Edge-assisted Intelligent Device Authentication in Cyber-Physical Systems

Yanrong Lu, Ding Wang, Mohammad S. Obaidat, *Fellow, IEEE*, and Pandi Vijayakumar, *Senior Member, IEEE*

***Abstract*—Cyber-Physical System (CPS) provides a foundation for the Industrial Internet of Things (IIoT) that interconnects all types of devices. The integration of CPS with IIoT generates the large volumes of data forcing the development of Artificial Intelligence (AI) to extract information more precisely. Nevertheless, the increasing volume/variety of data traffic and the ever-growing number of IIoT devices bring great challenges for the host-centric communication model of the current Internet. In this work, we present a novel Information-Centric Networking (ICN)-based system model in CPS, which enables processing data from IIoT devices closer to the edge as opposed to a content provider. Based on this ICN system model, we propose an edge-assisted authentication scheme in CPS, aiming to protect the system from unauthorized access and reduce workload for resource-constrained devices. The main features of our scheme include a delegation model of security operations and session handshake procedures through edge routers, addressing the rising challenges in managing and securing IIoT devices in the ICN. We formally prove the security of our scheme and conduct performance analysis to show its practicality.**

***Index Terms*—Authentication, Cyber-Physical System (CPS), Efficiency, Information Centric Networking (ICN), Industrial Internet of Things (IIoT), Security**

I. Introduction

Industrial 4.0 brings a communication and interconnectivity storm, enabling the intelligent manufacturing process to be more flexible, more advanced, and more smart by leveraging Artificial Intelligence (AI) [1]. AI makes it possible for industrial systems to focus more on data analytics automatically with acceptable quality of user experience. Based on such benefits, Industrial Internet of Things (IIoT) [2] together with Cyber-Physical System (CPS) as the kernel technologies for Industrial 4.0 provide a variety of advantages for manufacturing operations, industrial processes, and cooperative communication to refine high quality service and decrease framework overhead significantly [3]. Although the combination of AI-focused IIoT and CPS greatly increases efficiency in industrial systems, it still suffers from the issues of heavy burdensome, device incompatibility, security, and privacy [4]–[6].

A recent study predicted that multiple devices connected to the Internet will be over triple the global population by 2030 [7]. Such tremendous data traffic has posed severe challenges for resource-limited devices within the existing Internet architecture. With a surge in demand for bandwidth, Information-Centric Networking (ICN) architecture [8] induces an encouraging communication paradigm where the data detaches from the data source. This data-location-decoupling has wide applications in supporting high flexibility, such as the device-to-device data access [9]. As a typical IIoT example, industrial smart grid coupled with ICN, can enhance the resilience of information delivery against power failures and further minimize power distribution disruption. From this point of view, ICN is regarded as one of the best possible communication stacks for IIoT due to its significant advantage in eliminating transmission latency with in-network caching.

Despite the above-mentioned advantages, the deployment of ICN on CPS-based systems introduces several new challenges and authentication is the most challenging one [10]–[13]. Specifically, existing authentication strategies for CPS-over-IP networks embrace a two-party scheme that brings end-to-end trust between new joining devices and an authorization server [14], [15]. However, the unpredictability of data providers (e.g repositories) increases the difficulty in hampering false data injection attacks because of the in-network caching in ICN. The following requisition can be fulfilled by the routers lead to aggressors purporting to be honest individuals to get access and control the system in parallel. In addition, content nodes may easily identify current users and try to pry the privacy of them further. Motivated by such observation, IIoT devices and routers are obliged to check the data authenticity before fetching or storing them whereas the devices' identifications are required to be shielded. Thus, it is essential to seek to address those challenges with a single solution by leveraging the existing security mechanism.

The accessibility of ICN routers permits us to endorse an edge-assisted approach at the *entry* and *exit* routers in the framework. Moreover, IIoT applications allow small, low-cost intelligent devices at the edge to collect data. Along these lines, considering a delegation model to the IIoT is a native approach to decrease the huge pressure on such devices. Proxy signature [16] provides assurance with a slight computation overhead with a proxy that generates a cryptographic digest in support of the original signer with asymmetric cryptography. Anyone with access to the primitive signers' public keys and proxy can check the appeared signature afterward. Previous

Yanrong Lu is with School of Safety Science and Engineering, Civil Aviation University of China, Tianjin, China. (e-mail: yr_lu@cauc.edu.cn)

Ding Wang is with College of Cyber Science, Nankai University, Tianjin, China, and with State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China, and also with Tianjin Key Laboratory of Network and Data Security Technology, Tianjin, China. (Corresponding author: Ding Wang; Email: wangding@nankai.edu.cn)

Mohammad S. Obaidat, Fellow of IEEE and Fellow of SCS, Distinguished Professor, Department of Computer Science and Engineering, Indian Institute of Technology-Dhanbad, 826004, India, King Abdullah II School of Information Technology, University of Jordan, Amman 11942, Jordan and with University of Science and Technology Beijing, Beijing 100083, China. (e-mail: msobaidat@gmail.com or m.s.obaidat@ieee.org)

Pandi Vijayakumar is with the Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, India. (e-mail: vijibond2000@gmail.com)

work focuses on proxy signature on wide applications, such as grid computing [17], mobile communication [18], and long-term evolution wireless networks [19]. There are still few concerns about the security and performance of current and future IIoT when deployed on edge.

In this paper, we explore an innovative security framework for CPS that hosts intelligent IIoT devices with a broad spectrum of services such as data security, devices anonymity and safety, and energy-efficiency. Specifically, it leverages a delegation model to generate signatures for achieving data integrity and authenticity. The *exit* routers produce signatures according to those devices' security policies with untraceability of their real identities. For consumers, we adopt session establishment with the help of the *entry* routers that address authentication of devices without revealing their identities. Such approaches can make authentication more resilient, with lower latency and easier achievement than previous work. We highlight our contributions as follows:

1) We present a three-layer skeleton in CPS based on edge assistance. The upper layer is designed for registration management, while the center layer is for data transmission and the lower layer contains the IIoT devices. It separates the demand for a straight interconnection with the IIoT devices and reduces the system complexity.
2) We propose a two-way authentication scheme using proxy signature and session connection. It dramatically reduces the cost of signing on IIoT devices and blocks unauthorized retrieval at the edge, laying the foundation for privacy protection on the IIoT devices.
3) We show the security and performance analyses of the proposed scheme to present its resilience and practicality in comparison with the previous work.

This paper inherits the basic idea of the previous version [20]. They differ predominantly on the following sides: (1) We analyze the effects of the delegation model and show the impacts of the increased consumption due to the edge routers in the system. (2) We design an efficient revocation algorithm with hashchain to revoke offenders with very low consumptions. (3) We summarize a literature review to present relevant methods and gaps in the existing research. (4) We create a flowchart of the proposed system to represent the authentication workflow.

The remainder of this article is arranged as follows. Section II shows the literature review. We give the proposed framework, and threat model in Section III. We present our design in Section IV. In Section V, we analyze the security aspects, and in Section VI, we conduct performance efficiency analysis. Finally, we conclude in Section VII.

II. Literature review

A. New Era of AI in CPS Security

Rapid advancement in AI and machine learning enhances the scale, cost savings, speed, flexibility, and accuracy of the security in CPS. AI algorithms enable smart devices to imitate intelligent behaviors and intelligent mechanisms for processing complex and changing data sources. The advances in computing and data benefit AI for secure CPS that integrates a vast variety of smart devices, including computing devices, crowdsensing devices, sensors or actuators, and so on [21]. AI-based techniques can be used in intrusion detection, malware analysis, threats identification, suspicious behavior monitoring, preventing security attacks, and so on.

Recently, much attention has been drawn to security issues by the integration of AI technology and CPS communications [22]–[25]. Klumpp [22] proposed a forecast model that merged AI techniques, CPS, and the Internet of things to prevent accidental security leaks. Fulton-Andrae [23] used reinforcement learning to construct an autonomous CPS system model under control and verified that their systems are safe. Pan *et al.* [24] discussed possible threshold-based physical layer authentication and showed that machine learning algorithms could be very helpful in improving authentication accuracy, but at the cost of privacy leakage. Iqbal *et al.* [25] summarised an outline of computational intelligence of potential application areas in CPS based environment from three domains, health services, optimized transportation, and social networking sentiment analysis.

Most other related work has drawn more attention to AI-based cybersecurity attacks relating to CPS. Hussain *et al.* [26] utilized the deep convolutional neural networks to discover distributed denial-of-service attacks in CPS. In the first step, feature maps are constructed by extracting the characteristics of data packets, and in the second step, the abnormal traffic is detected. They declared accuracy of 91% using the detection strategy. Jahromi *et al.* [27] presented a two-layer ensemble industrial control system attack detection framework for industrial CPS based on deep neural networks. The proposed approach adopted an unsupervised deep representation learning model to detect the attack samples. They demonstrated that the proposed model can accurately attribute cyberattacks though with high computational complexity. However, both present AI-related advanced surveys are usually assumed that industrial CPS adequate higher quality cyber attacks, which, disobeys the real-time attack example-constrained scenario. Although AI technology enables improvements in computational and physical elements intelligence in centralized architecture, it brings a challenge in promoting edge processing, privacy and data security. To perform data processing at the edge instead of using a centralized cloud, ICN becomes a promising network candidate.

B. Progress in Access Security of ICN

Existing solutions on access security under the ICN backbone are authenticity in a manner that an individual signs the requested data, such as in [28], [29] or confidentiality in a manner that an individual encrypts the requested data, such as in [30], [31], [32]. Authenticity and integrity, for instance, Zheng *et al.* [28], introduced a revocable certificateless signature scheme to invade incorrect data injection. Such approach achieves data source authentication to any receiver who can confirm data provider. Similarly, Ghali *et al.* [29] discussed the root causes of the content poisoning attacks that are related to authenticity, integrity, and availability. The authors also proposed a network-layer trust management architecture based

on content ranking and evaluated its correctness and practicality using ndnSIM [33] simulator. Confidentiality, for instance, Fotiou *et al.* [30] put forward a proxy re-encryption scheme using identity-based cryptography. Compared to the public key infrastructure-based scheme, this scheme considerably minimizes the computational cost owing to non-essential public-key certificate management. Nevertheless, it is unrealistic in large-scale deployment with the need for pre-stored encryption keys. Li *et al.* [31] introduced an access control design that relied on attribute-based encryption, where the encrypted keys are produced with the authorized attributes. Despite its low overhead, revocation remains a challenge in such an approach; the private key corresponding to each attribute has to be regenerated and redistributed during revocation. By adopting cryptographic algorithms such as Shamir (t, n) threshold, Misra *et al.* [32] introduced an efficient access control framework that focused on privilege revocation. Unfortunately, the work did not cover all users' privileges so that the revocation approach is not efficient.

Searching for the heterogeneous panaceas, several investigators have switched their concerns to mixture paths. Xue *et al.* [34] designed a trusted data source based access control to combine group signature [35], and symmetric encryption [36]. This set of mechanisms satisfies privacy and confidentiality accordingly. Still, the end-to-end interconnection via a secure channel negates the in-network caching. To improve security on the consumer side, Nunes-Tsudik [37] presented a Kerberos authentication scheme that supports single sign-on. Although the combination of authentication and authorization enforcement provides the system security remarkably, it is easy to suffer from a single point failure if the whole system relies on a fully trusted platform. Additionally, it is impractical to interconnect between two ends directly.

C. ICN Meets IoT

For ICN-based applications, there is a sort of schemes to provide low communication delay for IoT. To meet the communication condition of the lighting control, De Silva *et al.* [38] deployed ICN on the smart home that separates the control level and the data level. To deal with data access communication for smart cities, Mick *et al.* [39] designed an on-boarding authentication scheme based on ICN pillar, which acts as a consolidation server to manage key distribution. Despite its flexibility, it needs to preset a symmetric key within an IoT device, which may seriously weaken its scalability and have an enormous effect on its performance. Kassab *et al.* [40] compared information-centric IoT devices access with the edge and cloud detection for a multi-cell system from the error exponents point-of-view. The authors also introduced optimal model-based detectors including optimal edge detection and optimal cloud detection and evaluated the performance of both with regard to the joint error probability. According to the popularity and freshness attributes of the IoT contents, Amadeo *et al.* [41] provided an NDN [42] caching strategy with respect to the cache hit rate at the edge.

A few recent studies have shifted IoT deployment to ICN environment for scalability [43], security threats [44], and communication optimization [45]. Baccelli *et al.* [43] provided a real IoT experiment with ICN deployment through 60 nodes situated in different rooms of different buildings. They reported that the proposed routing protocols indeed lower energy consumption on resource-constrained IoT devices. Sicari *et al.* [44] suggested a solid architecture for IoT favored ICN communication paradigm. This framework includes trusted model-orientated nodes and links, personal information protection for sensitive data, and an access control approach. To optimize live streaming service quality, a distributed multipath transmission framework also used ICN for IoT community [45], but it did not provide any adaption of the delivery approach and may induce the collapse of the live video if there is a large amount of data in the networks.

The related work can provide a certain access security, but those schemes sacrificed the usability of the in-network cache. Since the majority of them either provide a one-way authentication or need to interconnect between the endpoints devices. Additionally, each resource-restricted IoT device need to be generated a huge amounts of workload with asymmetric cryptography, which increases the interaction latency between the two ends unavoidably. Furthermore, privacy instantly turns out to be a top issue when IoT devices have access to the Internet service because the curious ICN routers can gather the vulnerable messages and exploit the identifications of the involved contributors in the message communication. In this paper, we use an edge-based service intelligence to create a system framework and subsequently propose an authentication scheme for IIoT in CPS. Our scheme ensures that only legitimate devices can access authentic sensor data.

III. Problem Statements

A. Notations

Table I listes the notations and the security assumptions in this paper.

B. System Model

In our model, the CPS controllers provide system infrastructure at the top, followed by the ICN communication pillar, and then the IIoT devices. The architecture places cached routers at the network's edge to communicate with their neighbouring devices via two packet classes, Interest and Data, respectively. The Interest packets are sent by the requesters with the named data, and the Data packets are returned by the providers or the in-cached routers binding with their cryptography signatures. The edge routers are responsible for making a match between the Interest and Data packets and then storing the corresponding content to be obtainable for the following requests.

The system model consists of four types of participants, CPS controllers, IIoT devices (e.g., actuators, sensors, computers), intermediate routers, and edge routers. Notably, CPS controllers are responsible for all of the participants registration. IoT devices allude to consumers or providers who employ terminals or applications to pay a subscription or provide power utility. Edge routers as edge servers are separated into two types: *entry* routers and *exit* routers. The *entry* routers connect consumers, which have imposed security strategies to

TABLE I
NOTATIONS

Notations	Descriptions
Q_0, s_0	the public (resp.private) key of the system
Q_{A}, s_{A}	the public (resp.private) key of an entity A
id_{A}	the identity of an entity A
x_{A}	the secret value of an entity A
MAC$(\cdot)$	hash functions
D_{A}	the secret information of an entity A
ξ_{A}	the initial value of hash chain of an entity A
t_{A_i}	i-th time interval of an entity A
p_{A}	the partial private key of an entity A
Rev_{A_i}	i-th revocation information of an entity A
RL_{A_i}	i-th partial revocation key of an entity A
$r \in S$	the element is selected from the set S at random
κ	security parameter
$\mathbb{G}_1$,$\mathbb{G}_2$	The cyclic additive (resp.multiplicative) group over prime finite field $\mathbb{F}_p$
P	a generator of $\mathbb{G}_1$
q	the prime order of $\mathbb{G}_1$ and $\mathbb{G}_2$
e	a pairing from $\mathbb{G}_1$ to $\mathbb{G}_2$ such that $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
Strong Diffie -Hellman(DH) assumption in $\mathbb{G}_1$ [34]	No probabilistic polynomial time opponent computes $b, \frac{1}{a+b}P \in \mathbb{Z}_q^* \times \mathbb{G}_1$ with non-negligible probability for given a (ℓ+1)-tuple $P, aP, a^2P, \ldots, a^\ell P \in \mathbb{G}_1$ with a random nonce $a \in \mathbb{Z}_q^*$.
Computational Diffie -Hellman(CDH) assumption in $\mathbb{G}_1$ [46]	No probabilistic polynomial time opponent computes $abP \in \mathbb{G}_1$ with non-negligible probability for given a triple $P, aP, bP \in \mathbb{G}_1$ with random choices of a, $b \in \mathbb{Z}_q^*$.

determine if an Interest and Data packet ought to be delivered and discarded according to the validation results. The *exit* routers connect providers, which are given authorization to execute proxy signature and sign on the request on behalf of the IIoT providers, e.g., temporary absence, lack of time, or computational power. Transitional routers are allocated in the ICN pillar to transmit the packets among devices.

To reduce response latency due to the current number of growing IoT devices, mist computing can be located at the extreme edge of the network infrastructure which consists of the very edge, sensors, and actuators [47]. Mist computing puts resources computing power accessible on the processing capability-limited edge devices. Mist computing utilizes those edge devices to transfer data to the fog node and eventually to the cloud. Our approach differs from mist computing as follows: 1) We define two edges routers that connect to the consumers and providers, respectively. Consumers generally are typically resource-constrained devices whereas providers are considered to be companies or factories which have more powerful computing power than consumers. 2) Packet transfer: As given in our system model, transport and forwarding tasks occur through the ICN transmission layer which handles content chunks about the unique routable names in terms of access strategies and application demands.

C. Threat Model

We consider both passive adversaries and active adversaries. Passive attacks may be initiated by the routers who have gathered a slew of Interest details to grasp "who is requesting" and "who is replaying" [48]. In contrast to the passive adversaries, the active adversaries have stronger power such that they perhaps perform some powerful attacks for any packets channeling within the ICN stacks, such as catch/explore Interest packets, change requests and response, and impersonate as permitted IIoT devices to forward Interest packets [49]. Under the system architecture, we suppose that each contributor is required to register on the CPS controller in advance if they are approved to connect to the system resources [50], [51]. To make our system more practical, we consider the CPS controller is uncertain to be a powerful, and reliable third party [52]. This is because a concentrated participant is grounds for a concentrated reliance and generates a single point of failure.

IV. EDGE-ASSISTED INTELLIGENCE DEVICE AUTHENTICATION IN CPS

We adopt proxy signature and session-based variant to lay out authentication for IIoT devices. The proxy signature is utilized to verify the alleged providers and the *exit* routers, the session-based variant is used to check the requesting consumers and the *entry* routers.

A. Overview

Our scheme gives assistance to conduct the following for intelligence device authentication in CPS based on edge assistance: (1) Allows the provider to delegate their signing capability to *exit* routers enabling the same requests from different requesters to be served. (2) Allows consumers to be authenticated themselves to *entry* routers enabling the requested contents to be returned to legitimate consumers. (3) Keeps IIoT devices anonymous to intermediate routers, according to the authentication policy. We simplify the system model, which includes a single CPS controller, consumer, *entry* router, *exit* router and provider in each domain.

A complete description of the authentication procedure involves six steps: The first step is the registration process between participants (intelligent devices, *entry* router, and *exit* router) and the controller. The third step is initiated by a consumer who issues a request for content, the *entry* router forwards the request to the routers only if the consumer is considered to be in a legitimate state in Step two. The fourth step is performed at a data provider side who assigns its signing capability to a nominated *exit* router. The fifth step is performed at the *exit* router side, which produces a message digest representing the providers and gives it back to the *entry* router through the initial path. The final step is the session handshake between the consumer and the *entry* router. The consumer is allowed to get access to the requested content once it is authenticated after the last step. Fig.1 illustrates the brief authentication procedure of the proposed system.

Based on abovementioned operations, any router may deduce transmitted content using its cache, but cannot associate cache to a precise IoT device. The design not only achieves "zero touch" end-to-end interaction, but realizes authentication without identity overflow of both two end devices.

B. Authentication Scheme

Step 1. *Registration*: The CPS controller starts the system and broadcasts the system parameters params. Both contributors should recognize themselves to the CPS controller and get

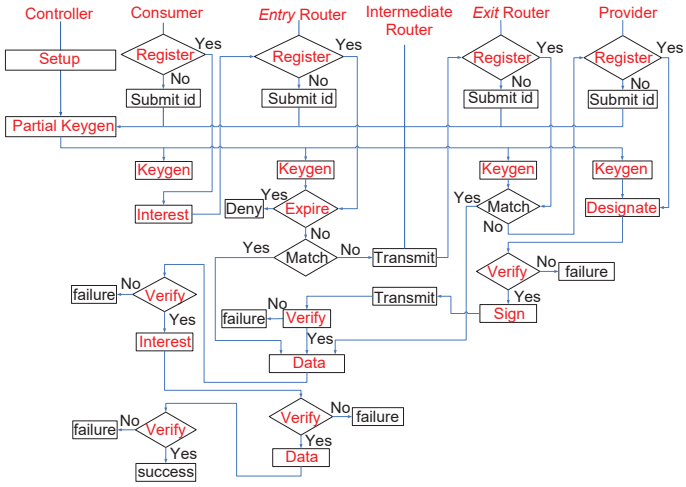


Fig. 1. Authentication process. Here match denotes if the ICN router is cache hit or not.

a set of keys $\langle Q_C, s_C\rangle$, $\langle Q_{ER1}, s_{ER1}\rangle$, $\langle Q_{ER2}, s_{ER2}\rangle$, $\langle Q_P, s_P\rangle$ for consumer, *entry* router, *exit* router and provider according to `Setup`, `PartialKeyGen` and `KeyGen` procedures described as follows.

`Setup`: The CPS setup process is presented below.

- Generate bilinear map groups $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$ with security parameter κ and choose the generators $P \in \mathbb{G}_1$.
- Choose cryptographic hash functions $\mathrm{h}_1, \mathrm{h}_3 : \{0,1\}^* \to \mathbb{G}_1$, $\mathrm{h}_2, \mathrm{h}_4 : \{0,1\}^* \to Z_q^*$, $\mathrm{h}_5 : \{0,1\}^* \to \{0,1\}^\kappa$.
- Choose a master-key $s \in \mathbb{Z}_q^*$ and compute a public key $Q_0 \leftarrow sP$. The public parameters are params= $\langle \mathbb{G}_1, \mathbb{G}_2, e, P, Q_0, \mathrm{h}_1, \mathrm{h}_2, \mathrm{h}_3, \mathrm{h}_4, \mathrm{h}_5, \mathrm{MAC}\rangle$. We suppose params are recognized in public all through, while the master-key is to be known by the CPS controller alone.

`PartialKeyGen`: The CPS controller produces the partial key corresponding to entity A. The process inputs params, master-key, a secret value $x_A \leftarrow \mathbb{Z}_q^*$ selected by entity A and an identifier for entity A with a string $id_A \leftarrow \{0,1\}^*$, as input. Each partial key consists of two components: the partial revocation key RL_A and the partial private key p_A. The revocation information is a set of hash chain with an initial string as inputs. The partial private key is computed by hashing an identity id_A and $x_A P$ to a point multiply with the master-key. Generally, this step is assumed to happen through a secure medium. The details are presented as follows.

- Entity A delivers $\langle id_A, x_A P\rangle$ to the CPS controller.
- Generate $\xi_A \in \{0,1\}^*$.
- Compute

$$
\begin{aligned}
Rev_{A_1} &\leftarrow \mathrm{h}_5(\xi_A), \ldots, Rev_{A_\kappa} \leftarrow \mathrm{h}_5(Rev_{A_{\kappa-1}}),\\
RL_{A_1} &\leftarrow \langle Rev_{A_1}, t_{A_1}\rangle, \ldots, RL_{A_\kappa} \leftarrow \langle Rev_{A_\kappa}, t_{A_\kappa}\rangle,\\
t_A &\leftarrow t_{A_1} \cup \ldots \cup t_{A_\kappa},\\
RL_A &\leftarrow RL_{A_1} \cup \ldots \cup RL_{A_\kappa},\\
D_A &\leftarrow \mathrm{h}_1(id_A, x_A P),\\
p_A &\leftarrow sD_A.
\end{aligned}
$$

`KeyGen`: The controller puts params, the partial private key p_A and secret value x_A as inputs and produces the private key s_A and public key Q_A, respectively. A collection of p_A and x_A consists of a full private key of an entity A, and its public key corresponds to $x_A P$. The procedure is executed by A who is the unique ownership of x_A.

Step 2. *Revocation Check*: If a consumer is revoked by the controller, all participants have to quit the content service. Thus, the controller periodically publishes a revocation list to all routers to check whether the consumer is revoked. The revocation check process is detailed as follows.

`Revocation Check`: The revocation check runs at the *entry* router side and checks if the consumer is attached to the revocation index before the session connection. It requires params, the current time interval t and the revocation list RL_C. After exploring the validity of the revocation parameter in the revocation list, the *edge* router can confirm the revocation evidence of the consumer. It makes the content request which generates after the time t_{C_κ} become invalid because of timestamp t_{C_κ} is not in t_C.

Step 3. *Interest Packet*: The consumer launches a subject to transmit its Interest, a content has the name of */domain/energy/Access/Query* within its surrounding district. Beginning from the root name, / fixes the borders of the portions. The *domain* refers to a detailed district exploration that a provider could provide the corresponding service. The *energy* refers to the primary service that is affiliated to the provider. The *Access* refers to the sub category service providing more specifics associated to the provider to construct a further reply, which is comprised in the Data. The *Query* refers to the consumer request.

Step 4. *Delegation Signing*: When receiving the Interest packet, the provider will delegate its signing rights to its *exit* router according to the following ways.

`Delegation Signing`: This step runs at the provider side and gets as input params, the provider's secret value x_P and a warrant m_ω that includes delegation period, message m, the identity information of an *exit* router id_{ER2}, the public key of the CPS provider Q_P and the *exit* router Q_{ER2}. The provider delegates its rights as follows.

- Compute $H_2 \leftarrow \mathrm{h}_2(id_{ER2}, m_\omega, Q_P, Q_{ER2})$, the secret value $D_{ER2} \leftarrow \mathrm{h}_1(id_{ER2}, Q_{ER2})$, and $\varpi \leftarrow \frac{x_P D_{ER2}}{x_P + H_2}$.
- Commit to the *exit* router record proxy-trans: $\langle m_\omega, \varpi\rangle$, and forward them to the *exit* router, which is appointed to verify it is employing the provider's public key later.

Step 5. *Delegation Verification and Proxy Sign Generation*: Upon receiving the delegation signature, the *exit* router will get a proxy signing key pair $\langle s_{ER2}, PK_{ER2}\rangle$ if the check is correct, where PK_{ER2} is a set of public key $\langle Q_{ER2}, Q_P\rangle$. If true, the *exit* router creates a digital signature from a message instead of the provider. The identities of the provider are not revealed publicly from a signature.

`Delegation Verification and Sign`: Algorithm I runs at the *exit* router side. First, it deals with the validness of the proxy signing key pair $\langle s_{ER2}, PK_{ER2}\rangle$, which enables the *exit* router to generate the proxy signature. If equation (1) holds, the *exit* router produces a digest of a message m in the name of the primitive provider. It requires params, the *exit* router's secrets s_{ER2}, the public-key of the *exit* router, and the

proxy-trans. The final result of the signature is a couple of values $\langle R, V\rangle$.

Algorithm I: `Delegation Verification and Sign`
Input: params, s_{ER2}, PK_{ER2}, proxy-trans
Output: **1:** yield σ; **0:** failure
1: Compute
$H_2 \leftarrow \mathrm{h}_2(id_{\text{ER2}}, m_\omega, Q_{\text{P}}, Q_{\text{ER2}})$.
2: Verify **if** $e(\varpi, Q_{\text{P}} + H_2 P) = e(Q_{\text{P}}, D_{\text{ER2}})$ **then**
3: Select $r \in \mathbb{Z}_q^*$.
4: Calculate
$R \leftarrow rP$, $H_3 \leftarrow \mathrm{h}_3(m, id_{\text{ER2}}, R, Q_{\text{ER2}})$,
$V \leftarrow p_{\text{ER2}} + H_2 Q_{\text{P}} + x_{\text{ER2}} H_2 P + rH_3$.
$\sigma \leftarrow \langle R, V\rangle$.
5: return **1**
6: **else**
7: return **0**
8: **end if**

Proof.

$$\begin{aligned} e(\varpi, Q_{\text{P}} + H_2 P) =& e(\frac{x_{\text{P}} D_{\text{ER2}}}{x_{\text{P}} + H_2}, Q_{\text{P}} + H_2 P) \\ =& e(\frac{x_{\text{P}} D_{\text{ER2}}}{x_{\text{P}} + H_2}, x_{\text{P}} P + H_2 P) \\ =& e(x_{\text{P}} D_{\text{ER2}}, P) \\ =& e(D_{\text{ER2}}, Q_{\text{P}}). \end{aligned} \tag{1}$$

The signature packet crosses a series of routers, each one verifies whether the embedded signature σ with piggybacked public keys of the provider and *exit* router, respectively.

`Verify`**:** The receiver verifies the validity of a signature using equation (2) of a known message m regarding params and PK_{ER2}, separately. Note that if σ is a rational signature with a message m, it accepts the signature and rejects, otherwise.

Proof.

$$\begin{aligned} e(V, P) =& e(p_{\text{ER2}} + H_2 Q_{\text{P}} + x_{\text{ER2}} H_2 P + rH_3, P) \\ =& e(p_{\text{ER2}}, P) \cdot e(H_2 Q_{\text{P}}, P) \cdot \\ & e(x_{\text{ER2}} H_2 P, P) \cdot e(rH_3, P) \\ =& e(sD_{\text{ER2}}, P) \cdot e(Q_{\text{P}}, H_2 P) \cdot \\ & e(H_2 P, x_{\text{ER2}} P) \cdot e(H_3, rP) \\ =& e(D_{\text{ER2}}, Q_0) \cdot e(Q_{\text{P}}, H_2 P) \cdot \\ & e(H_2 P, Q_{\text{ER2}}) \cdot e(H_3, R) \end{aligned} \tag{2}$$

Step 6. *Session Connection*: We catalog the instance when the *entry* router is demanding to reach an interrelation with the consumer. Suppose that the *entry* router has fetched a Data packet from the *exit* router. This step usually happens when the requested content could not be matched up to any routers.

After receiving signature packets, the *entry* router makes a session request by addressing a call link via a Data packet, */domain/*`energy`*/Access/Query/signature/sessioninvitepacket*, including four elements of a content, i.e., content name, content signature and content itself along with a created identity id at random, which is utilized subsequently by the *entry* router to recognize itself to the consumer. Accordingly, the *entry* router generates a *signature* including a collection of publicly known values with the help of some parameters since each router requires each content to be verified. The details are shown as follows.

– Select $r_{\text{ER1}} \in \mathbb{Z}_q^*$.
– Calculate $U \leftarrow r_{\text{ER1}} P$, $W \leftarrow p_{\text{ER1}} + r_{\text{ER1}} Q_0$.
– Generate $signature : \langle U, W\rangle$.

Upon receiving the Data packet inside the range of endurable period, the consumer needs to be connected with the adjacent *entry* router to respond to an asking message to get through the authentication step. The consumer responds with an Interest packet that takes the *entry* router's set of attributes such as public-key Q_{ER1}, identity id and private key s_{C} of the consumer associated with other essential public parameters params as inputs and outputs `Req` as the components of the reply messages. The consumer replies with an Interest packet procedures.

– Verify $e(W, P)$ is equal to $e(D_{\text{ER1}}, Q_0) \cdot e(U, Q_0)$. If it holds, execute the next step. Otherwise, stop session.
Proof.

$$\begin{aligned} e(W, P) =& e(p_{\text{ER1}} + r_{\text{ER1}} Q_0, P) \\ =& e(p_{\text{ER1}}, P) \cdot e(r_{\text{ER1}} Q_0, P) \cdot \\ =& e(sD_{\text{ER1}}, P) \cdot e(Q_0, r_{\text{ER1}} P) \cdot \\ =& e(Q_0, D_{\text{ER1}}) \cdot e(Q_0, U) \end{aligned} \tag{3}$$

– Select $r_{\text{C}} \leftarrow \mathbb{Z}_q^*$.
– Calculate $E \leftarrow r_{\text{C}} Q_{\text{ER1}}$, $S \leftarrow r_{\text{C}} P - x_{\text{C}} D_{\text{ER1}}$.
– Generate `Req`: $\langle E, S\rangle$ as the integrants of the answered messages.

The consumer then returns the Interest packet, a content has the name of */domain/*`authenticate`*/id/Communicate/*`Req` to the *entry* router inviting the session. The `authenticate` branch refers to the subcategories that accept the invitation containing the identity `id` of whom it correlates with the *entry* router which entitles a direct, bi-directional *Communicate* path between them.

The *entry* router acquires the Interest packet from its responded consumer and continues the steps as follows.

– Retrieve $r_{\text{C}} P \leftarrow x_{\text{ER1}}^{-1} E$.
– Verify using equation (4). If the verification is successful, go to next step. Otherwise, abort the session.
Proof.

$$\begin{aligned} & e(p_{\text{ER1}}, Q_{\text{C}}) \cdot e(S, Q_0) \\ =& e(sD_{\text{ER1}}, x_{\text{C}} P) \cdot e(r_{\text{C}} P - x_{\text{C}} D_{\text{ER1}}, sP) \\ =& e(sx_{\text{C}} D_{\text{ER1}}, P) \cdot e(r_{\text{C}} sP - x_{\text{C}} sD_{\text{ER1}}, P) \cdot \\ =& e(sr_{\text{C}} P, P) \cdot e(Q_0, r_{\text{C}} P) \end{aligned} \tag{4}$$

– Compute a shared value $K \leftarrow \mathrm{h}_4(r_{\text{ER1}} P, r_{\text{C}} P, r_{\text{ER1}} r_{\text{C}} P)$, and the MAC value $\tau \leftarrow \text{MAC}(r_{\text{ER1}} P, K)$.
– Generate a Data packet corresponds to the Interest packet, */domain/*`authenticate`*/id/Communicate/*`Req`*/signature /response packet*, including the content m and τ hidden in the *signature* together with the signature σ. It responds with the Data packet to the consumer who is calling for the content.

Finally, the consumer executes the last step to verify the legitimacy of the *entry* router as follows.

– Compute $K' \leftarrow \mathrm{h}_4(U, r_{\text{C}} P, r_{\text{C}} U)$.
– Check MAC function (U, K', τ). If the result is 1, then continue to the next step. Otherwise, refuse.

– Verify σ. If the verification is true, the session connection is successful. Otherwise, the consumer is not considered to be a legitimate one, and drops the session. However, the consumer begins to check the authenticity of the signature derived from the *exit* router alternatively.

V. Security Analysis

The proposed mechanism ensures that the CPS controller can uniquely obtain the partial private keys, preventing it from imitating a legitimate entity. We analyze the authentication scheme concerning the security goals listed below.

To prevent the adversaries, we pinpoint the following security goals of the authentication mechanism.

Integrity: The mechanism should provide trustworthiness to a signer that is incapable of being false to a Data packet.

Authenticity: The mechanism should provide the proven fact that a signed Data packet is legitimate.

Authentication: The mechanism should provide the process of verifying the identity of who is broadcasting an Interest and is answering what it claims to be [53].

Anonymity: The mechanism should provide protection to the IoT devices that their identities are not known to both the insider and outsider adversaries.

Key Establishment: The mechanism should provide a negotiated key between the consumer and its *entry* router so that no single party can control what the key will be [54].

Authenticity: A polynomial-time opponent $\mathcal{A}$ is in capable of counterfeiting a signature which is ascribed to an authorized entity in order that the entity is unable to deny.

Theorem 1: There is a polynomial-time challenge $\mathcal{C}$ which can solve the CDH problem with probability $\epsilon(\kappa)' > (\epsilon(\kappa)/2)(1 - q_s(q_{\mathrm{h}_3} + q_s)/2^{\kappa})(e(q_{\mathrm{r}} + 1))^{-1}$ depending on whether the opponent $\mathcal{A}$ can fake a signature σ with an advantage $\epsilon(\kappa)$. Where q_{h_3}, q_s, and q_r denote the numbers of making queries to the h_3, `signing` and `revealpartialkey` oracles, respectively, assuming that hash functions h_{i}(i=1,2,3) are random oracles.

Proof: Let $X \leftarrow aP$, $Y \leftarrow bP \in \mathbb{G}_1 \times \mathbb{G}_1$ denote a random challenge. We can create the algorithmic program $\mathcal{C}$ to output $abP \leftarrow \mathbb{G}_1$ by using the forger $\mathcal{A}$. Algorithm $\mathcal{C}$ first creates system parameters params as the protocol does and sends params to the forger $\mathcal{A}$, initializes $\mathcal{A}$ with $Q_0 \leftarrow X$, and then interacts with $\mathcal{A}$ as follows.

- h_1 and h_3 Queries: When $\mathcal{A}$ queries the random oracle h_1 (h_3) with a tuple $\langle id_i, Q_i\rangle$ ($\langle m_i, id_i, R_i, Q_i\rangle$), $\mathcal{C}$ preserves an index $\mathrm{L}_{\mathrm{h}_1}$ ($\mathrm{L}_{\mathrm{h}_3}$) of components $\langle id_i, Q_i, x_i, c_i, \nu_i\rangle$ ($\langle m_i, id_i, R_i, Q_i, y_i, d_i, \upsilon_i\rangle$) which is initialized empty and answers as follows:
  – If the query $\langle id_i, Q_i\rangle$ ($\langle m_i, id_i, R_i, Q_i, Q_j\rangle$) is already in $\mathrm{L}_{\mathrm{h}_1}$ ($\mathrm{L}_{\mathrm{h}_3}$), $\mathcal{C}$ outputs ν_i (υ_i) to $\mathcal{A}$.
  – Otherwise, $\mathcal{C}$ picks $x_i \in \mathbb{Z}_q^*$ ($y \in \mathbb{Z}_q^*$) at random, returns $\nu_i \leftarrow x_iP$ ($\upsilon_i \leftarrow y_iQ_0$) if a coin toss $c_i \leftarrow \{0,1\}$ ($d_i \leftarrow \{0,1\}$) that outputs 0 with probability δ (1/2) and returns $\nu_i \leftarrow x_iY$ ($\upsilon_i \leftarrow y_iP$) if $c_i = 1$ ($d_i = 1$) with probability $1 - \delta$ (1/2), and adds $\langle id_i, Q_i, x_i, c_i, \nu_i\rangle$ ($\langle m_i, id_i, R_i, Q_i, y_i, d_i, \upsilon_i\rangle$) into $\mathrm{L}_{\mathrm{h}_1}$ ($\mathrm{L}_{\mathrm{h}_3}$).
- h_2 Queries: When $\mathcal{A}$ queries the random oracle h_{i} with a list of tuples of the form $\top_i$, $\mathcal{C}$ maintains the corresponding list $\mathrm{L}_{\mathrm{h}_{\mathrm{i}}} \leftarrow \langle \top_i, \mu_i\rangle$. $\mathcal{C}$ returns the corresponding entry μ_i if the input is found in the list $\mathrm{L}_{\mathrm{h}_{\mathrm{i}}}$. Otherwise, returns a random value in Z_q^*.
- `RevealPartialKey` Queries: When $\mathcal{A}$ makes this query on identity id_i, $\mathcal{C}$ retrieves the corresponding component $\langle id_i, Q_i, x_i, c_i, \nu_i\rangle$ from the index $\mathrm{L}_{\mathrm{h}_1}$ and answers this query as follows:
  – If $c_i = 1$, then $\mathcal{C}$ outputs $\perp$ and aborts simulation.
  – Otherwise, sets $p_i \leftarrow x_iQ_0$ and gives it back to $\mathcal{A}$.
- `RequestPublicKey` Queries: When $\mathcal{A}$ makes this query on identity id_i, $\mathcal{C}$ sets $Q_i \leftarrow x_iP$ for a random value $x_i \in \mathbb{Z}_q^*$, gives it back to $\mathcal{A}$, and adds $\langle id_i, x_i\rangle$ into L_{PK}.
- `Signing` Queries: $\mathcal{A}$ requests a signature with id_i on a message m_i, $\mathcal{C}$ simulates the signature oracle and responds to the query as follows:
  – If h_3 has not been issued with $\langle m_i, id_j, R, Q_j\rangle$, $\mathcal{C}$ continues the algorithm by replying to h_1 queries to get $H_2 \leftarrow \mu_2$ and sets $R \leftarrow r_2Q_0$, $H_3 \leftarrow r_2^{-1}(x_1P - D_j)$, and $V \leftarrow r_1Q_0 + \mu_2Q_i + \mu_2Q_j$ with randomly chosen $r_1, r_2 \leftarrow \mathbb{Z}_q^*$. Otherwise, $\mathcal{C}$ ceases and abandons. The possibility of not aborting is $1 - (q_s(q_{\mathrm{h}_3} + q_s)/2^{\kappa})$ due to $\mathrm{L}_{\mathrm{h}_3}$ never having more than $q_{\mathrm{h}_3} + q_s$ entries.
  – $\mathcal{C}$ returns $\sigma \leftarrow \langle V, R\rangle$ as the valid signature on a content m.

Note that the challenger $\mathcal{C}$ successfully outputs the signature σ with probability $\epsilon(\kappa)'$ so that $\mathcal{A}$ fully satisfies the `Signing` answers.

Ultimately, $\mathcal{A}$ generates a forged signature $\sigma^* \leftarrow \langle V^*, R^*\rangle$ on a message m^*. Now $\mathcal{C}$ retrieves the component $\langle id_i^*, Q_i^*, x_i^*, c_i^*, \nu_i^*\rangle$ from $\mathrm{L}_{\mathrm{h}_1}$. If $c_i^* = 0$, then $\mathcal{C}$ yields a failure and stops. Otherwise, it goes on and recovers the tuple $\langle id_i^*, Q_i^*, Q_j^*\rangle$ from the list $\mathrm{L}_{\mathrm{h}_2}$ and $\langle m_i^*, id_i^*, R_i^*, Q_i^*, y_i^*, d_i^*, \upsilon_i^*\rangle$ from the list $\mathrm{L}_{\mathrm{h}_3}$. If $d_i^* = 0$, $\mathcal{C}$ subsequently yields 0 and stops. Otherwise, it performs the following:

$e(V^*, P) = e(Q_0, D_i^*) \cdot e(Q_i^*, \mu_i^* P) \cdot e(Q_j^*, \mu_i^* P) \cdot e(R_i^*, y_i^* P)$

with $R_i^* = r_i^* P$, and $H_1 = x_i^* Y$, $H_2 = \mu_i^*$, $H_3 = y_i^* P$ for known elements $r_i^*, x_i^*, \mu_i^* \leftarrow \mathbb{Z}_q^*$. The probability of not aborting at this step is $(1 - \delta)/2$. Therefore,

$$e(V^* - \mu_i^* Q_i^* - \mu_i^* Q_j^* - y_i^* R_i^*, P) = e(X, x_i^* Y)$$

and thus ${x_i}^{*^{-1}}(V^* - \mu_i^* Q_i^* - \mu_i^* Q_j^* - y_i^* R_i^*)$ is the resolution to the target CDH problem $(X, Y) \in \mathbb{G}_1 \times \mathbb{G}_1$. The overall probability $\mathcal{C}$ does not halt the game has an upper bound $(1 - q_s(q_{\mathrm{h}_3} + q_s)/2^{\kappa})/(2e(q_{\mathrm{r}} + 1))$, where $1/e(q_{\mathrm{r}} + 1)$ is taken from the maximum value $q_{\mathrm{r}}/(1 + q_{\mathrm{r}})$ [55] on the probability of non-abortion in key extraction queries and output of a valid and nontrivial forgery $(\delta^{q_{\mathrm{r}}}(1 - \delta))/2$. Therefore, the results show that the advantage of $\mathcal{C}$ breaking the CDH problem in $\mathbb{G}_1$ is at least $(\epsilon(\kappa)/2)(1 - q_s(q_{\mathrm{h}_3} + q_s)/2^{\kappa})(e(q_{\mathrm{r}} + 1))^{-1}$. ■

As such, the authenticity guarantees that the *exit* router is allied to its assigned capabilities.

Authentication: The policy contains two parts. One is to check the validity of a desired consumer for fear that a

hostile opponent can perform a spoof to impair other harmless consumers' interests. The other is to verify the validity of answering provider for fear that a hostile opponent can insert some false information into the system. For the prior, to authenticate attainable of the consumer, only the *entry* router can compare $e(p_{\mathrm{ER1}}, Q_{\mathrm{C}})\cdot e(S, Q_0)$ to $e(r_{\mathrm{C}}P, Q_0)$ owing to the fact that its unique private key p_{ER1} is owned in itself. If it does not happen, any forged Data packets of the consumer will be discarded. For the last-mentioned, the proxy signature favors authenticity such that the gained access content definitely stems from the declared provider. In addition, it is mandatory for the authentication of the *entry* router, due to repeated content supplied access, to let it simply turn into a goal of opponent. Obtaining a correct τ indicates that the *entry* router is authenticated in such a way that the consumer simultaneously verifies the *exit* router and the provider by checking σ with the assistance of both public keys.

Anonymity: This issue concentrates on hampering opponents from uncovering the identity of the IoT devices. In the session connection process, the identification of the consumer is only associated with its own private key, which is the output of the combination of the CPS controller's private key and a random nonce. Any opponents cannot gain the identity of the consumer on the condition that its private key is secure. Furthermore, it is also useless to compromise the *entry* router, which has no related identity information about consumer. In other words, any compromised *entry* router has no effect on the privacy of the consumer. In the proxy-based manner, the recognition of the provider is also prevented because the *exit* router obtains nothing about the identity information of the provider. As a consequence, curious intermediated routers don't get the identity information of who generates the content and who requests it. Moreover, for that reason, the property secures the identity security of IoT devices in the communication interconnection.

Key Establishment: A secure session key indicates that a polynomial-time opponent $\mathcal{A}$ cannot differentiate between a real negotiated key and a random number.

Theorem 2: The proposed session connection scheme $\prod$ is secure if the underlying CDH assumption holds in $\mathbb{G}_1$ and the hash function h_4 is a random instance.

Proof: Let $p(\kappa)$ and $s(\kappa)$ denote the number of entities and sessions separately. An instance $\prod_{i,j}^{t}$ specifies the oracle indexed by t of an ordered pair entity indexed by i with a collaborator indexed by j in a session, which has a pair conversation to $\prod_{j,i}^{s}$ with a key $\mathrm{h}_4(K)$. Let $\mathcal{A}$ have a non-negligible probability $\epsilon(\kappa)$ and C to be the challenger that $\mathcal{A}$ can request the random instance h_4. Let $Pr[\mathcal{A}]$ denote the probability that $\mathcal{A}$ yields a result $\hat{b}$ such that the equality $\hat{b} = b$ held by one of the oracles $\prod_{i,j}^{t}$. Let q_{h_4} denote the number of h_4 queries. We can get the result $\mathrm{P}[\mathcal{A}|\mathrm{C}] = 1/2$ based on the equality $\mathrm{P}[\mathcal{A}] = \mathrm{P}[\mathcal{A}|\mathrm{C}]\mathrm{P}[\mathrm{C}] + \mathrm{P}[\mathcal{A}|\overline{\mathrm{C}}]\mathrm{P}[\overline{\mathrm{C}}]$. Here, the session key is the output of the hash function h_4. Accordingly, we have $\mathrm{P}[\mathcal{A}] \leq (1+\mathrm{P}[\overline{\mathrm{C}}])/2$ and $\mathrm{P}[\mathcal{A}] \geq (1-\mathrm{P}[\overline{\mathrm{C}}])/2$ and then obtain $\mathrm{Pr}[\overline{\mathrm{C}}] \geq 2\epsilon(\kappa)$. Consequently, $\mathcal{A}$ has a success probability $(2\epsilon(\kappa))/(p(\kappa)^2 s(\kappa) q_{\mathrm{h}_4})$ with the picked oracle $\prod_{j,i}^{s}$, which is opposed to the CDH problem. ■

Revocation: In our system, the CPS controller can exclude revoked users by pushing its revocation list to others. Note that the revocation process is still highly efficient if the authenticated users or revoked users has a considerable size.

TABLE II
SECURITY COMPARISON BETWEEN OUR SCHEME AND THE AUTHENTICATION SOLUTION BASED ON ICN

Features	[28]	[34]	[37]	[39]	Ours
Security assumption	CDH	Strong DH			CDH
With random oracle	√	√			√
Lacking trusted entity	√				√
Anonymity		partial			√
Authenticity	√				√
Authentication		√	√	√	√

√ specifies that the attribute is achieved.

We compare the aforementioned security properties with the previous two-party authentication schemes for ICN [28], [34], [37], [39]. This is because these schemes depend on security assumptions which are similar to those provided by our scheme, as listed in Table II. It is shown that the proposed scheme could satisfy several security attributes, such as anonymity, absence of a trusted party, strong assumption, authentication, and authenticity, which are not achieved in others.

VI. PERFORMANCE ANALYSIS

We use Matlab R2019a to survey the performance of the advocated authentication scheme under the general overheads and the effectiveness of the proxy approach. For the former, we measure communication and computation consumption under the amount of the requested contents with prior schemes [28], [34], [37], and [39] in Table III, Fig.2(a)-2(b), and Fig.3(a)-3(b), respectively. We also present communication and computation resource consumption with the amount of the requested contents in our scheme in Fig.2(c) and Fig.3(c), respectively. We suppose that the content popularity keeps to Zipf law with parameters α [56], [57]:

$$q_i \leftarrow \frac{(\sum_{i=1}^{N} 1/i^{\alpha})^{-1}}{i^{\alpha}}, \tag{5}$$

where N is the all-inclusive requested content. For the latter, we show the performance results for different Zifp parameter (α) in Fig.4(a)-4(c), and by varying contents of popularity ranks in Fig.5(a)-5(c), respectively. With Vanilla scheme, the provider generates signatures only. Conversely, the proposed scheme seamlessly incorporates proxy signature that significantly alleviates a load of provider which is shown in Fig.6(a)-6(b). In Table III, Mac, Enc./Dec., $\mathbb{G}_1$, and Pair in the calculations separately indicate the computational complexity of a message authentication code, a symmetric encryption/decryption, a group operation and a pairing, and Mac, Enc., Exp., $\mathbb{G}_1$ in communication indicates the measurements of a message authentication code, a ciphertext, a modulus, and a group element. To better compute the incurred consumptions, Table IV lists the average cryptography computation cost in the authentication process after running 1000 times for each operation. The proposed cryptography is carried out on PC with an Inter(R) Pentium 3.20GHz processor and 4.0GB memory working Win 10 system using jPBC library [58].

TABLE III
COST COMPARISON BETWEEN OUR SCHEME AND THE AUTHENTICATION SOLUTION BASED ON ICN

	Communication	Computation			
		consumer	*entry* router	*exit* router	provider
Zheng *et al.* [28]	6($\mathbb{G}_1$)	5(Pair)			4($\mathbb{G}_1$)
Xue *et al.* [34]	6($\mathbb{G}_1$)+6(Exp.)+1(Enc.)	3(Pair)+9($\mathbb{G}_1$)+1(Dec.)	5(Pair)+8($\mathbb{G}_1$)		2($\mathbb{G}_1$)+1(Enc.)
Nunes-Tsudik [37]	5(Enc.)	2(Dec.)			4(Enc.)+2(Dec.)
Mick *et al.* [39]	7(Enc)	2(Mac)+2(Dec.)			2(Enc.)
Ours	7($\mathbb{G}_1$)+1(Mac)	7(Pair)+5($\mathbb{G}_1$)+1(Mac)	7(Pair)+4($\mathbb{G}_1$)+1(Mac)	2(Pair)+5($\mathbb{G}_1$)	1($\mathbb{G}_1$)

TABLE IV
COMPUTATION COST

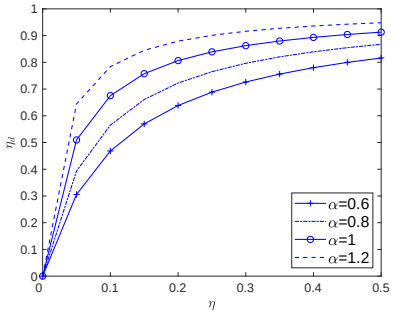
Authentication Module	Cost
One scalar multiplication in $\mathbb{G}_1$	10.51 ms
One pairing operation	6.28 ms
One symmetric cryptographic computation	0.18 ms
One Mac operation	0.04 ms

Communication Overhead: Table III summarizes the inclusive size of transmitted packets between the two end devices. It embraces a Mac and seven elements in the group $\mathbb{G}_1$. Applying the type A elliptic curve, each element of $\mathbb{Z}_q$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are 160, 512, and 1024 bits, respectively. Furthermore, symmetric cryptography and Mac function are 128 bits and 256 bits using AES-128 and SHA-256, respectively. The proposed scheme necessarily intensifies the communication burden owing to the piggybacked signature in each Data packet. We remark that the communication overheads of the presented scheme is higher than the schemes reported in [28], [37], and [39] but much lower than the scheme in [34].

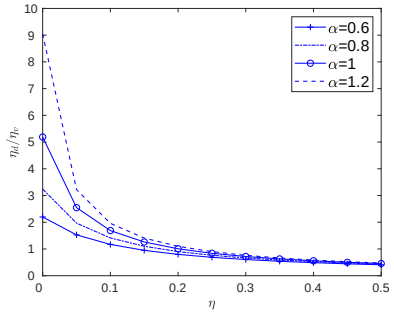
Since the signature packets size for the requested content influences the bandwidth of the Data packets, we take the verification communication cost performance into consideration with various underlying ICN authentication schemes. The performance of each scheme is determined with regard to the verification processing ratio which is equivalent to the rate of the signature packet length and the full transmitted packets length. Fig.2(a) shows the verification processing rate of different schemes increases with content request amounts rising from zero to 100. We discover that the verification processing ratio in our scheme is slightly higher than [37] and [39], but less than [28] and [34]. This is because in our scheme, the verification of a signature demands the verifier to acquire all of the packets that include the delegation information adopted to calculate that signature. However, in the figure, with a typical number of 50 contents, the verification processing rate in our scheme is less than 20%, which can be considered to be an acceptable performance in some latency-tolerant IIoT applications (e.g., plant safety).

To better investigate the amount of energy consumed by different schemes, we measure the transmission burden observed between consumer and provider in the authentication process. Here, we only consider transmitted packets when a Data packet is received successfully. Fig.2(b) summarizes our analysis of this transmission burden under growing the requested contents. A clear trend depicts the transmission burden is a linear correlation to the number of requested contents. It is noticeable that our scheme carries a slightly heavier burden compared with [28], [37], [39], but lower than [34]. However, our scheme has the advantage of providing two-way authentication and allowing content caching compared with those schemes.

The proposed scheme was assessed with its competitor schemes based on two-way authentication of IoT devices mechanism in a three-layer model. To reflect the reliability of communication overhead in the proposed scheme, we focus on the communication cost relationship between the verification against handshake transmission and the number of the requested content in Fig.2(c). The relationship ratio is defined as the signature packet size to the session connection transmitted packet length. We acknowledge that the transmission cost gradually increases with the increase of requested content while the verification consumption is less than the handshake process. For instance, with the number of requested content increasing from 50 to 100, the signature size increases only 10%. Although every signature packet has to be transmitted from the provider to the consumer, the proposed scheme has reasonable resource consumption because it does not cause large communication overhead fluctuations.



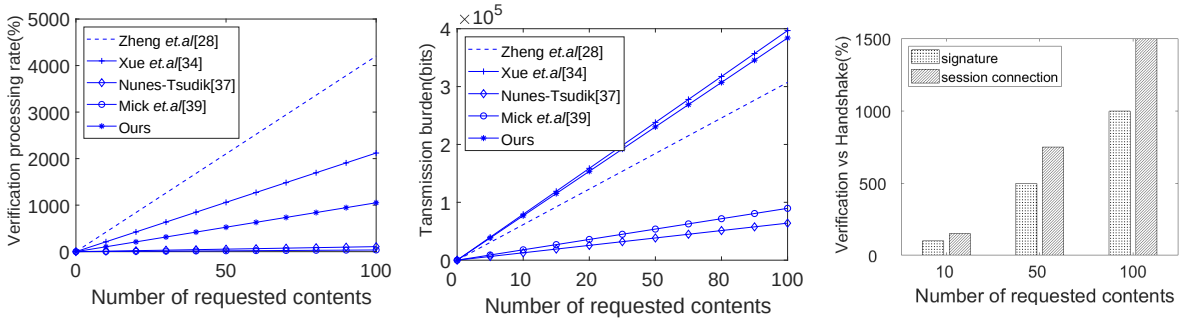
(a)



(b)

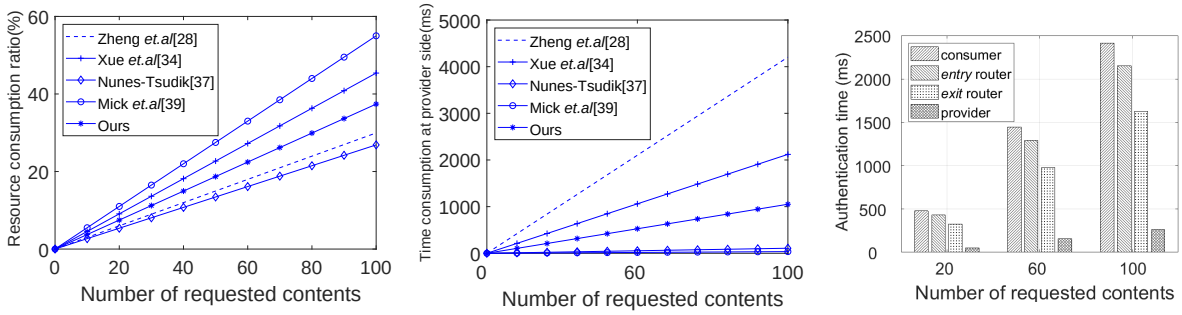
Fig. 6. Comparison in terms of the relationship between the delegation model metric η_d and the general metric η in our scheme when varying Zipf parameter α under different scenarios.(a) η_d against η. (b) the value η_d/η against η.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3151828, IEEE Internet of Things Journal



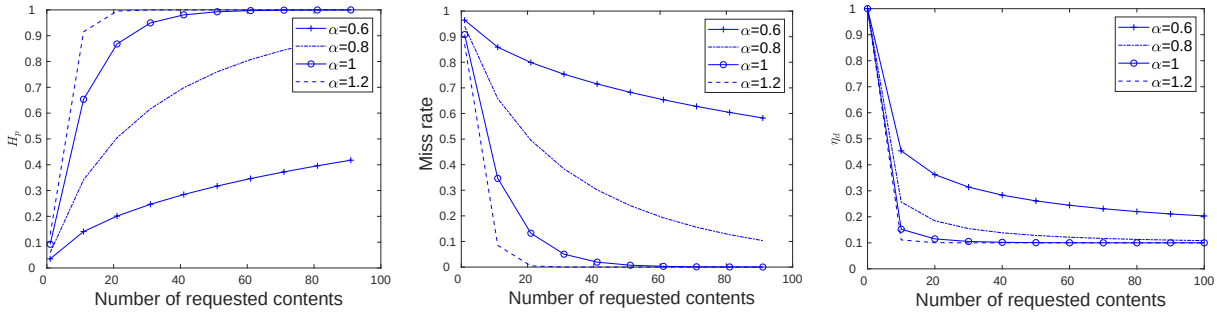
(a) (b) (c)

Fig. 2. Comparison of the communication cost with varying number of requested contents under different scenarios.(a) verification processing rate for different authentication schemes. (b) transmission burden for different authentication schemes. (c) verification cost against handshake cost in our proposed scheme.



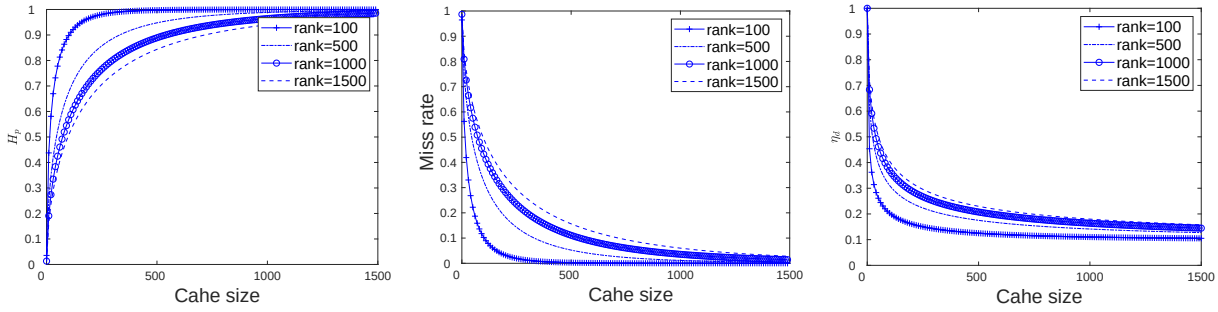
(a) (b) (c)

Fig. 3. Comparison of the computation cost with varying number of requested contents under different scenarios.(a) consumer side cost for different authentication schemes. (b) time consumption at provider side in different authentication schemes. (c) full authentication cost in our proposed scheme.



(a) (b) (c)

Fig. 4. Comparison in terms of the relationship between the content transfer performance and the number of requested contents in our scheme when varying Zipf parameter α under different three scenarios. (a) hit ratio against serving contents. (b) miss rate against serving contents. (c) η_d against serving contents.



(a) (b) (c)

Fig. 5. Comparison in terms of the relationship between the content transfer performance and cache size in our scheme when varying content popularity ranks under different three scenarios. (a) hit ratio against cache size. (b) miss rate against cache size. (c). η_d against cache size.

Computation Overhead: It is essential for both the consumer and *entry* router to verify the signed message from the *exit* router. We ignore light computations, such as map-to-point hash, and exponential modular in $\mathbb{Z}_q$. The consumer consumes a Mac, four group computations in $\mathbb{G}_1$, and seven pairings. The *entry* router utilizes a Mac operation, four group computations in $\mathbb{G}_1$, and seven pairings. The *exit* router takes five group computations in $\mathbb{G}_1$ and two pairings. The provider uses one group computation in $\mathbb{G}_1$. Table III displays that the presented scheme is costly in computation resources for comparison. This breakdown is ignored for the reason that the presented scheme could achieve security attributes like anonymity and authentication on both two ends of IIoT devices together, which is not provided in the compared schemes.

IoT devices are sensitive and have constrained resources memory, and energy, therefore, saving energy of these devices improves its productivity in terms of network lifespan. To evaluate the efficient utilization of consumer devices in the untrustworthy communication channel, the resource consumption ratio with the different schemes is considered in Fig.3(a). The ratio is described as the computational time of consumer devices successfully authenticated the Data packets to those which were transmitted. As shown in Fig.3(a), the resource consumption ratio increases as the number of requested contents increases. It is also observed that the resource consumption ratio in [28], [37], and our scheme is less than 40% when the number of requested contents increases to 100 packets compared to [34] and [39]. Considering the transmission and application requirements, our scheme has an appropriate computational resource consumption on the consumer side while achieving superior security goals among related schemes presented in Table II (e.g., authenticity).

The delegation procedure displayed in our scheme can be considered as general access control in that the provider releases rights and computation resource to a certain *exit* router. Thus, we analyze and compare the time consumption at the provider side of the proposed scheme and the existing two-party ICN authentication schemes. As expected in Fig.3(b), time consumption at the provider side is increased under the number of requested contents. The provider requires a slight increase in computational resource compared to [37] and [39], but the trend growth will be lower than [28] and [34]. Compared to the transmission burden shown in Fig.2(b), our scheme remains a relatively lower time consumption.

To further present the authentication efficiency of our scheme, Fig.3(c) shows changes in authentication time about each entities in terms of consumer, *entry* router, *exit* router, and provider under three different content request amounts with 20, 60 and 100, respectively. Following rising of requests from 20 to 100, computation overhead on the provider does not increase dramatically, and the fluctuation is kept within a small range. We can also conclude that the authentication time improves with the soaring amount of content requests, which is due to the increased time for verification of Data packets to achieve handshake. A replacement for insecure authentication is that both IIoT devices are required to be authenticated, which causes extra computation costs. It is noted that the increased computation cost is a trade-off for improved security which is shown in Table II.

Efficiency: To support the delegation model findings and to asses the model efficiency in our scheme, we define the metric given below,

$$\eta \leftarrow \frac{N_{\mathrm{P}}}{N_s}, \tag{6}$$

where N_{P} is the number of the largest computational overheads necessitated at the provider side and N_s is the overall operation of signing, respectively. The value of η_v in the Vanilla scheme corresponds to the ratio of the operation for the provider side to the total consumption, which is equal to η because all contents are matched. Nevertheless, the consumption of the proxy signature is separately borne by both the provider N_{P} and the proxy N_{ER2}. Let H_p be the transition probability, then N_{P} can be represented by $\lambda\eta$, where λ is the request arrival rate under the assumption that all the content arrivals follow the Poisson distribution [59]. Notice that H_p is equivalent to the cache hit ratio as it corresponds to the probability that the cache misses in other *exit* routers. Thus, the metric η_d in the proposed scheme is represented by:

$$\eta_d \leftarrow \frac{\lambda\eta}{\lambda\eta + \lambda(1-\eta)H_p}. \tag{7}$$

To analyze the most popular content caching performance results with regards the cache hit rate, miss rate, and the transfer index η_d, Fig.4(a)-4(c) show the results when the content items vary from 0 to 1500 for the least recently used policy presented by Che *et al*. [59], the Zipf distribution parameter α varying in the range 0.6 to 1.2 settings in 100 classes of popularity. Considering the hit rate H_p reported the approximation results in Fig.4(a), the values of H_p increase with the number of content requests on account of the high rise number of requests to be served. The impact of the hit rate H_p is more prominent for high α. In such a case, requests concentrate on a few popular contents, hence leading to a higher proxy hit rate. As more content arrives, more cache hits occur at the *exit* side since more contents need to be delivered and signed, leading to a higher cache miss rate and lower values η_d, respectively. Such a trend is verified by the results in Fig.4(b) and Fig.4(c), respectively. The suggested delegation model benefits in a larger proportion to more content requests which are likely to be satisfied promptly.

We further consider the impact of the hit ratio, miss rate, and the transfer index η_d vs cache size for contents of popularity rank 100, 500, 1000, and 1500 from a population of 1500 contents with Zipf(.6) popularity. The precision of the estimation is exemplified by the marks presented in Fig.5(a)-5(c), . As illustrated in Fig.5(a), popularity rank has the effect of the cache hit possibility across the forward rules along with the delegation model. The lower the popularity rank the larger the cache hit and vice versa. Conversely, when considering the miss possibility with the storage size, an opposite trend can be observed: the larger the popularity rank the lower the cache miss. (See Fig.5(b)). We derive the metric η_d as a function of the cache hit H_p following Eq.(7) with η=0.1, the larger proportion overhead at the provider side the higher the metric η_d (See Fig.5(c)). This is because the majority of content requests are satisfied with proxy matching. Under

these conditions, allowing for a higher cache size does improve proxy content delivery performance as the provider is already transferring all the available Interest packets.

To reflect the efficiency of the proposed delegation model with an accountable measure, we inspect the impact of the metric η with the Vanilla scheme and the metric η_d in Fig.6(a)-6(b). We consider 100 content items when varying the Zipf law popularity with an exponent of 0.6 to 1.2. As clearly shows in Fig.6(a), the lower the popularity parameter the lower the index η_d, the larger the metric η the larger the index η_d. This demonstrates the transition probability of a content request is for a given metric η largely depends on that the content's popularity. To compare the efficiency with the Vanilla scheme, Fig.6(b) gives the rate η_d/η_v in terms of the metric when varying the popularity settings. For content size set to 100, findings are as follows: (i) cache-hit dominantly affects the ratio when there is no consumption on the provider side (η=0); (ii) when η <0.2, the proposed scheme achieves higher consumption than the compared one. On the contrary, it achieves the minimum overhead with the increase of η. This result implies that our scheme effectively reduces the overhead on the provider side as the content request increases. As expected, these results validate the comparative efficiency of the delegation model in contrast to the Vanilla scheme.

VII. Conclusion

We proposed an authentication scheme to impose security strategies at the edge in CPS communication for IIoT such that it can provide secure communication for constrained devices. The central idea is to assimilate proxy signature and session connections on ICN architecture with the purpose of provisioning two-way authentication. Security analysis demonstrated that the proposed scheme maintained stronger defense compared with other competing schemes. We analyzed the computation and communication costs of the proposed scheme and illustrated that when the requested content grows, the proposed scheme requires an acceptable resource consumption compared to its competition. Using simulation, we displayed that the proposed delegation approach outperforms the Vanilla approach in terms of cost-effectiveness while reducing the workload on the provider side efficiently.

Even though our design provides a scalable resolution for device security in CPS, it is not apparent how to investigate its capabilities in a testing ground like waiting time and energy use between packets. A further limitation is the lack of the related pre-process data methods to enhance data transmission efficiency before authentication. Our scheme achieves secure authentication for IIoT in CPS based on edge assistance. However, these problems might be solved by ndnSIM and AI algorithms, and we take them as the future works.

Acknowledgment

We sincerely thank all the editors and anonymous reviewers for their valuable advice. Ding Wang is the corresponding author. This research is supported in part by the National Natural Science Foundation of China under Grant 61802276, by the Scientific Research Project of Tianjin Municipal Education Commission (2021KJ038), and by the Beijing-Tianjin-Hebei Basic Research Cooperation Program.

References

[1] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Sci. China Inf. Sci.*, vol. 65, 2022.

[2] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Trans Industr Inform.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.

[3] I. Akkaya, Y. Liu, and E. A. Lee, "Uncertainty analysis of middleware services for streaming smart grid applications," *IEEE Trans. Serv. Comput.*, vol. 9, no. 2, pp. 174–185, Mar./Apr. 2016.

[4] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[5] A. Karati, I. S. Hafizul, B. G. P., B. M. Z. Alam, V. Pandi, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2018.

[6] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 1, pp. 69–78, Aug. 2015.

[7] "Cisco annual internet report 2018-2023 white paper." [Online]. Available: http://www.cisco.com

[8] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architectur," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 181–192, Oct. 2007.

[9] G. Chandrasekaran, N. Wang, and R. Tafazolli, "Caching on the move: towards d2d-based information centric networking for mobile content distribution," in *Proc. Conf. Local Comput. Netw. (LCN)*, 2015, pp. 312–320.

[10] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2018.

[11] Y. Lu, G. Xu, L. Li, and Y. Yang, "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Syst J.*, vol. 13, no. 2, pp. 1454–1465, June 2019.

[12] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9390–9401, Sept. 2020.

[13] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Trans. Dependable Secure Comput.*, 2020, doi: 10.1109/TDSC.2020.3022797.

[14] A. Compagno, M. Conti, and R. Droms, "Onboardicng: a secure protocol for on-boarding iot devices in icn," in *Proc. 3rd ACM Conf. Inf.-Centric Netw.(ICN)*, 2016, pp. 166–175.

[15] Y. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for cyber-physical system communications," *IEEE Trans Smart Grid*, vol. 9, no. 4, pp. 2478–2487, Jul. 2018.

[16] T. Okamoto, A. Inomata, and E. Okamoto, "A proposal of short proxy signature using pairing," in *Int. Conf. Inf. Technol. Coding Comput.*, 2005, pp. 631–635.

[17] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in *Proc. 5th ACM Conf. Comput. Commun. Secur.*, 1998, pp. 83–92.

[18] H.-U. Park and I.-Y. Lee, "A digital nominative proxy signature scheme for mobile communication," in *Int. Conf. Inf. Technol. Commun. Secur.(ICICS)*, vol. 2229, 2001, pp. 451–455.

[19] Y. Qiu, M. Ma, and X. Wang, "A proxy signature-based handover authentication scheme for lte wireless networks," *J. Netw. Comput. Appl.*, vol. 83, pp. 63–71, Jan. 2017.

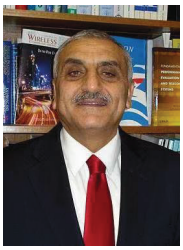
[20] Y. Lu, M. Zhang, and X. Zheng, "An authentication framework in icn-enabled industrial cyber-physical systems," in *4th EAI Int. Conf. Secur. Privacy New Comput. Environ.(SPNCE)*, ser. Lect. Notes Inst. Comput. Sci. Soc. Informatics Telecommun. Eng., vol. 344, 2021, pp. 223–243.

[21] X. Liu, M. Dong, K. Ota, P. Hung, and A. Liu, "Service pricing decision in cyber-physical systems: insights from game theory," *IEEE Trans. Serv. Comput.*, vol. 9, no. 2, pp. 186–198, Mar./Apr. 2015.

[22] M. Klumpp, "Innovation potentials and pathways merging ai, cps, and iot," *Appl. Syst. Innov.*, vol. 1, no. 1, pp. 1–5, 2018.
[23] N. Fulton and A. Platzer, "Safe ai for cps," in *Proc. Int. Test Conf.*, 2018, pp. 1–7.
[24] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-free physical layer authentication based on machine learning for industrial wireless cps," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6481–6491, Dec. 2019.
[25] R. Iqbal, F. Doctor, B. More, S. Mahmud, and U. Yousuf, "Big data analytics and computational intelligence for cyberphysical systems: recent trends and state of the art applications," *Future Gener. Comput. Syst.*, vol. 105, pp. 766–778, Apr. 2020.
[26] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep learning-dased ddos-attack detection for cyberphysical system over 5g network," *IEEE Trans. Industri. Inform.*, vol. 17, no. 2, pp. 860–870, Feb. 2021.
[27] A. N. Jahromi, H. Karimipour, A. Dehghantanha, and K.-K. R. Choo, "Toward detection and attribution of cyber-attacks in iot-enabled cyber-physical systems," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13 712–13 722, Sept. 2021.
[28] Q. Zheng, Q. Li, A. Azgin, and J. Weng, "Data verification in information-centric networking with efficient revocable certificateless signature," in *IEEE Conf. Commun. Netw. Secur.(CNS)*, 2017, pp. 1–9.
[29] C. Ghali, G. Tsudik, and E. Uzun, "In content we trust: network-layer trust in content-centric networking," *IEEE ACM Trans. Netw.*, vol. 27, no. 5, pp. 1787–1800, Oct. 2019.
[30] N. Fotiou and G. C. Polyzos, "Securing content sharing over icn," in *Proc. 3rd ACM Conf. Inf.-Centric Netw.(ICN)*, 2016, pp. 176–185.
[31] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for icn naming scheme," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 2, pp. 194–206, Mar./Apr. 2018.
[32] S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd, and H. Huang, "Accconf: an access control framework for leveraging in-network cached data in the icn-enabled wireless edge," *IEEE Trans. Dependable Secure. Comput.*, vol. 16, no. 1, pp. 5–17, Jan.-Feb. 2019.
[33] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of ndnsim: an open-source simulator for ndn experimentation," *SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 3, pp. 19–33, Sep. 2017.
[34] K. Xue, X. Zhang, Q. Xia, D. S. Wei, H. Yue, and F. Wu, "Seaf: a secure, efficient and accountable access control framework for information centric networking," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2018, pp. 2213–2221.
[35] Q. Feng, D. He, H. Wang, D. Wang, and X. Huang, "Multi-party signing protocol for the identity-based signature scheme in ieee p1363 standard," *IET Inf. Secur.*, vol. 14, no. 6, pp. 724–732, 2020.
[36] H. Yuan, X. Chen, J. Li, T. Jiang, J. Wang, and R. H. Deng, "Secure cloud data deduplication with efficient re-encryption," *IEEE Trans. Emerg. Topics Comput.*, vol. 15, no. 1, pp. 442–456, Jan.-Feb. 2022.
[37] I. O. Nunes and G. Tsudik, "Krb-ccn: lightweight authentication and access control for private content-centric networks," in *16th Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, ser. Lect. Notes Inst. Comput. Sci., vol. 10892, 2018, pp. 598–615.
[38] U. De Silva, A. Lertsinsrubtavee, A. Sathiaseelan, and K. Kanchanasut, "Named data networking based smart home lighting," in *Proc. ACM Conf. Special Interest Group Data Commun.*, 2016, pp. 573–574.
[39] T. Mick, R. Tourani, and S. Misra, "Laser: lightweight authentication and secured routing for ndn iot in smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 755–764, Apr. 2018.
[40] R. Kassab, O. Simeone, and P. Popovski, "Information-centric grant-free access for iot fog networks: edge vs. cloud detection and learning," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 10, pp. 6347–6361, Oct. 2020.
[41] M. Amadeo, G. Ruggeri, C. Campolo, A. Molinaro, and G. Mangiullo, "Caching popular and fresh iot contents at the edge via named data networking," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2020, pp. 610–615.
[42] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2019.
[43] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wählisch, "Information centric networking in the iot: experiments with ndn in the wild," in *Proc. 1th ACM Conf. Inf.-Centric Netw.(ICN)*, 2014, pp. 77–86.
[44] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "A secure icn-iot architecture," in *IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2017, pp. 259–264.
[45] M. Wang, C. Xu, X. Chen, H. Hao, L. Zhong, and D. O. Wu, "Design of multipath transmission control for information-centric internet of things: a distributed stochastic optimization framework," *IEEE Internet things J.*, vol. 6, no. 6, pp. 9475–9488, Dec. 2019.
[46] D. He, Y. Zhang, D. Wang, and K.-K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the ieee p1363 standard for public key cryptography," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 1124–1132, Sep./Oct. 2020.
[47] B. Ahlgren, P. A. Aranda, P. Chemouil, S. Oueslati, L. M. Correia, H. Karl, M. Sllner, and A. Welin, "Content, connectivity, and cloud: ingredients for the network of the future," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 62–70, Jul. 2011.
[48] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, "On preserving privacy in content-oriented networks," in *Proc. ACM SIGCOMM Workshop Inf.-Cent. Networking (ICN)*, Aug. 2011, pp. 19–24.
[49] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 870–885, Apr. 2019.
[50] Z. Ma, Y. Yang, X. Liu, Y. Liu, S. Ma, K. Ren, and C. Yao, "Emir-auth: eye movement and iris-based portable remote authentication for smart grid," *IEEE Trans Industr. Inform.*, vol. 16, no. 10, pp. 6597–6606, Oct. 2020.
[51] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 507–523, Jan.-Feb. 2022.
[52] X. Liu, R. H. Deng, K.-K. R. Choo, and Y. Yang, "Privacy-preserving outsourced support vector machine design for secure drug discovery," *IEEE Trans. on Cloud Comput.*, vol. 8, no. 2, pp. 610–622, Apr.-Jun. 2020.
[53] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Comput. Secur.*, vol. 88, p. 101619, 2020.
[54] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized fuzzy commitment based key agreement protocol for wireless body area network," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 2, pp. 839–853, Apr.-Jun. 2021.
[55] J.-S. Coron, "On the exact security of full domain hash," in *Proc. CRYPTO 2000*, vol. 1880, 2000, pp. 229–235.
[56] A. Mahanti, C. Williamson, and D. Eager, "Traffic analysis of a web proxy caching hierarchy," *IEEE Netw*, vol. 14, no. 3, pp. 16–23, May./Jun 2000.
[57] C. Fricker, P. Robert, J. Robert, and N. Sbihi, "Impact of traffic mix on cahing perfotmance in a content-centric network," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2012, pp. 310–315.
[58] "Java pairing based cryptography library (jpbc)." [Online]. Available: http://gas.dia.unisa.it/Projects /jpbc
[59] H. Che, Y. Tung, and Z. Wang, "Hierarchical web caching systems: modeling, design and experimental results," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 7, pp. 1305–1314, Sept. 2002.

Yanrong Lu received the M.S. degree from Xidian University, Xi'an, China, in 2012, and the Ph.D. degree from Beijing University of Posts and Telecommunications of China, Beijing, China, in 2017. She is currently with School of Safety Science and Engineering, Civil Aviation University of China, Tianjin, China. Her current research interests focus on information network and security.

Ding Wang (SM'14, M'17) received his Ph.D. degree in Information Security at Peking University in 2017, and currently, he is a full professor at Nankai University. As the corresponding author or first author, he has published more than 70 papers at venues like IEEE S&P, ACM CCS, NDSS, Usenix Security, IEEE TDSC and IEEE TIFS. His research has been reported by over 200 medias like Daily Mail, Forbes, IEEE Spectrum and ACM Technews, appeared in the Elsevier 2017 "Article Selection Celebrating Computer Science Research in China", and resulted in the revision of part of the authentication guideline NIST SP800-63-2. He has been invited as a TPC member for over 40 international conferences such as ACM CCS, ACSAC, PETS, AsiaCCS, and ISC. He has been given the ACM China Doctoral Dissertation Award (two winners each year), CCF Doctoral Dissertation Award, the INSCRYPT 2018 Best Paper Award, and the Outstanding Youth Award of China Association for Cryptologic Research. His research interests focus on Identity Security, including password, multi-factor authentication and cryptographic protocols.



Mohammad S. Obaidat (F'05) is an internationally well-known academic/researcher/scientist. He received Ph.D. and M. S. degrees in Computer Engineering from Ohio State University. He is currently Founding Dean and Professor, College of Computing & Informatics at University of Sharjah, UAE. Prior to joining University of Sharjah, he was an advisor to president of Philadelphia University, a president of SCS, a dean of the college of engineering at Prince Sultan University, a chair & professor at department of CIS and Fordham university, and a chair & professor at Monmouth University. He is the recipient of the PR of China Ministry of Education Distinguished Overseas Professor at the University of Science and Technology Beijing, China and the Honorary Distinguished Professor at the Amity University-A Global University.

He has received numerous research funding and authored/coauthored more than 95 books, 70 Book Chapters and about 1000 academic papers. Dr. Obaidat was the recipient of the IEEE Systems Journal Best Paper awards, in 2018, 2019 (2 Best Paper Awards) and 2020 (4 Best Paper Awards), respectively. He also was the recipient of many conference proceedings Best Paper awards like IEEE ICC, IEEE Globecom, AICSA, CITS, SPECTS, and DCNET. He is currently the founding Editor-in-Chief of Wiley Security and Privacy Journal. He is an Editor-in Chief of 3 academic journals and an editor of several journals. Dr. Obaidat is founder or co-founder of 5 International Conferences. He is chair of more than 160 international conferences and has given more than 160 presentations as the keynote speaker. He has served as ABET/CSAB evaluator and on IEEE CS Fellow Evaluation Committee.

Dr. Obaidat is the recipient of the 2018 IEEE ComSoc-Technical Committee on Communications Software 2018 Technical Achievement Award in Cybersecurity, Wireless Networks Computer Networks and Modeling and Simulation Award, SCS prestigious McLeod Founder's Award, Presidential Service Award, SCS Hall of FameLifetime Achievement Award for his contribution to modeling and simulation, outstanding visionary leadership and improving the effectiveness and broadening the applications of modeling and simulation worldwide, as well as the SCS Outstanding Service Award and the IEEE CITS Hall of Fame Distinguished and Eminent Award. He is a Life Fellow of IEEE and a Fellow of SCS.

Pandi Vijayakumar received the B.E. degree in Computer Science and Engineering from Madurai Kamaraj University, Madurai, India, in 2002, the M.E. degree in Computer Science and Engineering from the Karunya Institute of Technology, Coimbatore, India, in 2005, and the Ph.D. degree in Computer Science and Engineering from Anna University, Chennai, India, in 2013. He is the former Dean and currently an Assistant Professor with the Department of Computer Science and Engineering, University College of Engineering Tindivanam, Melpakkam, India, which is a constituent college of Anna University Chennai, India. He has seventeen years of teaching experience and he has produced four Ph.D. candidates successfully. He has also authored and co-authored more than 100 quality papers in various IEEE transactions/journals, ACM transactions, Elsevier, IET, Springer, Wiley and IGI Global journals. He is serving as Associate Editor in many SCI indexed journals namely International Journal of Communication Systems (Wiley), PLOS One, International Journal of Semantic Web and Information Systems (IGI Global), and Security and Communication Networks (Wiley—Hindawi). Moreover, He is serving as an Academic Editor in the International Journal of Organizational and Collective Intelligence (IGI Global), International Journal of Software Science and Computational Intelligence (IGI Global), International Journal of Cloud Applications and Computing (IGI Global), International Journal of Digital Strategy, Governance, and Business Transformation (IGI Global) and Security and Privacy (Wiley. He is also serving as a Technical Committee member in the journal Computer Communications (Elsevier). Recently, He was elevated to Editor-in-Chief Position in the journal Cyber Security and Applications (KeAi—Elsevier). Till now he has authored four books for various subjects that belong to the Department of Computer Science and Engineering. He is a senior member of IEEE. He is also listed in the world's Top 2% Scientists for citation impact during the calendar year 2020 by Stanford University.