Stateless Blockchain-Based Lightweight Identity Management Architecture for Industrial IoT Applications

Kening Zhang, Carman K. M. Lee, *Senior Member, IEEE*, and Yung Po Tsang, *Member, IEEE*

***Abstract*—The rapid development of the Industrial Internet-of-Things (IIoT) has led to an exponential growth in the deployment of industrial applications on user-owned smart devices, which poses significant challenges in identity management (IDM) concerning both privacy and quantity. The advent of blockchain technology can fulfill some of these requirements. However, as the number of identities in the IIoT environment grows exponentially, the storage occupied by nodes in the blockchain system gets larger gradually and can never be curtailed. In addition, to maintain the security of identity information, the characteristics of blockchain on openness and transparency are not appropriate for IDM. To this end, we propose a lightweight, secure, and trustworthy stateless blockchain-enabled IDM architecture for IIoT. Specifically, by incorporating the cryptographic accumulator with blockchain, the set of transactions can be turned into a length-constant proof that does not change when identities are modified, in which the identity information is concealed completely. Furthermore, the stateless blockchain structure is formulated and new consensus, identity modification and verification algorithms are presented. Then, we give a comprehensive threat model and security analysis of the proposed system. Finally, the experimental results demonstrate that total time cost and blockchain size are 130.25 ms and 100.13 MB, which significantly improves portability and efficiency in IIoT scenarios.**

***Index Terms*—Blockchain-based identity, identity management (IDM), Industrial Internet of Things (IIoT), LSTIDM-SB, stateless blockchain.**

I. Introduction

THE Industrial Internet of Things (IIoT) has emerged as a critical enabler for Industry 4.0, enabling intelligent and connected devices to improve productivity, quality, and safety in various industrial sectors, which creates a "digital transformation" of the factory as well as the supportability of infrastructure [1]. Such connectivity facilitates real-time monitoring, data analysis, remote control, and automation, which provides industrial enterprises with greater flexibility and efficiency.

Although the IIoT application has evolved at an increasing rate and made our lifestyles abundantly possible, the rapid proliferation of sensitive data generated by devices has raised significant concerns due to the security and privacy [2], [3]. For example, automated vehicles have currently grown into the Internet of Vehicles (IoV) [4], which provides numerous intelligent services in terms of route navigation, digital maps, and instant location. However, all kinds of data from users are collected and analyzed by the third-party institutions, such as Google, Apple, and Meituan [5]. When there is an information leakage, it will lead directly to privacy and personal safety issues. According to the identity (i.e. ID), path, and other private data of users, attackers can calculate the regular range of users, and thus predict the users' future locations and the occupations [6]. In practical applications, such privacy leakage issues have come up. To address this issue, a typical approach to maintain the location privacy is adopting anonymous credentials or pseudonyms to guarantee the anonymity of users [7].

It is still vulnerable to data tampering, even though identities can be anonymized. In addition, databases are subject to single points of failure in the centralized system, which incurs huge costs when they occur. Therefore, secure and effective identity management (IDM) is urgently needed, and blockchain technology can be a good solution. Blockchain has emerged as a prospective solution for decentralized identifiers (DID) in IIoT, which provides a distributed ledger that stores transactions in a secure and transparent manner. [8], [9], [10] have added various functions into blockchain-based IDM, such as selective revocation, traceability, etc. However, most classic blockchains are traditionally stateful and there is a corresponding index called state for the transaction validation in memory database, such as LevelDB and MongoDB. In the bitcoin system, the state is a set of immutable coins named unspent transaction outputs (UTXO), while the state is a set of variable accounts in the account-based system (i.e., Ethereum). Until now, the UTXO set in Bitcoin is around 4.3 GB and (includes 75 million transactions [11]) and grows in essence most recently, which is called state explosion problem. It is burdensome and high-cost to locally maintain this

Manuscript received 24 July 2023; revised 21 November 2023; accepted 8 February 2024. Date of publication 18 March 2024; date of current version 5 June 2024. This work was supported by Research Institute for Advanced Manufacturing, The Hong Kong Polytechnic University (Project code: 1-CD4E). Paper no. TII-23-2775. *(Corresponding author: Carman K. M. Lee.)*

The authors are with the Department of Industrial and Systems Engineering, Research Institute for Advanced Manufacturing, The Hong Kong Polytechnic University, Hong Kong 999077 SAR, China (e-mail: kenzhang@polyu.edu.hk; ckm.lee@polyu.edu.hk; yungpo.tsang@polyu.edu.hk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2024.3367364.

Digital Object Identifier 10.1109/TII.2024.3367364

kind of growing sets in the system. In contrast, the stateless blockchain employs cryptographic accumulator and only needs a commitment which is length-constant no matter how many elements there are in abovementioned sets. Only an additional proof along with the transaction is required, so that validators can validate one transaction with the membership or nonmembership proof based on the commitment to judge whether it is legal. The advantage is clearly indicated that it is lightweight enough for light nodes with insufficient storage resources, such as mobile wallets and industrial machines, to complete validation independently without requesting from full nodes or worrying about insufficient storage resources. On top of that, the original information is not leaked from the commitment after being accumulated [12].

As identity information is growing in huge volumes, the storage of traditional blockchain-based IDM suffers from the problem of exponential explosion, which has a significant impact on resource-constrained devices. But existing accumulators, such as the Merkel tree-based accumulator, have high computational complexity and cannot match the industrial demand. Second, IDs belong to sensitive information compared with other data and identity verification should be carried out without using plaintext. Furthermore, only the full node can process independent verification in the traditional blockchain system, and light nodes need to request information from the full node. This way can cause new security risks, like long-range attacks [13], so independent authentication is highly desirable to to ensure adaptation to various industrial scenarios. Finally, current IDM architecture needs to meet blindness, unforgeability, traceability, unlinkability, revocability, antiattack capability, lightweight, trustworthiness, and efficient verifiability simultaneously.

For more effective solutions to these problems, a generic topology of identity authentication in the IIoT ecosystem is first defined as Fig. 1. The whole process can be divided into four parts: identity providers (IP), identity verifiers (IV), resource owners (RO), and the trust system (TS). The RO passes official files (i.e., license, ID card, and account) to IP and obtains homologous conforming identities, attributes, secret keys, and credentials. At once, IP records these data into the TS, which can be a centralized database or decentralized ledger. Then, if RO wants to apply for the permission of entrance or service, IV can ask TS for verification presentation and the operation of RO will be allowed when meeting the requirements. For instance, we give an actual scenario in Fig. 1. There is a truck owned by Factory A transporting appointed industrial products to a destination and needing to get the entrance permission. The factory distributes the licence to the truck and the trust system, respectively, and the entrance guard of destination will let the truck pass once the data in the system has been verified. Then, we naturally propose one new stateless blockchain-based IDM architecture for IIoT with the RSA-based accumulator in such a topology.

In this article, we critically reviewed the abovementioned goals and our major contributions are as follows.

1) We present a RO-IP-TS-IV topology and give a common instance in IIoT, so that LSTIDM-SB, a lightweight, secure, and trustworthy IDM architecture enabled by stateless blockchain is proposed relying on this topology. It holds *blindness, unforgeability, traceability, unlinkability, revocability, anti-attack capability, lightweight, trustworthiness,* and *efficient verifiability* simultaneously, in which World Wide Web Consortium (W3C) DID standard [14] is also adopted, and therefore future applications can utilize this architecture for updating on the Internet sustainably.
2) The proposed system is based on stateless blockchain technology integrated with RSA-based accumulator, which makes existent identity set (EIDS) a length-constant identity commitment (IDC) and add it into the block header, so that storage does not grow exponentially with the increasing of data.
3) We suggest a new consensus algorithm for stateless blockchain (SPoW), ID modification and validation algorithm with NI-PoE proofs, the noninteractive protocol using the Fiat–Shamir heuristic [15], and new algorithms allow efficient block creation and validation.
4) A comprehensive threat model and security analysis are presented specifically to prove the reliability of the system, and we demonstrate the superior performance of LSTIDM-SB compared with other [9] and [10] from several evaluation metrics.

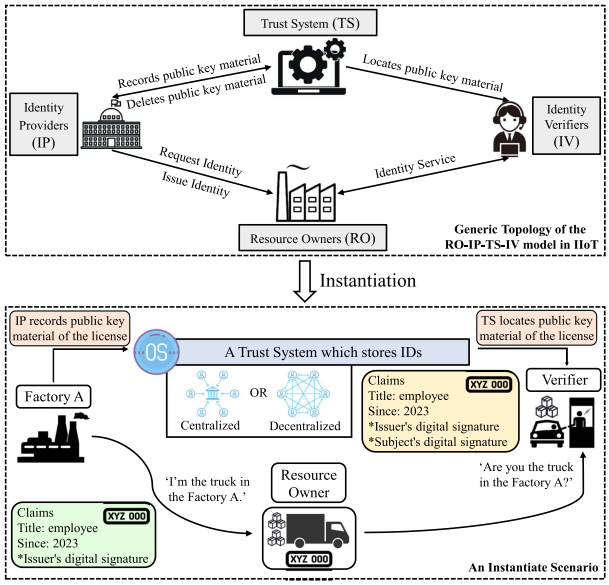

Fig. 1. Generic RO-IP-TS-IV model and an instance. RO owns the IDs, IP gives credentials, TS stores information, and IV verifies ID credentials. The instance is an industrial application.

The rest of this article is organized as follows. In Section II, we offer an overview of the existing research on blockchain-based IDM systems tailored for IIoT. Section III presents preliminaries of mathematical and cryptographic theories. Section IV outlines the design goals and entire model of the system architecture. The protocol procedure of LSTIDM-SB and technical specifications of stateless blockchain are expressed in Section V. In Section VI, lemmas and proofs are rigorously given for security analysis of the proposed system. Then, the performance of experiments is comprehensively analysed in Section VII.

TABLE I
COMPARISON WITH RECENT RELATED WORK

	LSTIDM-SB (ours)	PBIDM (2023) [9]	TAB-SAPP (2023) [8]	Candid (2021) [16]	Y. Yu et al.(2020) [10]	DIMS (2020) [17]	Coconut (2019) [18]	Y. Zhou et al. (2019) [19]
Blindness	√	√	√	√	√	√	√	√
Unlinkability	√	√	√	√	√	√	√	√
Unforgeability	√	√	√	√	√	√	√	√
Traceability	√	√	×	×	×	×	×	×
Revocability	√	√	×	×	√	×	×	×
Efficient Verifiability	√	×	×	×	×	×	×	×
W3C DID Standard	√	√	×	×	×	×	×	×
Trustworthiness	√	√	√	×	×	×	×	×
Anti-attack Capability	√	×	×	√	×	×	×	×
Lightweight	√	×	√	×	×	√	×	×

Note: Symbols " √ " indicates the method satisfies the corresponding feature and "×" means the feature is unsatisfied.

Finally, Section VIII concludes this article by summarizing the contributions made and highlighting potential avenues for future research.

II. Related Work

For privacy-preserving IDM, numerous anonymous authentication methods have been proposed gradually. Chaum [7] presented that anonymous credential is a predominant technology in anonymous authentication. In [20], a group member was permitted to sign a message to represent it, which do not revealed related identity information of the genuine signer. Many common applications adopt CL signatures [21] for anonymous credentials, such as electronic cash [22]. A more effective method named Pointcheval–Sanders (PS) signature that only included two elements was introduced in [23]. A threshold issuance selective disclosure credential named Coconut was suggested by Sonnino et al. [18], which utilized the PS signature. Zhou et al. [19] proposed a privacy-preserving authentication framework with key agreement for the sustainable IoT. For the anonymous authentication enabled by blockchain, Yu et al. [10] first gave a model with selective revocation for the industry. Lightweight and communication security in the Internet are urgently needed with the development of IoT, which can significantly reduce the number of attacks [3]. Maram et al. [16] proposed a decentralized IDM that can meet antiattack capability and recovery. However, it depends on the Oracle system not blockchain for credentials. Deebak et al. [8] designed a lightweight IDM with crypto-operations and the communication cost for massive industrial IoT-applications, which provides a reliable transmission rate and improves the connectivity of users. The development of standards for distributed digital ID, including verified credentials (VC), verified presentation (VP) and distributed identifiers, has been led by the global standards organization W3C. Then, W3C approved related reports for data model implementation. Microsoft established the blockchain-based identity authentication [24]. IBM proposed the blockchain system for digital identity and credentials [25], which explored the next evolution of digital identity. Bao et al. [9] presented a privacy-preserving blockchain-based IDM scheme enabled with W3C, traceability, and revocability. Yet, efficient verifiability, antiattack capability, and lightweight storage are not considered in the blockchain-based system.

Here, we present a comparison of some recent works that are similar to LSTIDM-SB in the Table I. As for blindness, unlinkability, and unforgeability, all following works can achieve these goals. For state-of-the-art systems, PBIDM [9] realized both traceability and revocability, and it is supported by this W3C DID standard, while Yu et al. [10] work only satisfies revocability. TAB-SAPP [8] can realize lightweight and trustworthiness. Candid [16] does not adopt blockchain and can only support sybil-resistance. No work considered efficient verification of IDM, but it is urgently needed in the fast-moving IIoT. Only LSTIDM-SB enables efficient verifiability and comprehensive threat analysis for antiattack capability. In addition, the proposed system implements all the features in Table I at the same time, which has not been achieved in previous works.

III. Preliminaries

In this section, we review following cryptographic primitives utilized in LSTIDM-SB, which includes bilinear map, identity-based encryption (IBE), zero knowledge proof, cryptographic assumptions, RSA accumulator, elliptic curve (EC) cryptography, and EC digital signature.

A. Bilinear Map

Let ρ be a prime number. Let $\mathbb{G}_x$ and $\mathbb{G}_y$ be an additively written group of order ρ with identity ∞, and let $\mathbb{G}_T$ be a multiplicatively written group of order ρ with identity $1_{\mathbb{G}_T}$. A bilinear pairing on $(\mathbb{G}_x, \mathbb{G}_y, \mathbb{G}_T)$ is a map $e : \mathbb{G}_x \times \mathbb{G}_y \to \mathbb{G}_T$. The bilinear map should satisfy the following properties:

1) *(Bilinearity):* For all $m \in \mathbb{G}_x, n \in \mathbb{G}_y$, and $i, j \in \mathbb{Z}_\rho$, $e(m^i, n^j) = e(m, n)^{ij}$.
2) *(Nondegeneracy):* For all generators $g_x =< \mathbb{G}_x >, g_y =< \mathbb{G}_y >, e(g_x, g_y) \neq 1_{\mathbb{G}_T}$.
3) *(Computability):* $e(g_x, g_y) \in \mathbb{G}_T$ can be efficiently computed.

B. Identity-Based Encryption (IBE)

By using the IBE scheme, one can encrypt directly relevant messages easily, instead of a complicated public key which is hard to remember or type in correctly. A highly effective IBE scheme was proposed by Boneh and Franklin [26], in which a private key generate (PKG) was introduced, and the IP issued

secret keys to ROs based on their data. This PKG held a master secret key (MSK) msk $\in \mathbb{Z}_p$ with an associated master public key (MPK) mpk $= g_x^s$, where $< g_x >= \mathbb{G}_x$.

C. Zero-Knowledge Proof

In [27], a zero-knowledge proof of knowledge (ZKPoK) protocol was presented that the prover trusted a statement from a verifier, and the verifier got nothing except the validity of the statement. A typical kind of ZKPoK protocols is the three-round Σ protocol [17]. For simplicity, ZKPoK$\{(x) : y = g^x\}$ represents a ZKPoK protocol that proves the knowledge of $x \in \mathbb{Z}_q$ such that $y = g^x$. Then, a series of relation instances are proved, e.g., ZKPoK$\{(a, b) : h = g_a^1 g_b^2\}$ and ZKPoK$\{(a) : h = g_a^1 \wedge t \neq g_1^a\}$.

D. Cryptographic Assumption (CA)

There are several CAs utilized in hidden-order groups. Let $\mathbb{G}_?, |\mathbb{G}_?|$, and $1_{\mathbb{G}_?}$ denote a generic hidden-order group, the order, and the identity element in such a group. Specifically, the RSA group is defined as $\mathbb{G}_? = \mathbb{Z}_N^*$, in which $\mathbb{Z}_N^* = \{0 < x < N | \gcd(x, N) = 1\}$ and $|\mathbb{Z}_N^*| = \phi(N) = (p-1)(q-1)$[28]. $Pr[\ldots] = \text{negl}(\lambda)$ is regularly expressed as for all polynomial probabilistic time adversaries $\mathfrak{A}$, there exists a negligible function negl(.) such that $Pr[\ldots] = \text{negl}(\lambda)$. There are theorems including factoring, discrete logarithm [29], and RSA assumption [30].

1) *(Factoring):* From group theory, there is an axiom for factoring an integer.

$$Pr\left[\begin{array}{c} p, q \xleftarrow{\$} \text{Primes}_{\text{poly}(\lambda)}, \\ N = pq : \\ (p, q) \leftarrow \mathfrak{A}(N) \end{array}\right] \leq \text{negl}(\lambda). \quad (1)$$

2) *(Discrete Logarithm):* [29] demonstrated that factoring N reduces to computing discrete logs in $\mathbb{Z}_N^*$.

$$Pr\left[\begin{array}{c} \mathbb{G}_? \leftarrow \text{GenGroup}_?(\lambda), \\ (g, h) \xleftarrow{\$} \mathbb{G}_? \times \mathbb{G}_?, \\ \ell \leftarrow \mathfrak{A}(\mathbb{G}_?, g, h) : \\ g^\ell = h \end{array}\right] \leq \text{negl}(\lambda). \quad (2)$$

3) *(RSA Assumption):* The assumption is explained by Rivest et al. [30] on public-key cryptosystems.

$$Pr\left[\begin{array}{c} \mathbb{G}_? \leftarrow \text{GenGroup}_?(\lambda), \\ (g, h) \xleftarrow{\$} \mathbb{G}_? \times \mathbb{Z} \ \gcd(\ell, |\mathbb{G}_?|) = 1, \\ u \leftarrow \mathfrak{A}(\mathbb{G}_?, g, \ell) : \\ g^{1/\ell} = u \end{array}\right] \leq \text{negl}(\lambda). \quad (3)$$

E. RSA-Based Accumulator

Let $A_T = \{x_1, x_2, \ldots, x_n\}$ and let $p_j = \text{Hash}(x_j)$ be the prime representative of x_j. The accumulator of A_T is: $\alpha = g^{\prod_{j\in[n]} p_j}$ and it can be computed in $O(n)$ exponentiations in $\mathbb{G}_?$.

A membership witness ω_j can be computed by: $\omega_j = g^{\prod_{j\in[n]\setminus\{j\}} p_j} = \alpha^{1/p_j}$. The verification of the witness against the accumulator α can be: $\alpha = \omega_j^{p_j}$. To precompute all membership witnesses fast, every p_jth root of α (i.e., $g^{p_1 p_2 \cdots p_j \cdots p_{n-1} p_n}$) can be represented by the algorithm RootFactor() in Boneh et al. [12], [31]: RootFactor$(g, (p_j)_{i\in[n]}) = (p_j)_{j\in[n]} = (\alpha^{1/p_j})_{j\in[n]} = ((g^{\prod_{i\in[n]} p_i})^{1/p_j})_{j\in[n]}$.

F. Elliptic Curve Cryptography (ECC)

ECC is a public key cryptosystem working on the basis of the EC theory [32]. The EC is a plane curve over a finite field, which is composed of the points, which follow the equation: $M^2 = N^3 + uN + v$. ECC is secure as there is a very long time determining the discrete logarithm of a random EC at any given point [33]. The group structure is inherited from the divisor group of the underlying algebraic variety: $\text{Div}^0(E) \rightarrow \text{Pic}^0(E) \simeq E$. ECC shows that it also spends a very long time to decide the discrete logarithm of a stochastic EC at an arbitrary given point.

G. EC Digital Signature

We briefly review the elliptic curve digital signature algorithm (ECDSA) [34], which is widely used in applications for high-speed realization due to its short length, small storage, and fast computation. An entity X's key pair is associated with a particular set of EC domain parameters $P^g = (a_0, b_0, G_p, N_0, h, q, F^g)$, a message $\check{M}$ and the key pair (Kp_i, Kp_p). For signature generation, randomly choose an integer $k_{N_0} (0 < k_{N_0} < N_0)$, compute $k_{N_0} G_p = (x_g, y_g)$, $r_g = x_g \bmod N_0$, $k_{N_0}^{-1} \bmod N_0$, $SHA\_256(\check{M})$, $s_{\mathcal{D}} = k_{N_0}^{-1}(e + r_g Kp_i) \bmod N_0$ and get the signature $(r_g, s_{\mathcal{D}})$ of the message $\check{M}$. For signature verification, Compute $SHA\_256(\check{M})$, $u_g = s_{\mathcal{D}}^{-1} \bmod N_0$, $f_1 = eu_g \bmod N_0$, $f_2 = r_g u_g \bmod N_0$, $X = f_1 G_p + f_2 Kp_p$, $v_{\mathcal{D}} = \overline{x_g} \bmod N_0$, and accept the signature if and only if $v_{\mathcal{D}} = r_g$. There is no sub exponential-time method that can address ECC problem, so that the robustness of the strength-per-key-bit will increase significantly.

IV. Design of LSTIDM-SB

A. Design Goals

We have integrated stateless blockchain into the identity system and achieved design requirements of *blindness, unforgeability, traceability, unlinkability, revocability, antiattack capability, lightweight, trustworthiness, and efficient verifiability*.

1) *Blindness:* This feature requires the IP to make it difficult to speculate about the ROs anything when issuing identity credentials.
2) *Unforgeability:* No other institution can provide legal and valid identity credentials other than the IP.
3) *Traceability:* The IP can recover RO's identities and track the process of addition and revocation from the identity system.
4) *Unlinkability:* Similar to the first property, but it is the IV, not the IP, that has difficulty in obtaining information about RO's identities.

5) *Revocability:* When a malicious identity is traced, the system can revoke the related data to prevent it from continuing to get verification.
6) *Antiattack Capability:* The blockchain-enabled system should have the ability to tolerate and resist malicious nodes and ensure its availability and serviceability.
7) *Lightweight:* The classic blockchain system requires the maintenance of the UTXO, which causes exponential growth of the storage. Lightweight means that the proposed system only requires a constant-length IDC instead of the ever-increasing UTXO, so that the storage will be significantly reduced.
8) *Trustworthiness:* Due to the IDC in the blockchain system, no identity information can be obtained when entire data of the blockchain is publicly verified.
9) *Efficient Verifiability:* Efficient verifiability requires that IV can verify RO's identities by using the IDC anywhere even when original identities are lost. That is, light nodes, i.e., smart devices, personal computer, and industrial machines can complete verification without requesting extra hash trees from full nodes.

B. Data Structure

In LSTIDM-SB, we give our simple DID string consisting of three components: 1) the DID URI scheme, 2) proposed method LSTIDM-SB, and 3) the specific identifier.

The identity document includes ID $\mathbb{D}$, attributes $\mathbb{A}$, other authentication information. Since the stateless blockchain is powered by the RSA-based accumulator, which only provides commitment and not reveal private identity credentials, we collectively regard both public and private identity credentials as $\mathbb{D}$. All the information is stored in the InterPlanetary File System (IPFS), while the record and commitment are uploaded to the blockchain. Due to the nature of the RSA-based accumulator, the commitment can only be utilized for verification and identities can not be compromised.

VC issues descriptive declarations to endorse certain attributes and attaches identity's digital signature to prove the authenticity of those attributes. For privacy reasons, the full content of VC cannot be displayed, so that only certain attributes need disclosing selectively. VP means complete or partial data of VC, which can satisfy privacy expectations.

All documents comply with W3C standards, and detailed descriptions are shown in Fig. 2.

C. System Model

LSTIDM-SB involves three layers: application layer, encryption, and verification layer, stateless blockchain-based IDM layer as shown in Fig. 3.

1) *Application Layer:* Resource owners include smart houses, smart devices, industrial machines, users, etc., and they can issue identity credentials from the identity provider (phase 1). Identity verifiers, e.g., applications, access control, then give permissions to RO after completing verification on the blockchain system (phase 5).

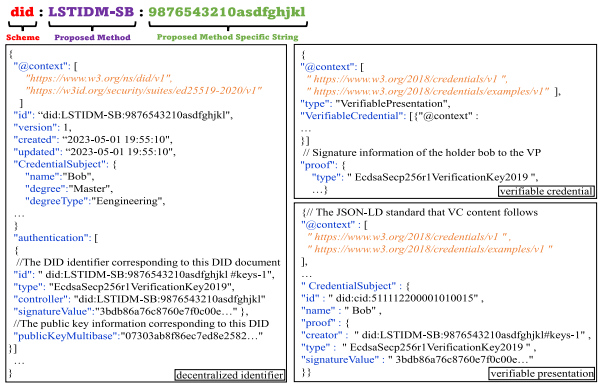

Fig. 2. Data structure of RO, including DID, verifiable credential and verifiable presentation. The code on top of the picture consists of the ID scheme, proposed protocol, and specific string.

2) *Encryption and Verification Layer:* Upon receipt of the RO's request, the identity provider creates a legitimate VC of the identity, composed of credential metadata, claims and proofs, and adds data to the next layer. When authentication is requested, the system gives the verifiable presentation to the IV, which is partial data of the VC, i.e., presentation metadata, VC, and proofs (phase 3 and 4).
3) *Stateless Blockchain-based IDM Layer:* First, identity credentials received from the IP are recorded in the IPFS (phase 2). In the meanwhile, the record can be added on the blockchain as a transaction after hash encryption. Additionally, by adopting RSA-based accumulator, EIDS in the IPFS is completely converted to a constant-length IDC, which becomes a part of the block header and be updated when each block is miner. If the IV asks for verification from the blockchain system, full nodes, and light nodes can both support the command independently with IDC in the block header.

V. Development of LSTIDM-SB

A. IDM Protocol

The proposed LSTIDM-SB is structured in eight main phases, including *{SysSetup, SysKeyGen, IdIssue, IdProve, IVVerify, IdTrace, IdRecover, IPRevoke}*, which utilizes IBE, ZKPoK, and ECDSA. The detailed procedures are as follows. For clearer description of choice in each step, the whole flowchart is illustrated as Fig. 4.

1) *SysSetup:*
a) Initially, the IP generates an ID security parameter for cyclic groups $(\mathbb{G}_x, \mathbb{G}_y, \mathbb{G}_T)$ of order ρ. Denote the bilinear map as $e : \mathbb{G}_x \times \mathbb{G}_y \to \mathbb{G}_T$, and generators are g_x and g_y, where $g_x =< \mathbb{G}_x >, g_y =< \mathbb{G}_y >$, respectively.
b) Set the hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_\rho$ and $\mathcal{H}_x : \mathbb{G}_x \to \mathbb{G}_x$. A parallel copy of the parameters $(\mathbb{G}_x, \mathbb{G}_y, \mathbb{G}_T, \rho, e, g_x, g_y)$ is stored in IPFS and blockchain.

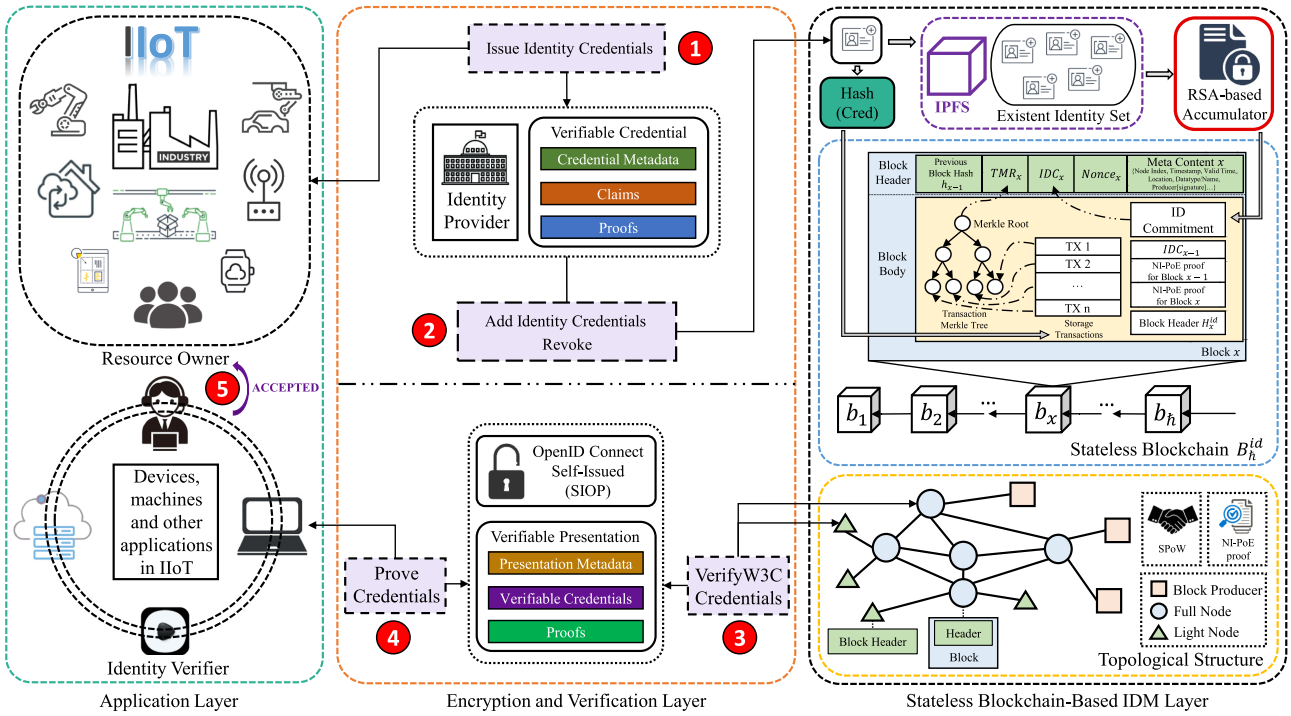

Fig. 3. System architecture of LSTIDM-SB, including three layers: application layer, encryption and verification layer and stateless blockchain-based IDM layer, and five phases: issue ID, add ID to TS, verify credentials, prove credentials, and accept ID.

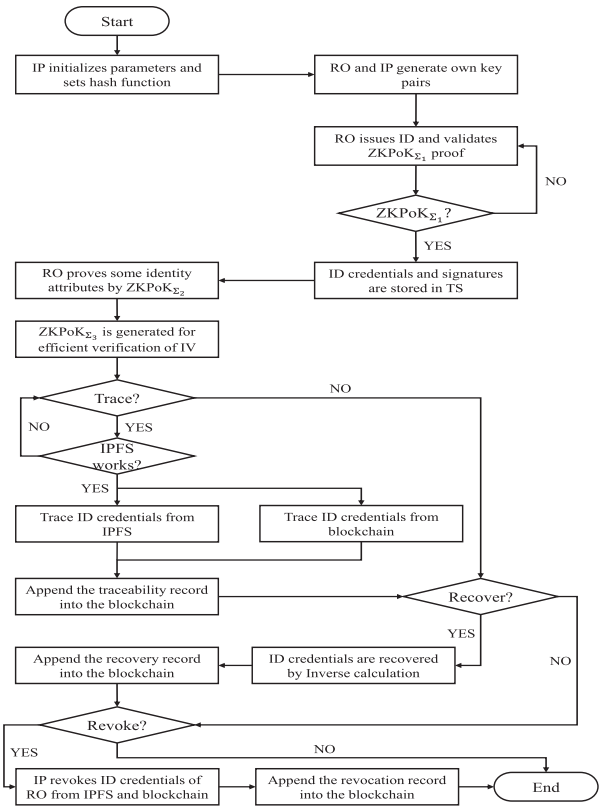

Fig. 4. Whole flowchart of proposed LSTIDM-SB, including the normal processing flow and the other special functions for ID credentials, i.e., traceability, recovery, and revocation, which can be chosen to be executed or not.

2) *SysKeyGen:*

a) ORKGen: The RO generates a key pair (κ_s^i, κ_p^i) when the ith identity $(i \in \mathbb{N}^+)$ needs adding, where $\kappa_s^i \in \mathbb{Z}_\rho$ and $\kappa_p^i = \text{hash}(\kappa_s^i)$. κ_p^i are put in IPFS and blockchain.

b) IPKGen: The IP randomly selects $\widehat{g}_0 =< \mathbb{G}_x >$, $\mathfrak{a}, \mathfrak{b} \in \mathbb{Z}_\rho$, $z_1, \ldots, z_{2I} \in \mathbb{Z}_\rho$ (I represents the number of ROs), and calculate $\mathcal{A} = g_x^{\mathfrak{a}}$, $\mathcal{B} = g_x^{\mathfrak{b}}$, $\widetilde{\mathcal{A}} = g_y^{\mathfrak{a}}$, $\widetilde{\mathcal{B}} = g_y^{\mathfrak{b}}$, $\Omega = \widehat{g}_0^{\prod_{j=1}^{2I}(\mathfrak{b}+z_j)}$. Then, the key pair can be denoted as $\kappa_s^{\text{IP}} = (\mathfrak{a}, \mathfrak{b})$, $\kappa_p^{IP} = (g_y, \mathcal{B}, \widetilde{\mathcal{A}}, \widetilde{\mathcal{B}})$. κ_p^{IP}, $\widehat{g}_0$, Ω and an empty list CRL is published in IPFS and blockchain.

3) *IdIssue:*

When an identity is requested, the RO interacts with the IP through the following substeps.

a) The ith identity $\mathbb{D}_i$ includes attributes $\mathbb{A}^i = \{\lambda_1^i, \lambda_2^i, \ldots, \lambda_{L_i}^i\}$, where $i, L_i \in \mathbb{N}^+$, and for $l \in \{1, 2, \ldots, L_i\}$, $\lambda_l^i \in \mathbb{Z}_\rho$. Denote $\mathbb{A}_s^i$ as a subset of $\mathbb{A}^i$, which means $\mathbb{A}_s^i \subseteq \mathbb{A}^i$, and then the RO can select $\mathbb{A}_s^i$ for the interaction. Randomly pick a parameter $\mu_i \in \mathbb{Z}_\rho$, and computes $T_i = g_x^{\mu_i} \mathcal{B}^{\prod_{\lambda \in \mathbb{A}_s^i} \lambda}$, $\widetilde{T}_i = \widetilde{\mathcal{B}}^{\prod_{\lambda \in \mathbb{A}_s^i} \lambda}$.

b) Send μ_i to the IP, generate the following proof based on ZKPoK, and put T_i on blockchain in the TS:

$$\Theta = \text{ZKPoK}_{\Sigma_1}\{(\mu_i, \mathbb{A}_s^i) : T_i = g_x^{\mu_i} \mathcal{B}^{\prod_{\lambda \in \mathbb{A}_s^i} \lambda} \wedge \widetilde{T}_i = \widetilde{\mathcal{B}}^{\prod_{\lambda \in \mathbb{A}_s^i} \lambda}\}. \quad (4)$$

c) After validating Θ, error is returned to the RO if the result is invalid. If Θ is true, and obtain $P_i^g =$

$(z_i)^{-1}(\text{SHA\_256}(T_i)+\kappa_p^i \times R_i) \bmod \rho$ according to ECDSA, where $R_i^3+uR_i=(\mu_i^*\widehat{g_0})^2-v,\ u,v\in\mathbb{N}^+$. Randomly choose $\omega_i\in\mathbb{Z}_\rho$ to get $U_i=T_i\mathcal{B}^{z_i}$, $M_i=g_x^{\omega_i}$, $N_i=(\mathcal{A}U_i)^{\omega_i}$, and compute a witness $W_i=\Omega^{\frac{1}{z_i+\mathfrak{b}}}$. Then, the quaternion (M_i,N_i,W_i,z_i) is sent to the RO and $(i,\widetilde{T}_i,z_i)$ is stored in the list Φ locally.

d) Upon receiving (M_i,N_i,W_i,z_i), the RO works out $\hat{\mu}_i=\mu_i+z_i$ and $N_i^*=N_iM_i^{-\mu_i}$. The identity credential can be represented as $\mathbb{D}_i=(\hat{\mu}_i,M_i,N_i^*,W_i,z_i)$, which is put in Φ.

4) *IdProve:*
To prove identity attributes $\mathbb{A}^i$, the RO needs to select two parameters $\varepsilon_i,\delta_i\in\mathbb{Z}_\rho$, and calculate $P_i=M_i^{\varepsilon_i}, Q_i=N_i^{*\delta_i}, V_i=g_y^{\varepsilon_i}\widetilde{\mathcal{A}}\widetilde{\mathcal{B}}^{\hat{\mu}_i}, E_i=P_i^{\varepsilon_i}$ so that another ZKPoK $\beth$ proof can be generated as

$$\begin{aligned}\beth=\text{ZKPoK}_{\Sigma_2}\{(\hat{\mu}_i,\varepsilon_i,W_i,z_i):V_i=g_y^{\varepsilon_i}\widetilde{\mathcal{A}}\widetilde{\mathcal{B}}^{\hat{\mu}_i}\wedge E_i\\ =P_i^{\varepsilon_i}\wedge e(\Omega,g_y)=e(W_i,\widetilde{\mathcal{B}}g_y^{\mu_i})\}.\end{aligned}\tag{5}$$

5) *IVVerify:*
For easier verification, randomly select $c_\tau\in\mathbb{Z}_\rho$ and compute $f_1=\widetilde{\mathcal{B}}^{c_\tau}, f_2=W_ig_x^{c_\tau}, f_3=c_\tau z_i$, so that ZKPoK_{Σ_2} $\beth$ can be transformed into another ZKPoK_{Σ_3} $\aleph$ with these intermediate parameters.

$$\begin{aligned}\aleph=\text{ZKPoK}_{\Sigma_3}\{(\hat{\mu}_i,\varepsilon_i,c_\tau,f_3,z_i):V_i=\widetilde{\mathcal{A}}\widetilde{\mathcal{B}}^{\hat{\mu}_i}g_y^{\varepsilon_i}\wedge\\ E_i=P_i^{\varepsilon_i}\wedge f_1=\widetilde{\mathcal{B}}^{c_\tau}\wedge\frac{e(f_2,\widetilde{\mathcal{B}})}{e(\Omega,g_y)}=\frac{e(g_x,f_1g_y^{f_3})}{e(f_2,g_y)^{z_i}}\}.\end{aligned}\tag{6}$$

6) *IdTrace:*

a) If the IPFS is working and not under attack, the identity $\mathbb{D}$ can be acquired directly in the local list Φ.

b) If all nodes in IPFS are failed, the IP can track the identity $\mathbb{D}$ from the blockchain system. When tracing request $\Lambda^T=\{\mathbb{D}_i,\kappa_p^{IP}\}$ is sent to the system, headers are traversed through the IDC $g^\Lambda=\widehat{g_0}^{\prod_{l=1}^{L_i}\lambda_l^i}$ from the latest generated block to oldest.

7) *IdRecover:* If identities are lost or erroneously revoked, the system can recover them. When RO i sends a recovering request $\Lambda^R=P_i,\ \mathcal{H}_x(P_i)^{\hat{\mu}_i}$, the IP verifies whether $e(\mathcal{H}_x(P_i)^{\hat{\mu}_i},\widetilde{\mathcal{B}})=e(\mathcal{H}_x(P_i),\widetilde{T}_i\widetilde{\mathcal{B}}^{\prod_{\lambda\in\mathbb{A}^i}\lambda})$. If the result is unequal, error is returned to the IP break the process. Conversely, the IP choose z_{i+I} to calculate $O_i=P_i^{\mathfrak{b}}$ and $W_{z_{i+I}}=(z_{i+I})^{-1}(\text{SHA\_256}(T_{i+I})+\kappa_p^{i+I}\times R_{i+I}) \bmod \rho$. Then, the IP sends $(O_i,W_{z_{i+I}},z_{i+I})$ to the RO i and substitutes z_{i+I} for z_i. Randomly choose $\eta\in\mathbb{Z}_\rho$ and calculate $V_i=O_i^{\eta(z_{i+I}-z_i)}Q_i^\eta$, $U_i=P_i^\eta$ and $\xi_i=(\hat{\mu}_i+z_{i+I}-z_i) \bmod \rho$ to recover the identity credential of the RO i, denoted as $(\xi_i,U_i,V_i,W_{z_{i+I}},z_{i+I})$.

8) *IPRevoke:* The IP revokes the identity credential of the RO i with z_{i+I} and $\widetilde{T}_i$ on stateless blockchain, and the system updates CRL with the formula CRL $\longleftarrow$ CRL $\cup$ z_{i+I}. Simultaneously, the IV verifies whether $e(V_i,g_y)=e(U_i,\widetilde{\mathcal{A}})e(U_i,\widetilde{T}_i\widetilde{\mathcal{B}}^{z_{i+I}})$ for confirmation of the revocation.

B. Stateless Blockchain for IDM

There are many accumulators available to construct stateless blockchains, such as Merkel tree-based accumulators. However, the complexity of Merkel tree-based accumulator is $O(\log_2\tilde{}N)$ and N is the size of the EIDS. Second, updating the proof consumes a lot of bandwidth resources. Other cryptographic accumulators do not support batch processing while deleting elements is too costly. Only the RSA-based accumulator enables batch processing and can add and remove elements efficiently. Also, RSA-based accumulators are used in blockchain-based on complete mathematical theory [11], while other accumulators are not rigorously proven to be properly utilized in blockchain systems. Meanwhile, RSA's accumulator is a standardized cryptographic algorithm, so the proposed framework can be seamlessly integrated with existing IDM systems.

1) Block Structure: When the height of the blockchain is $\hbar$ ($\hbar\in\mathbb{N}^+$), denote it as $B_\hbar^{\text{id}}$ with a vector, and each element b_x ($x\in 1,2,\ldots,\hbar$) is a set. $B_\hbar^{\text{id}}=(b_1,b_2,\ldots b_x,\ldots,b_\hbar)$, where

$$b_x=\{H_x^{\text{id}},T_x^{\text{id}},(\text{IDC}_{i-1},\pi_\beta^{\text{del}},\pi_\alpha^{\text{add}})\}.\tag{7}$$

The first element H_x^{id} is block header of each block b_x, and second is $T_x^{\text{id}}=\{t_1,t_2,\ldots,t_{|T_x^{\text{id}}|}\}$, which includes all transactions representing identity storage records

$$H_x^{\text{id}}=(h_{x-1},\text{TMR}_x,\text{IDC}_x,\text{nonce}_x,\text{MC}_x)\tag{8}$$

where, $h_{i-1}=\mathcal{H}_{\text{id}}(H_{x-1}^{\text{id}})$, and $\mathcal{H}_{\text{id}}$ is a rime representation hash function. TMR_x, IDC_x, nonce_x denote the transaction merkle root of T_x^{id}, the IDC of EIDS being accumulated and the variable for the SPoW puzzle. MC_x is the meta content for the block b_x composed of timestamp, valid time, location, version, difficulty, etc. The last one $(\text{IDC}_{x-1},\pi_\beta,\pi_\alpha)$ of b_x denotes a tuple resulting from IDC in the block header and commitment proof in the IPFS. IDC_{x-1} is the IDC in block b_{x-1}, which means previous identity set commitment when the blockchain is B_{x-1}^{id}. π_β^{del} and π_α^{add} indicate the NI-PoE proof for deletion and addition of identities, respectively.

2) RSA-Based Accumulator: According to [12] and [31], we give following definitions of RSA-based accumulator in proposed stateless blockchain for EIDS.

Denote $\mathbb{G}_{\text{id}}$ as a group of order ρ_{id}, and $g_{\text{id}}=<\mathbb{G}_{\text{id}}>$. Let $\mathbb{B}_\hbar=\{B_t^{\text{id}}|t=1,2,\ldots,\hbar\}$, $\gamma_t=\mathcal{H}_p(B_t^{\text{id}})$ and $\xi_i=\mathcal{H}_p(\mathbb{D}_i)$, where $i=\{1,2,\ldots,I\}$ and $\mathcal{H}_p$ is the prime representation hash function. The IDC_x in block b_x can be computed as

$$\text{IDC}_x=g_{\text{id}}^{\prod_{i=1}^I\xi_i}.\tag{9}$$

The membership witness for the identity credential $\mathbb{D}_e\in\mathbb{D}$ can be computed by $\omega_{\mathbb{D}_e}=g_{\text{id}}^{\prod_{i=1,i\neq e}^I\xi_i}$. If there are old identity credentials $\mathbb{D}^{\text{del}}$ being revoked and new identity credentials $\mathbb{D}^{\text{add}}$ being issued, EIDS is modified, and a new block is mined after a specified time. The block producer computes new IDC_x. In

Algorithm 1: ID Modification Algorithm.

// IDM_MD($T_\hbar^{id}$, $h_\hbar$, $TMR_\hbar$)
Data: $T_\hbar^{id}$, $h_\hbar$, $TMR_\hbar$
Result: $\mathbb{D}^{del}$, $\mathbb{D}^{add}$
$T \leftarrow T_\hbar^{id}$
$H \leftarrow h_\hbar$
$Root \leftarrow TMR_\hbar$
for t_n in T **do**
  $IsTure \leftarrow$ Varify_tx(t_n, $Root$)
  if *IsTure* **then**
    for $IPRevoke$ in T **do**
      $Id \leftarrow IPRevoke$.get_hash()
      B.revoke($IPRevoke, Id$)
      $\mathbb{D}^{del}$.append($IPRevoke, Id$)
    end
    for $IdIssue$ in t_n **do**
      $Id \leftarrow IdIssue$.get_hash()
      B.add($IdIssue, Id$)
      $\mathbb{D}^{add}$.append($IdIssue, Id$)
    end
  else
    return $False$
  end
end
return $\mathbb{D}^{del}$, $\mathbb{D}^{add}$

Algorithm 2: SPoW Alogrithm.

// IDM_SPoW($B_{\hbar-1}^{id}$)
Data: $T = \emptyset$, $B_{\hbar-1}^{id}$, $TxPool$
Result: $B_\hbar^{id}$
$B \leftarrow B_{\hbar-1}^{id}(\hbar - 1)$.get_header()
$T \leftarrow B$.get_tx()
$h \leftarrow$ hash_func(B)
$TMR \leftarrow B$.get_TMR()
for t_i in $TxPool$ **do**
  T.append(t_i)
  if $B.get\_size() > B$ **then**
    break
  end
end
$\mathbb{D}^{del}$, $\mathbb{D}^{add} \leftarrow$ IDM_MD(T, h, TMR)
ω_{del},$\pi_\beta^{del} \leftarrow$ BatchDel($IDC_{\hbar-1}, \mathbb{D}^{del}$)
ω_{add},$\pi_\alpha^{add} \leftarrow$ BatchAdd($\omega_{del}, \mathbb{D}^{add}$)
$nonce \leftarrow$PoW($B, TMR, IDC_\hbar, \hbar$)
$IDC_\hbar \leftarrow$ UpdateMemWit($IDC_{\hbar-1}, \omega_{add}, \mathbb{D}^{del}, \mathbb{D}^{add}$)
$H \leftarrow$(hash_func(B), $TMR, IDC_\hbar, \hbar, nonce$)
$B_\hbar^{id}(\hbar) \leftarrow \{H, \pi_\beta^{del}, \pi_\alpha^{add}, t_i\}$
return $B_\hbar^{id}$

Algorithm 3: Block Validation Algorithm.

// IDM_VD($b_{\hbar-1}, IDC_{\hbar-1}, TMR_{\hbar-1}$)
Data: $b_{\hbar-1}$, $IDC_{\hbar-1}$, $TMR_{\hbar-1}$
Result: $B_\hbar^{id}$, $IDC_\hbar$
$T \leftarrow b_{\hbar-1}$.get_tx()
$num \leftarrow 0$
for t in T **do**
  $IsTure \leftarrow$ Varify_tx($t, TMR_{\hbar-1}$)
  if *not* $IsTure$ **then**
    return $False$
  end
  $num \leftarrow num + 1$
end
if $TMR_{\hbar-1} != MerkelRoot(T)$ **then**
  return $False$
end
if $num == |T|$ **then**
  $\omega_{del}, \pi_\beta^{del}, \pi_\alpha^{add} \leftarrow B_\hbar^{id}$
  $IDC_{\hbar-1} \leftarrow b_{\hbar-1}$.MenWit()
  $\mathbb{D}^{del}, \mathbb{D}^{add} \leftarrow$
   IDM_MD(T,hash_func($b_{\hbar-1}$), $TMR_{\hbar-1}$)
  $p \leftarrow$ NI-PoE.VF($\prod_{d \in \mathbb{D}^{del}} d, \omega_{del}, IDC_{\hbar-1}, \pi_\beta^{del}$)
  $q \leftarrow$ NI-PoE.VF($\prod_{d \in \mathbb{D}^{add}} d, \omega_{del}, IDC_\hbar, \pi_\alpha^{add}$)
end
if $p \wedge q$ **then**
  $IDC.Acc(IDC_\hbar) == 1$
  $B_\hbar^{id} \leftarrow (B_{\hbar-1}^{id}, b_{\hbar-1})$
end
return $B_\hbar^{id}$, $IDC_\hbar$

the meanwhile, the Non-interactive PoE (NI-PoE) proofs [12] π_β^{del} and π_α^{add} are created for our proposed stateless blockchain, which can be verified efficiently without any interaction among block producers, light nodes, and full nodes. For updated identity credentials, $\mathbb{D}^{\text{del}} = \{\mathbb{D}_{d_s}^{\text{del}} | d_s = 1, 2, \ldots, I_d\}$ and $\mathbb{D}^{\text{add}} = \{\mathbb{D}_{a_s}^{\text{add}} | a_s = 1, 2, \ldots, I_a\}$. Let $\xi^{\text{del}} = \prod_{\mathbb{D}_{d_s}^{\text{del}} \in \mathbb{D}^{\text{del}}} \mathcal{H}_p(\mathbb{D}_{d_s}^{\text{del}})$ and $\xi^{add} = \prod_{\mathbb{D}_{a_s}^{\text{add}} \in \mathbb{D}^{\text{add}}} \mathcal{H}_p(\mathbb{D}_{a_s}^{\text{add}})$. When BatchDel() is executed, the membership witness ω_{del} and π_β^{del} can be computed with Shamir Trick [12].

$$\omega_{\text{del}} = g_{\text{id}}^{\prod_{\mathbb{D}_i \in \mathbb{D} \setminus \mathbb{D}^{\text{del}}} \mathcal{H}_p(\mathbb{D}_i)} \tag{10}$$

$$\pi_\beta^{\text{del}} = \text{NI} - \text{PoE}(\omega_{\text{del}}, \xi^{\text{del}}, \text{IDC}_{x-1}). \tag{11}$$

Finally, IDC_x and π_α^{add} can be calculated by BatchAdd() through this similar approach, and then $\mathbb{D}$ can be updated with $\mathbb{D} \longleftarrow \mathbb{D} \setminus \mathbb{D}^{\text{del}} \cup \mathbb{D}^{\text{add}}$.

$$\text{IDC}_x = (\omega_{\text{del}})^{\xi^{\text{add}}} \tag{12}$$

$$\pi_\alpha^{\text{add}} = \text{NI} - \text{PoE}(\omega_{\text{del}}, \xi^{\text{add}}, \text{IDC}_x). \tag{13}$$

Furthermore, the membership witnesses for all $\mathbb{D}_{a_s}^{\text{add}} \in \mathbb{D}^{\text{add}}$ can be obtained by $\omega_{\mathbb{D}_{a_s}^{\text{add}}} = (\omega_{\text{del}})^{\prod_{\mathbb{D}_s^{\text{add}} \in \mathbb{D}^{\text{add}}, \mathbb{D}_s{}^{add} \neq \mathbb{D}_{a_s}{}^{add}} \mathbb{D}_s^{add}}$. The membership witnesses can be updated by UpdateMemWit() function. Denote the membership witnesses of EIDS as $\omega_{\mathbb{D}}$ before revoking identities when the blockchain is B_{x-1}^{id}. Afterward, the membership witnesses can be computed wit$\omega_{\mathbb{D}_e}^* = \text{ShamirTrick}(\omega_{\text{del}}, \omega_{\mathbb{D}_e}, \xi^{\text{del}}, \mathbb{D}_e)$ when $\mathbb{D}_e \in \mathbb{D} \setminus \mathbb{D}^{\text{del}}$. After adding new identities in IPFS, the membership witnesses for all $\mathbb{D}_e \in \mathbb{D} \setminus \mathbb{D}^{\text{del}} \cup \mathbb{D}^{\text{add}}$ can be updated by $\omega_{\mathbb{D}_e}^{**} = (\omega_{\mathbb{D}_e}^*)^{\xi^{\text{add}}}$.

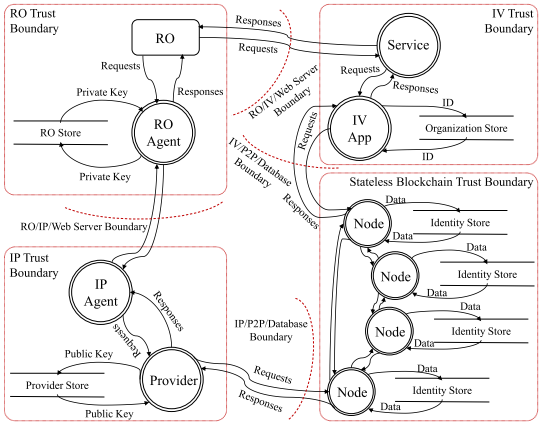

Fig. 5. DFD of proposed LSTIDM-SB for the comprehensive threat model, which shows how data flows logically through the system.

3) Blockchain Operations: The EIDS in the IPFS dynamically changes when the IP adds or revokes identity credentials, and a new block is appended to the blockchain. Algorithm 1 explains process of ID modification operated by the RO and IP, which returns revoked credentials set $\mathbb{D}^{\text{del}}$ and added credentials set $\mathbb{D}^{\text{add}}$.

For the stateless blockchain, we proposed a new consensus algorithm named SPoW in Algorithm 2 to mine new blocks, which includes accumulator commitment IDC, NI-PoE proofs $(\pi_\beta^{\text{del}}, \pi_\alpha^{\text{add}})$, credentials set $(\mathbb{D}^{\text{del}}, \mathbb{D}^{\text{add}})$.

Block Validation Algorithm: For efficient validation, a method is presented in Algorithm 3 to validate whether accumulator commitment IDC, T_x^{id}, TMR_x, NI-PoE proofs $(\pi_\beta^{\text{del}}, \pi_\alpha^{\text{add}})$ are legal or not. If parameters are valid, the node broadcasts a confirmation message to other nodes and the IV.

VI. System Analysis

In this section, we give a two-part analysis of the LSTIDM-SB, including threat analysis and security analysis. The first part contains a data flow diagrams (DFD) for the comprehensive threat model, the STRIDE (Spoofing, Tampering, Repudiation, Information Conflict of interest, Denial of Service, Elevation of Privilege)-based threat categorization and countermeasures. The second part consists of Lemmas and proofs for security features of the system.

A. Threat Analysis

Threat modeling can expose the attack surface, present countermeasures and provide adequate protection for system and software components [35], [36]. In our proposed LSTIDM-SB, detailed attack categories and analysis are explained using DFD in Fig. 5 according to [37], which combines data flow, control flow, and storage of data in these components. Suppose a computationally limited attacker [38] tries to compromise the stateless blockchain-based IDM due to a violation of any security objective. Consequently, our analysis remains unaffected by the specific whereabouts of the adversary.

1) Spoofing Node Messages: A potential threat involves an adversary isolating a node through manipulation of its known neighboring nodes. Mitigation against this threat is achieved through vigilant and independent monitoring of the blockchain network.

2) Tampering With Trusted IP: An adversary can tamper with the list of identity maintained by the IP. The way to prevent this attack is to ensure that the process of distributing IDs follows standard protocols.

3) Repudiate Blockchain Nodes: P2P utilizes a low-level communication protocol for message exchange. Typically, message repudiation is not incorporated into a gossip protocol within this structure.

4) Reveal Information: The node securely stores data encrypted by the RSA-based accumulator, ensuring that no additional confidential details can be revealed. Consequently, no threats exist within this category.

5) Deny Identity Service: This threat is an adversary that sends the false command to the goal node in an attempt to disrupt established connections with neighboring peers. Countermeasure for this threat can be achieved through message sender verification.

6) Elevate Privileges on the Identity: The RO assumes a higher privileged identity and carries out actions. Implementing a split control scheme in the assignment of identities serves as a countermeasure to this potential threat.

B. Security Analysis

LSTIDM-SB meets our design requirements including*blindness, unforgeability, traceability, unlinkability, revocability, antiattack capability, lightweight, trustworthiness, and efficient verifiability*. Specifically, similar to security analysis in [9] and [10], the security properties of LSTIDM-SB are derived progressively from cryptographic assumptions [30], [39], ECDSA [33], zero-knowledge proof, RSA-based accumulator, and soundness of the ZKPoK.

Lemma 1: LSTIDM-SB achieves unforgeability if ECDSA signature and cryptographic assumptions (in Section III) are secure in the random oracle model.

Proof: Assume that an opponent $\mathcal{O}^A$ wants to destroy the unforgeability of LSTIDM-SB and a challenger $\mathcal{O}^C$ answers ECDSA signature queries. For identity credentials in IPFS, when $\mathcal{O}^A$ can forges a legal identity, it shows that legal IBE can be already cracked successfully, but this situation contradicts the cryptographic assumptions. For IDC in the block header, if $\mathcal{O}^C$ forges a legal ECDSA signature or an identity $\mathbb{D}^{\text{IL}}$ with attributes $\mathbb{A}^{\text{IL}}$ that do not exist, these cases contradict the RSA assumption and RSA-based accumulator. ■

Lemma 2: LSTIDM-SB achieves blindness if the protocol ZKPoK_{Σ_1} named Θ satisfies zero-knowledge property.

Proof: In the IdIssue phase, by using $\mathcal{P}_{\text{sys}} = (\mathbb{G}_x, \mathbb{G}_y, \mathbb{G}_T, \rho, e, g_x, g_y)$ along with $\kappa_p^{\text{IP}} = (g_y, \mathcal{B}, \widetilde{\mathcal{A}}, \widetilde{\mathcal{B}})$, the IP adopts $\Theta = \text{ZKPoK}_{\Sigma_1}\{(\mu_i, \mathbb{A}_s^i) : T_i = g_x^{\mu_i}\mathcal{B}^{\prod_{\lambda\in\mathbb{A}_s^i}\lambda} \wedge \widetilde{T}_i = \widetilde{\mathcal{B}}^{\prod_{\lambda\in\mathbb{A}_s^i}\lambda}\}$ of $\mathbb{A}_s^i$, which are partial attributes selected from $\mathbb{A}^i$ for verifiable presentation, where $\mathbb{A}_s^i \subseteq \mathbb{A}^i, \mathbb{A}^i = \{\lambda_1^i, \lambda_2^i, \ldots, \lambda_{L_i}^i\}$. The zero-knowledge property guarantees that the commitment of $\mathbb{A}_s^i$ will not be divulged. Then, the RO

interacts with the IP by sending $(i, \widetilde{T}_i, z_i)$ and generates an EC digital signature P_i^g. ■

Lemma 3: LSTIDM-SB achieves unlinkability if the protocol ZKPoK_{Σ_2} named $\beth$ satisfies zero-knowledge property.

Proof: In the IdProve phase, the RO utilizes $\mathcal{P}_{\text{sys}} = (\mathbb{G}_x, \mathbb{G}_y, \mathbb{G}_T, \rho, e, g_x, g_y)$ along with $\kappa_p^{\text{IP}} = (g_y, \mathcal{B}, \widetilde{\mathcal{A}}, \widetilde{\mathcal{B}})$ to rerandomize the identity credential $\mathbb{D}_i = (\hat{\mu}_i, M_i, N_i^*, W_i, z_i)$ and dispatches the zero-knowledge proof $\beth = \text{ZKPoK}_{\Sigma_2}\{(\hat{\mu}_i, \varepsilon_i, W_i, z_i) : V_i = g_y^{\varepsilon_i}\widetilde{\mathcal{A}}\widetilde{\mathcal{B}}^{\hat{\mu}_i} \wedge E_i = P_i^{\varepsilon_i} \wedge e(\Omega, g_y) = e(W_i, \widetilde{\mathcal{B}} g_y^{\mu_i})\}$ to the IP, which enables attributes $\mathbb{A}^i$ to be securely protected. In addition, this property ensures that each RO i is entitled to hold a legal identity $\mathbb{D}_i$ while the specific data of $\mathbb{D}_i$ and $\mathbb{A}^i$ are not leaked. ■

Lemma 4: LSTIDM-SB achieves revocability and traceability if the stateless blockchain attains public accessibility and $\beth$ is a noninteractive signature proof of knowledge protocol, which satisfies soundness.

Proof: In the IdTrace and IPRevoke phase, the IP updates CRL and W_i with z_i and β. Due to the soundness of $\beth$, the RO who owns the legal identity authorised by the IP can generate this ZKPoK_{Σ_2} legitimately and the IV can decrypt it correctly. In the meanwhile, the IP can revoke a specified identity credential with the public accessibility of stateless blockchain. ■

Lemma 5: LSTIDM-SB achieves efficient verifiability, lightweight, and trustworthiness if the blockchain enables efficiently verifiable and stateless.

Proof: The blockchain structure guarantees secure verification as decentralized P2P network, proposed SPoW consensus and hash function can jointly maintain correctness and inerrability of data. For EIDS $\mathbb{D}$ in IPFS, the system computes ξ_i and IDC_x in block b_x with $\xi_i = \mathcal{H}_p(\mathbb{D}_i)$ and $\text{IDC}_x = g_{id}^{\prod_{i=1}^{I} \xi_i}$. The IV can attain efficient verifiability after obtaining the IDC $\omega_e of \mathbb{D}_e$, the proof of revocability π_β^{del} and the proof of addition π_α^{add}, where $\omega_e = g_{\text{id}}^{\prod_{i=1, i\neq e}^{I} \xi_i}$, π_β^{del} =NI-PoE $(\omega_{\text{del}}, \xi^{\text{del}}, \text{IDC}_{x-1})$, π_α^{add} = NI-PoE$(\omega_{\text{del}}, \xi^{\text{add}}, \text{IDC}_x)$ on the stateless blockchain. Thanks to the RSA-based accumulator, IDC is a length-constant commitment which will not increase when the number of identities becomes more substantial and not reveal specific identity details compared with UTXO in stateful blockchain, so that the system is lightweight and trustworthy.■

Lemma 6: LSTIDM-SB achieves antiattack capability if ECDSA signature P_i^g is secure and the blockchain reaches SPoW consensus mechanism.

Proof: For key search attack and man-in-the-middle (MITM) attack, the IP sends z_i, T_i, κ_p^i, R_i and compute $P_i^g = (z_i)^{-1}(\text{SHA\_256}(T_i) + \kappa_p^i \times R_i) \bmod \rho$, in which the signature will not be reused and leaked if P_i^g is a legal signature. For replay attack and single-point-of-failure, it is impossible for one or less than 51% of attackers to destroy the system when blocks are generated by obeying SPoW consensus mechanism. ■

VII. Performance

In this section, we implement LSTIDM-SB on Intel(R) Core(TM) i7-6700 CPU 3.40 GHz 3.41 GHz 32.0 GB RAM with Windows 10 operating system (OS). Python 3 syntax is used, where code uses the Crypto module, which is part of the *PyCryptodome* library. Specifically, classes such as ECC, DSS, and SHA256 are utilized for handling RSA key pairs, digital signatures, and SHA-256 hashing. More details are in Table II. In our code, *IdentityAccumulator()* class represents an accumulator for identity information, using the RSA accumulator logic. *IIoTTransaction()* contains device ID, timestamp, and sender's address. The "$sign - transaction$" method is used to digitally sign the transaction. *IIoTBlockchain()* class provides methods for creating the genesis block, creating transactions, mining, verifying SPoW, and printing the blockchain. *Vector-commitment()* class incorporates both binary and general vector commitments by leveraging the RSA accumulator. The experiment implements the SPoW consensus, block structure, IDM, and mining process. The process of transaction creation, mining, ID accumulating, and blockchain updating are simulated through method calls between nodes, which meets the requirements of system security, consistency algorithms, error handling, and monitoring metrics.

We present the simulated experimental performance of proposed LSTIDM-SB and analyze the result in Fig. 6, in which the comparison with [9] and [10] are included for clear expression. We give a bilinear map $e : \mathbb{G}_x \times \mathbb{G}_y \to \mathbb{G}_T$. Then, Ψ_x^E, Ψ_y^E, Ψ_x^M and Ψ_y^M represent the exponentiation and EC multiplication operation in $\mathbb{G}_x$ and $\mathbb{G}_y$, respectively. Ψ_T^E, Ψ_T^M, and Ψ_T^B indicate the exponentiation, EC multiplication, and bilinear pairing operation in $\mathbb{G}_T$. All these operations are counted to measure the performance of the proposed system, and the complexity analysis is listed in Table III.

TABLE II
System Setup, Containing Basic System Parameters, and Descriptions

Simulation Parameter	Description and Value
Area of IIoT Devices	3000 m^2
Number of Identities	100
Number of Devices	10
Mobility Model	Random Waypoint (RWP)
Communication Speed	1.8ms
Networking Protocol	IPFS, Bitcoin
Communication Standard	IEEE 802.11ah
Encryption Method	Hash, SHA-256, RSA
Used Library	pycryptodome, hashlib, time
Bit length of an element in $\lvert\mathbb{G}_T\rvert$	1024 bits
Bit length of an element in $\lvert\mathbb{D}_i\rvert$	2048 bits
Hash, SHA-256, RSA Operation	0.03 ms, 0.04 ms, 0.06 ms

TABLE III
Computation Cost, Including Algorithms and Time Required for Mathematical Calculation Operations

Algorithm	Computation Cost
SysKeyGen	$3\Psi_x^E + 2\Psi_y^E$
IdIssue	$12\Psi_x^E + 4\Psi_y^E + 7\Psi_x^M + \Psi_y^M$
IdProve	$5\Psi_x^E + 6\Psi_y^E + 3\Psi_x^M + 4\Psi_y^M + 5\Psi_T^B + 2\Psi_T^E + 3\Psi_T^M$
IVVerify	$2\Psi_x^E + 5\Psi_y^E + 2\Psi_x^M + 5\Psi_y^M + 8\Psi_T^B + 4\Psi_T^E + 5\Psi_T^M$
IdTrace	$\Psi_x^E + \Psi_y^E + 3\Psi_x^M + 3\Psi_y^M$
IdRecover	$2\Psi_x^E + \Psi_y^E + \Psi_x^M + \Psi_y^M + 2\Psi_T^B$
IPRevoke	$\Psi_y^E + \Psi_y^M + 3\Psi_T^B$

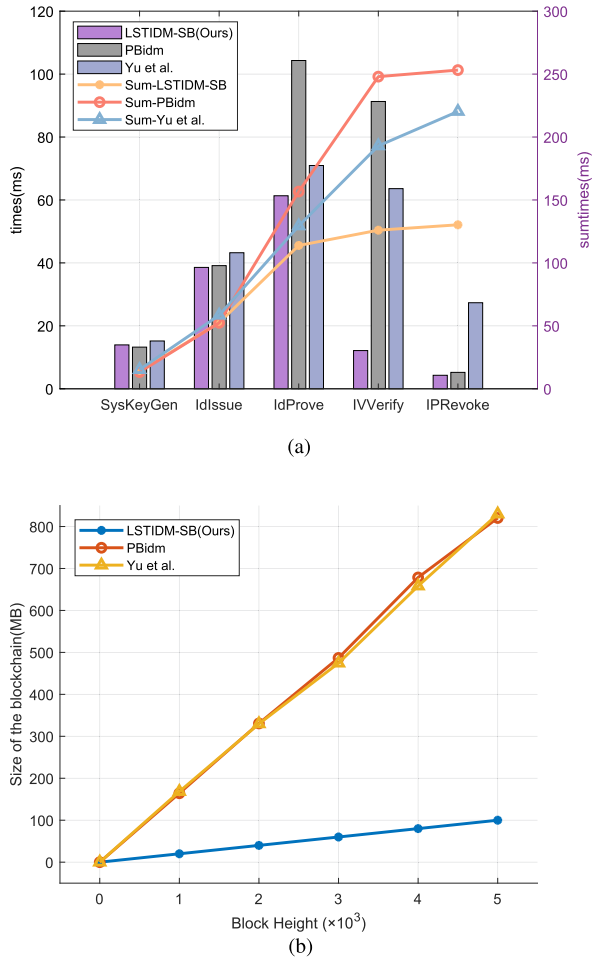

Fig. 6. Comparison with LSTIDM-SB, [9] and [10], which contains specific values of time cost and blockchain size.

TABLE IV
COMMUNICATION COST, INCLUDING ALGOTITHMS, STORE ALGEBRA, AND SPECIFIC VALUES THAT REPRESENT THE CONSUMPTION REQUIRED FOR COMMUNICATION

Algorithm	Cost	Values
IdIssue	$I\|\mathbb{D}_i\| + \|\Theta\| + 2\|req\|$	$(360 + 2048I)$ bits + $\|\Theta\|$
IdProve	$\|\beth\| + 3\|\mathbb{G}_T\|$	3072 bits + $\|\beth\|$
IVVerify	$\|\aleph\| + 6\|\mathbb{G}_T\| + \|req\|$	6324 bits + $\|\aleph\|$
IdTrace	$\|\mathbb{D}_i\| + 2\|req\|$	2408 bits
IdRecover	$\|\mathbb{D}_i\| + 3\|\mathbb{G}_T\| + 3\|req\|$	5660 bits
IPRevoke	$\|req\|$	180 bits

For communication cost, ZK proofs are needed in IdIssue, IdProve, and IVerify phases, ID costs for sending exists in IdIssue, IdTrace, and IdRecover. All the phases send request command and calculate elements in groups. We provide entire the algebra and specific values in Table IV.

In Fig. 6(a), LSTIDM-SB, [9] and [10] take approximately the equivalent time in the SySKeyGen and IdIssue phase. LSTIDM-SB takes 13.94 ms in the SySKeyGen phase due to multiple attributes in one identity credential, which resembles [10]. In the second phase, LSTIDM-SB, [9] and [10] take 38.56 ms, 39.13 ms, and 43.23 ms. In the IdProve and IVerify phase, as the stateless blockchain is adopted, the computation cost is less than [9] and [10], especially the IVerify phase. Our proposed system spends 61.33 ms and 12.14 ms, while [9] and [10] need 104.32 ms, 91.3 ms, 70.95 ms, 63.60 ms, respectively. In the IPRevoke phase, LSTIDM-SB and [9] need 4.28 ms and 5.21 ms, which are more efficient than 27.34 ms in Yu et al.'s scheme [10].

In Fig. 6(b), we give an analysis for the trend of the blockchain size with increasing of blocks. The storage of the blockchain is basically a linear growth with the blocks with the proliferation of blocks, as there is only an IDC in each block. [9] and Yu et al.'s scheme [10] are traditional blockchain systems, in which the size grows rapidly due to the exponential growth of the UTXO or accounts. When there are 5×10^3 blocks, LSTIDM-SB is around 100 MB while [9] and [10] are both about 800 MB. We strongly believe that this advantage brings opportunities to deploy the system on smart devices and applications in IIoT.

VIII. CONCLUSION

In this article, we proposed a lightweight, secure, and trustworthy IDM system with stateless blockchain for IIoT. By utilizing ECDSA, zero-knowledge proof, stateless blockchain with RSA-based accumulator, we present a professional and feasible scheme to satisfies lots of essential properties. Furthermore, the stateless blockchain structure is formulated and new consensus named SPoW, ID modification, and NI-PoE proofs-based verification algorithms are presented. Then, we provide a comprehensive threat model and security analysis with relevant lemmas and proofs to logically secure entire and suitable requirements. In experiments, it is evident to find that computation cost and storage of LSTIDM-SB are more superior compared with [9] and [10], which is more beneficial to smart devices and applications in IIoT.

REFERENCES

[1] R. Huo et al., "A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges," *IEEE Commun. Surv. Tut.*, vol. 24, no. 1, pp. 88–122, Firstquarter 2022.
[2] M. Borhani, M. Liyanage, A. H. Sodhro, P. Kumar, A. D. Jurcut, and A. Gurtov, "Secure and resilient communications in the Industrial Internet," in *Guide Disaster-Resilient Communication Network*. Cham, Switzerland: Springer Nature Switzerland, 2020, pp. 219–242.
[3] C. Nykvist, M. Larsson, A. H. Sodhro, and A. Gurtov, "A lightweight portable intrusion detection communication system for auditing applications," *Int. J. Commun. Syst.*, vol. 33, no. 7, 2020, Art. no. e4327.
[4] B. Häfner, V. Bajpai, J. Ott, and G. A. Schmitt, "A survey on cooperative architectures and maneuvers for connected and automated vehicles," *IEEE Commun. Surv. Tut.*, vol. 24, no. 1, pp. 380–403, Firstquarter 2022.
[5] D. J. Wu, J. Zimmerman, J. Planul, and J. C. Mitchell, "Privacy-preserving shortest path computation," in *Proc. Netw. Distrib. Syst. Secur. (NDSS) Symp.*, San Diego, CA, USA, Feb. 21–24, 2016.
[6] J. Ni, K. Zhang, X. Lin, Y. Yu, and X. Shen, "Cloud-based privacy-preserving parking navigation through vehicular communications," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, 2016, pp. 85–103.
[7] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.
[8] B. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, W. Wang, and N. M. F. Qureshi, "TAB-SAPP: A trust-aware blockchain-based seamless authentication for massive IoT-enabled industrial applications," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 243–250, Jan. 2023.

[9] Z. Bao, D. He, M. K. Khan, M. Luo, and Q. Xie, "PBidm: Privacy-preserving blockchain-based identity management system for Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1524–1534, Feb. 2023.
[10] Y. Yu, Y. Zhao, Y. Li, X. Du, L. Wang, and M. Guizani, "Blockchain-based anonymous authentication with selective revocation for smart industrial applications," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3290–3300, May 2020.
[11] X. Dai, B. Xiao, J. Xiao, and H. Jin, "An efficient block validation mechanism for UTXO-based blockchains," in *Proc. IEEE Int. Parallel Distrib. Process. Symp.*, 2022, pp. 1250–1260.
[12] D. Boneh, B. Bünz, and B. Fisch, "Batching techniques for accumulators with applications to IOPs and stateless blockchains," in *Proc. Adv. Cryptology 39th Annu. Int. Cryptology Conf.*, 2019, pp. 561–586.
[13] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Proc. Data Privacy Manage., Cryptocurrencies Blockchain Technol. Int. Workshops*, 2017, pp. 297–315.
[14] W. W. W. Consortium et al., "Verifiable credentials data model 1.0: Expressing verifiable information on the web," 2019. [Online]. Available: https://www.w3.org/TR/vc-data-model/?#core-data-model
[15] D. Bernhard, O. Pereira, and B. Warinschi, "How not to prove yourself: Pitfalls of the fiat-shamir heuristic and applications to helios," in *Proc. 18th Int. Conf. Theory Appl. Cryptology Inf. Secur. Adv. Cryptology–ASIACRYPT*, 2012, pp. 626–643.
[16] D. Maram et al., "Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability," in *Proc. IEEE Symp. Secur. Privacy*, 2021, pp. 1348–1366.
[17] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Comput. Secur.*, vol. 99, 2020, Art. no. 102050.
[18] A. Sonnino, M. Al-Bassam, S. Bano, S. Meiklejohn, and G. Danezis, "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers," in *Proc. Netw. Distrib. Syst. Secur. (NDSS) Symp.*, San Diego, CA, USA, Feb. 24–27, 2019.
[19] Y. Zhou, T. Liu, F. Tang, F. Wang, and M. Tinashe, "A privacy-preserving authentication and key agreement scheme with deniability for IoT," *Electronics*, vol. 8, no. 4, 2019, Art. no. 450.
[20] D. Chaum and E. Van Heyst, "Group signatures," in *Proc. Adv. Cryptology Workshop Theory Appl. Cryptographic Techn.*, 1991, pp. 257–265.
[21] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Proc. Adv. Cryptology–CRYPTO 24th Annu. Int. Cryptology Conf.*, 2004, pp. 56–72.
[22] S. Canard, D. Pointcheval, O. Sanders, and J. Traoré, "Divisible E-cash made practical," in *Proc. Public-Key Cryptography–PKC 18th IACR Int. Conf. Pract. Theory Public-Key Cryptography*, 2015, pp. 77–100.
[23] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. Topics Cryptol.-CT-RSA Cryptographers' Track RSA Conf.*, 2016, pp. 111–126.
[24] J. Song, P. Zhang, M. Alkubati, Y. Bao, and G. Yu, "Research advances on blockchain-as-a-service: Architectures, applications and challenges," *Digit. Commun. Netw.*, vol. 8, no. 4, pp. 466–475, 2022.
[25] R. Bhuvana and P Aithal, "Blockchain based service: A case study on IBM blockchain services & hyperledger fabric," *Int. J. Case Stud. Business, IT, Educ.*, vol. 4, no. 1, pp. 94–102, 2020.
[26] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Adv. Cryptology–CRYPTO 21st Annu. Int. Cryptology Conf.*, 2001, pp. 213–229.
[27] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Proc. Providing Sound Found. Cryptogr.: Work Shafi Goldwasser Silvio Micali*, 2019, pp. 203–225.
[28] J. Buchmann and H. C. Williams, "A key-exchange system based on imaginary quadratic fields," *J. Cryptol.*, vol. 1, pp. 107–118, 1988.
[29] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. IEEE 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
[30] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[31] N. Barić and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 1997, pp. 480–494.
[32] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[33] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes Cryptogr.*, vol. 19, pp. 173–193, 2000.
[34] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, pp. 36–63, 2001.
[35] A. Shostack, *Threat Modeling: Designing for Security*. Indianapolis, IN, USA: Wiley, 2014.
[36] D. J. Bodeau, C. D. McCollum, and D. B. Fox, "Cyber threat modeling: Survey, assessment, and representative framework," Mitre Corp, Mclean, 2018. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf
[37] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and attack centric integrated threat modeling for quantitative risk assessment," in *Proc. Symp. Bootcamp Sci. Secur.*, 2016, pp. 99–108.
[38] N. Alexopoulos, J. Daubert, M. Mühlhäuser, and S. M. Habib, "Beyond the hype: On using blockchains in trust management for authentication," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 546–553.
[39] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures," in *Proc. Workshop Theory Appl. Cryptographic Techn.*, 1993, pp. 274–285.

Kening Zhang received the B.Eng. from the School of Computer Science and Technology, Anhui University, Hefei, China, in 2021, and the M.Sc. degree from the Department of Computing, The Hong Kong Polytechnic University, Hong Kong, in 2022.

He is currently a Research Assistant with the Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University. His main research areas include blockchain technology, Internet of Things (IoT), and distributed system.

Carman K. M. Lee (Senior Member, IEEE) received the B.Eng. degree in manufacturing engineering and the Ph.D. degree in industrial and systems engineering from The Hong Kong Polytechnic University (PolyU), Hong Kong, in 2000 and 2004, respectively.

She is currently an Associate Professor with the Department of Industrial and Systems Engineering, PolyU, where she is also the Program Leader of [B.Sc. (Hons.)] Enterprise Engineering with Management and the Lab-in-Charge of the Cyber Physical Systems Laboratory. She has authored or coauthored more than 130 articles in various international journals and seminars. Her research interests include logistics and supply chain management, the Industrial Internet of Things (IIoT), cyber-physical systems, data analytics, and swam intelligence optimization.

Dr. Lee was awarded the Silver Medal at the 47th International Exhibition of Inventions of Geneva in 2019 and the Outstanding Paper Award of Emerald Network Awards in 2019.

Yung Po Tsang (Member, IEEE) received the B.Sc. (Hons) degree in logistics engineering management and the Ph.D. degree in industrial and systems engineering from the Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, in 2015 and 2020, respectively.

He is currently a Research Assistant Professor with the Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University. His current research areas cover artificial intelligence for decision-making, industry 4.0 technologies, and cold chain e-fulfilment.

Dr. Tsang was a recipient of the Outstanding Paper Award in IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2023, and 2019 Highly Commended Award from Emerald Literati Awards. He is also the certified ESG planner CEP, committee member of manufacturing and industrial engineering section of IET Hong Kong, and council member of Hong Kong Logistics Association.