, models, and mechanisms. In: International School on Foundations of Security Analysis and Design. Springer, pp. 137–196.

[56] Sedjelmaci, H., Senouci, S. M., 2013. Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks. In: Global Information Infrastructure Symposium-GIIS 2013. IEEE, pp. 1–6.

[57] Sedjelmaci, H., Senouci, S. M., Al-Bahri, M., 2016. A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology. In: 2016 IEEE International Conference on Communications (ICC). IEEE, pp. 1–6.

[58] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., Tschofenig, H., 2015. Authorization for the Internet of Things using oauth 2.0. Internet Engineering Task Force (IETF): Fremont, CA, USA.

[59] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., Tschofenig, H., 2017. Authentication and authorization for constrained environments (ACE). Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07.

[60] Shahzad, M., Singh, M. P., 2017. Continuous authentication and authorization for the internet of things. IEEE Internet Computing 21 (2), 86–90.

[61] Shivraj, V., Rajan, M., Singh, M., Balamuralidhar, P., 2015. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In: 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW). IEEE, pp. 1–6.

[62] Singh, S., Sharma, P. K., Moon, S. Y., Park, J. H., 2017. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 1–18.

[63] Srivatsa, M., Liu, L., Iyengar, A., 2011. Eventguard: A system architecture for securing publish-subscribe networks. ACM Transactions on Computer Systems (TOCS) 29 (4), 1–40.

[64] Stojmenovic, I., Wen, S., 2014. The fog computing paradigm: Scenarios and security issues. In: 2014 federated conference on computer science and information systems. IEEE, pp. 1–8.

[65] Stojmenovic, I., Wen, S., Huang, X., Luan, H., 2016. An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience 28 (10), 2991–3005.

[66] Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., Halunga, S., Fratu, O., 2015. Big data, internet of things and cloud

convergence–an architecture for secure e-health applications. Journal of medical systems 39 (11), 141.

[67] Tian, Y., Zhang, N., Lin, Y.-H., Wang, X., Ur, B., Guo, X., Tague, P., 2017. Smartauth: User-centered authorization for the internet of things. In: 26th {USENIX} Security Symposium ({USENIX} Security 17). pp. 361–378.

[68] Trnka, M., Cerny, T., 2018. Authentication and authorization rules sharing for internet of things. Software Networking 2018 (1), 35–52.

[69] Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y., Lin, W.-Y., 2009. Intrusion detection by machine learning: A review. expert systems with applications 36 (10), 11994–12000.

[70] Tsai, C.-W., Lai, C.-F., Chiang, M.-C., Yang, L. T., 2013. Data mining for internet of things: A survey. IEEE Communications Surveys & Tutorials 16 (1), 77–97.

[71] Turkanović, M., Brumen, B., Hölbl, M., 2014. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks 20, 96–112.

[72] Usman, M., Ahmed, I., Aslam, M. I., Khan, S., Shah, U. A., 2017. Sit: a lightweight encryption algorithm for secure internet of things. arXiv preprint arXiv:1704.08688.

[73] Valenta, M., Sandner, P., 2017. Comparison of ethereum, hyperledger fabric and corda. [ebook] Frankfurt School, Blockchain Center.

[74] Wang, Q., Hassan, W. U., Bates, A., Gunter, C., 2018. Fear and logging in the Internet of Things. In: Network and Distributed Systems Symposium.

[75] Wang, X., Karri, R., 2016. Reusing hardware performance counters to detect and identify kernel control-flow modifying rootkits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 35 (3), 485–498.

[76] Wang, X., Konstantinou, C., Maniatakos, M., Karri, R., 2015. Confirm: Detecting firmware modifications in embedded systems using hardware performance counters. In: Proceedings of the IEEE/ACM international conference on computer-aided design. IEEE Press, pp. 544–551.

[77] Wong, K., Dillabaugh, C., Seddigh, N., Nandy, B., 2017. Enhancing suricata intrusion detection system for cyber security in scada networks. In: 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, pp. 1–5.

[78] Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K.-K. R., Wazid, M., Das, A. K., 2017. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications 89, 72–85.

[79] Xiao, M., Zhou, J., Liu, X., Jiang, M., 2017. A hybrid scheme for fine-grained search and access authorization in fog computing environment. Sensors 17 (6), 1423.

[80] Ye, N., Zhu, Y., Wang, R.-c., Malekian, R., Qiao-Min, L., 2014. An efficient authentication and access control scheme for perception layer of internet of things. Applied Mathematics & Information Sciences 8 (4), 1617.

[81] Yi, S., Qin, Z., Li, Q., 2015. Security and privacy issues of fog computing: A survey. In: International conference on wireless algorithms, systems, and applications. Springer, pp. 685–695.