

IdNet: Identity-Based Networking

Engin Zeydan*, Josep Manges-Bafalluy*, Suayb S. Arslan[§], Yekta Turk[†], Kapal Dev[‡]

*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, 08860.

[§] Bogazici University, Istanbul, Turkey, 34080.

[◇] Massachusetts Institute of Technology, MA, USA, 02139.

[†] Aselsan Corp., Istanbul, Turkey, 34906.

[‡] CONNECT Centre and Department of Computer Science, Munster Technological University, Ireland.

Email: {engin.zeydan, josep.manges}@cttc.cat, sarslan@mit.edu, yektaturk@aselsan.com, kapal.dev@ieee.org

Abstract—This paper introduces and evaluates a novel networking paradigm: Identity-Based Networking (IdNet), developed to address the growing complexity and security challenges of modern internet of things networks. By shifting the focus from traditional IP-based management to an identity-centric approach that relies on the concept of blockchain network (BCN)-based self-sovereign identity (SSI). IdNet promises enhanced security, higher efficiency and greater adaptability in dynamic network environments. The experimental setup, implemented in the GNS3 emulation environment, includes Open vSwitches (OVSS), virtual machines (VMs) and advanced network management tools such as OpenDaylight and Kubernetes. The experimental results focused on various operational metrics that are critical to the implementation and management of identity-driven network services. In addition, new insights into the operational dynamics of IdNet emerged, including the balance between operational efficiency and stringent security measures. At the end of the paper, we also discussed future directions and challenges, particularly in dynamically adapting legacy systems to manage digital identities without compromising operational speed, as evidenced by the observed long identity verification and revocation times.

Keywords—Self-sovereign identity, blockchain, identity-based networking, 6G use cases.

I. INTRODUCTION

The dawn of the digital age has exponentially increased the complexity of network environments and poses new challenges in terms of security, scalability and manageability [1]. The dynamic nature of modern digital

ecosystems, characterized by mobile users, IoT devices and cloud-based services, requires a more flexible and responsive approach to network management. Traditional IP-based network architectures are increasingly unable to meet the demands of dynamic and distributed digital ecosystems, necessitating a re-evaluation of network management paradigms. Implementing automation through network management tools therefore increases efficiency and reliability while reducing manual intervention [2]. Recent advances in blockchain technology have enabled novel identity-based solutions in several areas, including the secure integration of consumer electronics into the metaverse [3] and mutual authentication for UAVs [4]. These previous works highlight the growing importance of lightweight, secure and distributed identity systems that also align with Identity-Based Networking (IdNet)’s goals of providing robust and adaptable identity management in dynamic network environments.

A. Identity Management in Networking

The authors of [5], for example, have leveraged the best features of blockchain technology and Named Data Networking (NDN) to go beyond IP-based networking. However, NDN is content-centric approach and focuses only on the “what” of networking (the requested data) and not on the “who” (the identities of the users and devices). Details regarding an individual’s authorization to access a specific location and their permission to conduct transactions can also be embedded within their digital identification [6]. For network devices, identity information can also go beyond authentication and includes essential configuration features that define the scope of use within the network [7]. Our previous work in [8] explored a BCN-based SSI system designed as a new identity layer to allow owners of routing devices

This work was partially funded by “ERDF A way of making Europe” MCIN/AEI/ 10.13039/501100011033 project Grant PID2021-126431OB-I00, Generalitat de Catalunya grant 2021 SGR 00770 and Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55)

in autonomous systems (ASs) greater control over inter-domain networks (IDNs), potentially over multiple paths corresponding to preferences defined by routing devices.

Figure 1 shows the general identity management structure which includes interactions between the issuer, networking device, verifier and Self-Sovereign Identity (SSI) Blockchain Network (BCN). In this diagram, BCN-based SSI can be used to verify the identity and trustworthiness of network nodes during service provisioning or networking decisions as follows: (i) *Verifiable credentials*: They are used to attest to specific attributes or claims about a node, such as its capabilities, performance history, and security measures. These credentials are issued by trusted entities (e.g. network administrators as in Figure 1) and stored in the blockchain. Trusted entities can be the owner of the corporate network, the Internet Service Provider (ISP)/Cloud Service Provider (CSP) or the Mobile Network Operator (MNO). (ii) *Digital signatures*: When a node participates in the network (e.g. networking device such as Software Defined Networking (SDN) switch, container, Virtual Machine (VM) or switch as shown in Figure 1), it signs its communication and transactions with its private key. The public key, which corresponds to the private key used for signing, is part of the decentralized identity and can be used for verification by Verifier as in Figure 1. (iii) *Trust scores and reputation updates*: Over time, the network can determine trust scores for each node based on its historical behavior, performance and compliance with network rules. Nodes with higher trust scores are more likely to be selected for networking operations (e.g. Federated Learning (FL) [9]). (iv) *Smart contracts for dynamic networking decisions*: Smart contracts on the blockchain can be programmed to dynamically execute networking decisions based on predefined criteria and conditions.

B. Motivation for an Identity Layer in Network Management

In contrast, the identity of participants, enabling precise control over network access and interactions based on user and device identities should be emphasize. This is expected to improve security by directly managing the entities involved and also support more granular and dynamic customization of network services to user-specific contexts and needs, which is critical in environments that require stringent security measures and personalized network experiences. This paper embeds a versatile identity layer into the core of the network architecture

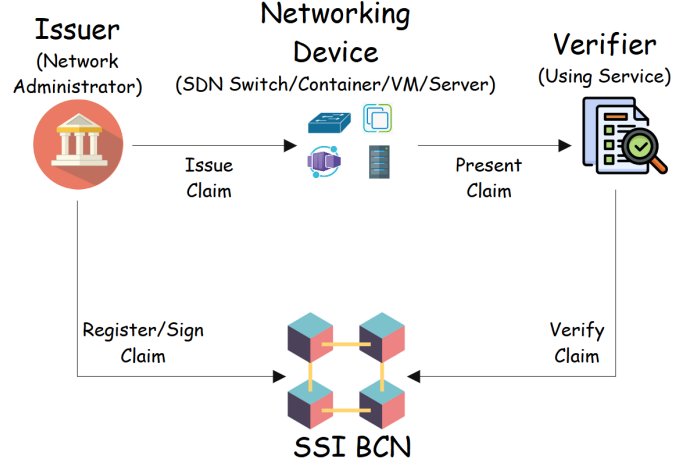


Fig. 1: Components of BCN based SSI Network Management.

that enables dynamic and automated management across different domains. We address the complex dynamics of digital identity and show its central role not only as a component, but as a key architectural element that redefines the configuration, management and optimization of network services in Identity-based Networking (IdNet). Furthermore, we demonstrate through rigorous experimentation how this approach improves security, efficiency and adaptability in modern network environments.

II. IDENTITY BASED NETWORKING ARCHITECTURE

A. Key Benefits

IdNet's focus is on the digital identity of users and devices rather than their IP addresses or physical access points which can enable precise access control and more effective dynamic security policies that reduce the attack surface and protect privacy of individual users and devices based on the context and identity of devices and users. However, this reliance on digital identities also requires robust identity verification and management processes to prevent identity theft and ensure that only legitimate users and devices can access network resources. Table I provides a comparison of IP-based and IdNet-based networking approaches. Unlike traditional authentication-centric approaches, the SSI BCN system acts as a separate layer and enables the seamless transfer of a comprehensive set of attributes to network devices, from authentication details to device inventory tracking and configuration parameter information. This shift represents a fundamental change in the management of network services and security, enabling more granular

TABLE I: Comparison of IP-Based and IdNet-Based Networking Approaches

Aspect	IP-Based Networking	IdNet
Focus	Focuses on the IP addresses or physical access points of devices.	Focuses on the digital identity of users and devices, not limited to their IP addresses or physical locations.
Access Control	Typically uses static access control lists and firewall rules based on IP addresses.	Enables precise access control based on the context and identity of devices and users, dynamically adjusting access rights.
Security Policies	Security policies are often static and IP-centric, requiring manual updates and are less adaptive to dynamic network changes.	Implements dynamic security policies that automatically adapt to changes in user behavior and context, effectively reducing the network's attack surface.
Privacy Protection	Limited privacy protection capabilities, often exposing user and device IP addresses to potential surveillance and attacks.	Enhances privacy protection by managing identities in a way that can keep actual user and device details confidential and secure.

control, greater security and more efficient network management. On the other hand, implementing such a system as a separate layer in the IdNet architecture may also introduce complexity, including integration challenges with existing systems, scalability concerns and potential performance overheads. As a solution, integrating IdNet with traditional IP-based systems requires strategies such as hybrid networks, overlay networks and gateway solutions to enable seamless coexistence while minimizing service disruption.

B. High-Level Design

Figure 2 shows the high-level design view and the position of the identity layer for a given IdNet. In our proposed design, we add another layer for identity. By integrating an identity layer (e.g. BCN-based SSI) into networking, it becomes possible to create a more secure, transparent and resilient system in which the identity and trustworthiness of nodes is verifiable and tamper-proof. The specific features of IdNet architecture are as follows: (i) *Decentralized Identity Creation*: Each network node is assigned a unique, decentralized identity on the blockchain. This identity is created by the individual or organization that owns the node, ensuring control and ownership of the identity. This identity includes information about the node's capabilities, historical performance, and any relevant attributes that contribute to its reputation. (ii) *Consensus Mechanism*: The BCN uses a consensus mechanism to validate and agree on the state of the decentralized identity information. This ensures that the information about each node is correct and tamper-proof. Some SSI-based systems may also include a consensus mechanism where the community of nodes collectively sets reputation values. This ensures a more democratic and decentralized approach to reputation management. (iii) *Redundancy Structure*: In a corporate ISP or MNO

network that operates with multiple Data Centers (DCs) and resilient DC in case of disaster, each BCN node can be located in a DC (and resilient DC). These DC nodes can take part in consensus transactions. In addition, in case of a problem in the Main DC, since a copy of the ledger is also in the resilient DC (thanks to the distributed structure of BCN), the device information in the IdNet will be automatically restored without the need for extra backup operations.

(iv) *Identity Revocation*: If a node behaves maliciously or violates the network rules, its identity can be revoked. This ensures that only trustworthy nodes participate in the network and that their credentials are updated accordingly in the blockchain. A device that is planned to be removed from the network or to be replaced due to malfunctioning/failure, identity revocation can be triggered. (v) *Selective Disclosure*: BCN-based SSI allows nodes to selectively disclose only the information that is necessary for a particular decision. This increases privacy and minimizes the disclosure of sensitive data while providing enough information for other nodes to make informed decisions. (vi) *Interoperability*: The landscape of BCN-based SSI standards is still forming, and interoperability among diverse blockchain technologies remains a complex challenge. As these standards evolve, future solutions can be compatible with global standards and integrate seamlessly into wider network systems.

C. Device Classes

There can be different classes of devices such as standalone, semi-autonomous and fully autonomous devices. Some of these devices can also have the intelligence with the embedded Artificial Intelligence (AI) abilities. The capabilities of the devices can be restricted by the use of IdNet. Fully autonomous devices are fully AI-capable

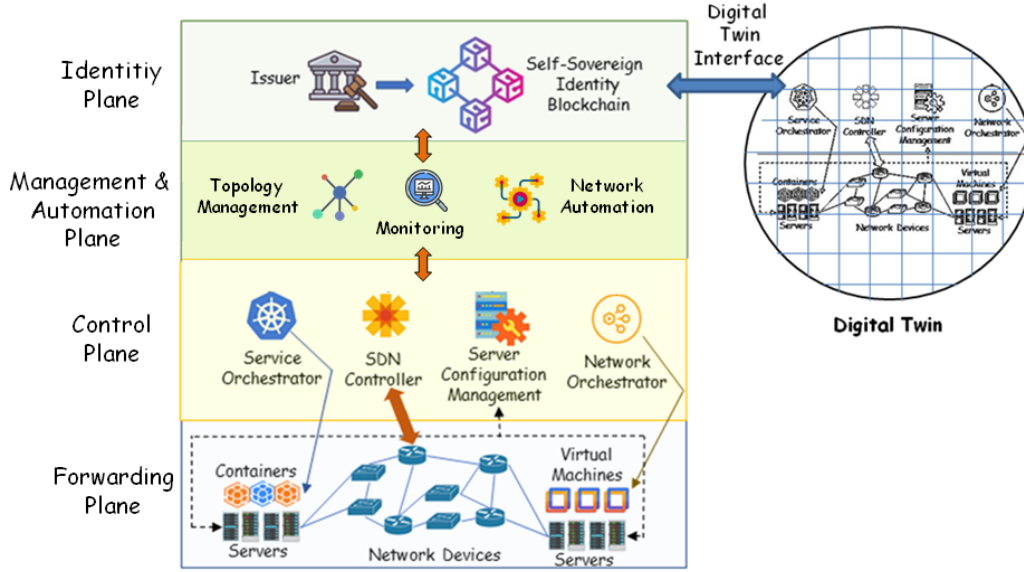


Fig. 2: Identity plane is positioned on the top of the control plane in IdNet architecture.

devices and can use their features independently within the network to provide alternative routing, quality-of-service implementation decision, etc. Semi-autonomous devices, on the other hand, can use the AI results within an external or hierarchical guidance. Semi-autonomous devices make their decisions under the control of a higher-level orchestration system. All of these devices could have AI capabilities and, in some specific cases, federated AI capabilities written into their IDs.

D. Enhancements with ZTA and SASE Principles

IdNet fundamentally shifts the focus from the perimeter-based defense mechanisms to identity-based access controls and policies complementing Zero-trust architecture (ZTA) paradigm initially proposed by NIST [10]. IdNet extends the principles of ZTA and Secure Access Service Edge (SASE) by placing digital identity at the center of network operations and using DIDs and verifiable credentials for secure, real-time identity verification. IdNet is characterized by the integration of decentralized identity management, blockchain technology and privacy. It complements the principles of ZTA and SASE while addressing gaps in identity granularity and security. Compared to NDN, IdNet can offer a more holistic approach by combining content management with identity-centric policies, making it ideal for modern, dynamic network environments. The ZTA, which operates on the principle of "never trust, always verify", requires continuous verification of identities and strict access controls regardless of the perceived security perimeter. Similarly, SASE integrates wide-area

networking with comprehensive security features such as Secure Web Gateways, Cloud Access Security Brokers and Zero-Trust Network Access into a single cloud-delivered service [11]. The identity layer overlaps with these concepts by providing a consistent and scalable method of authenticating, authorizing and monitoring identities across diverse and distributed environments.

E. Digital Twins Interactions

IdNet can be used to provide an interface to the digital twin network. IdNet can help with network-related configuration management both in the real network and in the digital twin environment by providing corresponding IDs in SSI BCN. This ensures that exactly the same devices with the same configuration are located in the real and digital twin environments [12]. An example scenario in which the digital twin interface can be used to predict traffic patterns is that of a telecommunications provider using a digital twin of its network to simulate traffic patterns during peak hours, e.g. during major events or holidays. IdNet can provision identity-driven configurations for devices and network elements in the digital twin, ensuring that the simulated environment accurately reflects the real network. In this way, the telecommunications provider prevents network congestion and ensures a high-quality service for end users by proactively optimizing the network based on the predictions.

In another scenario, an enterprise can deploy a digital twin to test new security policies or to simulate potential

security breaches. Before the policies are applied to the live network, the digital twin can be used to validate their effectiveness and identify potential problems. In this setup, IdNet can provide real-time feedback on how policies interact with user identities, allowing administrators to refine policies before deployment. IdNet can provide the digital twin with identity-based configurations for virtual machines, routers and services managed by Kubernetes. Simulations in the digital twin can be used to evaluate the performance of these configurations under different workloads and determine optimal setups.

III. NETWORK SERVICES AND APPLICATION DOMAINS

A. Service Models

IdNet opens up new possibilities for the development of highly personalized and user-centric network services. By leveraging the rich context provided by digital identities, network services can be tailored to the specific needs, preferences and security requirements of individual users and devices. This could lead to a more intuitive and responsive network environment where resources are dynamically allocated based on user activity and services are customized for individual experiences compared to traditional orchestration approaches. *In IoT networks*, issuing verifiable credentials to IoT devices based on their capabilities, firmware version and other relevant attributes can be used during network provisioning services. In a smart home scenario, for example, IdNet could enable seamless and secure interaction between a user's devices, by automatically adjusting settings and permissions based on the user's location, time of day and specific preferences. *In industrial automation*, smart contracts implemented on the blockchain can be used to automate and optimize production processes and determine the most efficient paths for data and commands within the industrial network. *In mobile edge computing*, verifiable credentials can be issued to edge devices based on their computing power, latency and other capabilities. IdNet can also provide a foundation for dynamic and flexible routing paths by leveraging the reputation and capabilities of network nodes (e.g. vehicular networks as in [9]).

B. Networking Scenarios

Figure 3a is a potential use case for a fixed ISP, a DC or an enterprise network that demonstrates the synergy between IdNet, digital twins and network automation,

providing a framework for managing complex network environments more securely and efficiently. All devices and users within the building are registered in the IdNet system with unique identities. A digital twin of the building's network is created, mirroring every device, every user and every network segment in a virtual model. This twin is constantly updated with real-time data from the physical network. Based on identity and context (extracted from the digital twin data), network access and security policies are automatically enforced to ensure that users and devices have appropriate access rights.

Figure 3b represents a use case for a CSP where IdNet can be used to enhance security, streamline operations, and improve resource allocation by managing VMs based on the identities of the VMs themselves, their users, and their application context. Each VM can be assigned a unique identity that includes its purpose, the sensitivity level of its data and its operational context. Users are also assigned identities based on their roles (e.g. developer, system administrator, end user) and the projects or departments to which they belong. Based on VM and user identities, access and operational policies are defined that determine which user roles can access or manage specific VMs under which conditions (e.g. time-based access for testing environments) and which resources are assigned to VMs based on their operational context. For example, the identity "VM-Dev-ProjectX" can be used as a development environment VM for Project X, which is classified as low sensitivity, while the identity "VM-Prod-WebServer" can be a production web server, which is classified as high sensitivity. The identity "Alice-Dev-ProjectX" can be a developer assigned to project X, and according to the policy "Alice-Dev-ProjectX" can access "VM-Dev-ProjectX", but not "VM-Prod-WebServer".

C. Privacy Considerations

Privacy-preserving technologies, such as Zero-Knowledge Proofs (ZKPs) can play a crucial role in ensuring that IdNet complies with data protection. IdNet can use ZKPs so that devices can prove certain attributes of their identity (e.g. switching capacity, network functions or location). When accessing network resources, ZKPs can allow users to authenticate and obtain authorization without having to transmit sensitive identity data over the network and prove that a device is authorized to access a segment of the network without sharing device-specific credentials. ZKPs can also align with the privacy principle of minimizing the processing of device data by ensuring that only the information necessary for

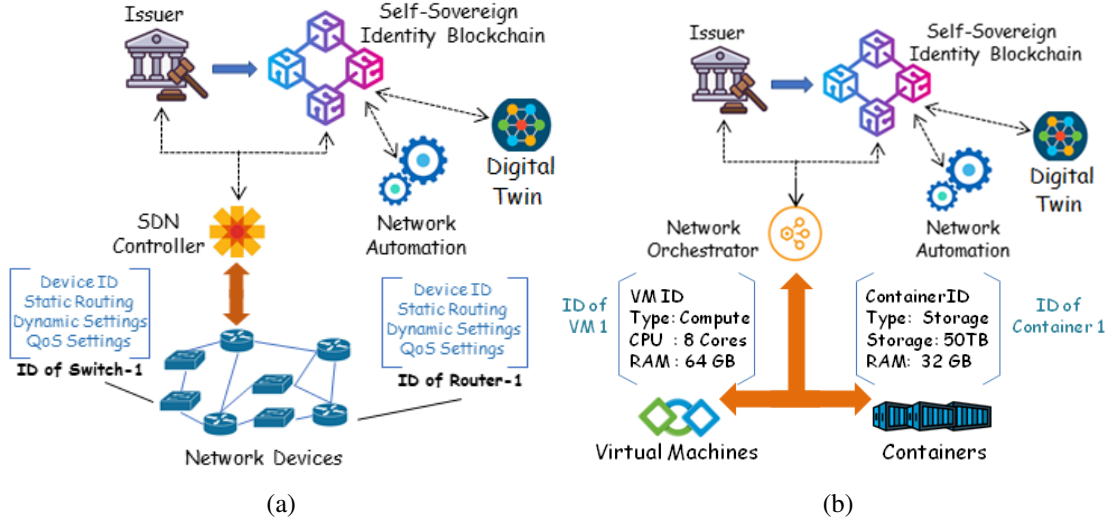


Fig. 3: (a) A routing/switching use case for identity-based networking architecture interacting with digital twins and network automation concepts, (b) A secure and dynamic VM management use case in a cloud environment with identities stored in IdNet layer.

a transaction is disclosed without revealing extraneous details. During authentication, ZKPs can provide proof of identity attributes without storing or transmitting unnecessary data. When verifying the compliance of devices, ZKPs enable proof of compliance without transmitting the actual configuration details. In IdNet, identity data is stored in device-controlled wallets, and sensitive information is not permanently stored on the network. This decentralization, combined with ZKPs, can enable compliance with this regulation. IdNet's blockchain-based infrastructure can also use ZKPs for verifiable credentials and decentralized identifiers. This ensures that identity verification processes are decentralized, secure and privacy-preserving. With ZKPs, IdNet can dynamically enforce identity-based access policies while ensuring that no sensitive data is exposed.

IV. EXPERIMENTAL EVALUATIONS

A. Test Setup

The test setup was implemented in the Graphical Network Simulator 3 (GNS3) emulation environment as shown in Figure 4. There are 4 OpenvSwitches (OVSs) that were installed in GNS3. In addition, 4 VMs set up with Ubuntu 16 LTS were installed. Two of the virtual machines are positioned as servers that take over the transmission of the services. The SSI BCN network is set up in in one of the VMs. The installation of

the SSI BCN network was provided by Von-network. Two separate ledgers were created in Von-network to store the identities of the server VMs and OVSs. A wallet was created for each device in the corresponding ledger. Subsequently, a Decentralized Identifier (DID) was added to the wallets. The configuration parameters are located in the metadata area of the DIDs. In the other VM, OpenDaylight was installed to manage OVSs and Kubernetes to manage the services created on the servers. The configuration parameters are retrieved from the SSI BCN VM using Python scripts, since these 2 VMs are connected to the same OVS and positioned on the same subnet. Hyperledger Indy scripts are extended to read the metadata information of the digital identities in wallets. This metadata field of the ID includes the OVS configuration and scripts sent these data to the REST Application Programming Interface (API) of the OpenDaylight. Additionally, if the ID belongs to a server, then the related service configuration stored in the metadata field is sent to Kubernetes. Flutter service is deployed with the parameters obtained from the device ID. In the test setup, a service was activated from end to end between Server-1 and Server-2, including OVSs and servers.

B. Results

In this section, various performance indicators related to the operation of IdNet and service configurations are

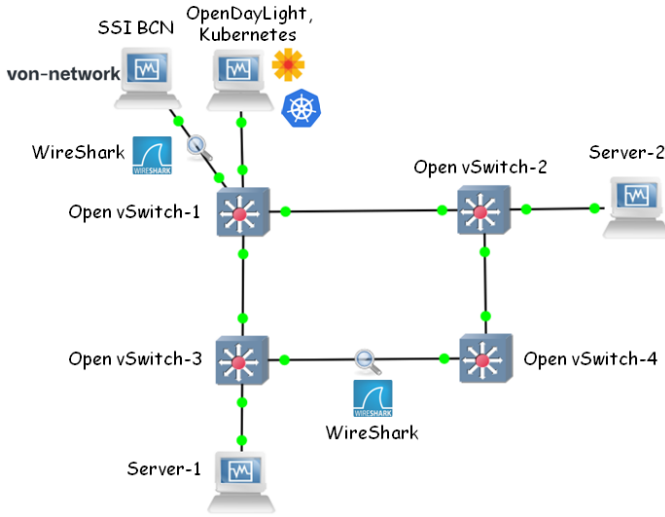


Fig. 4: Experimental setup created with the GNS3 emulation environment for validation purposes.

evaluated. Table II contains data that are crucial for understanding the efficiency and responsiveness of IdNet systems in practical applications. Eight different metrics are evaluated. *The wallet creation time* indicates the time it takes to create a digital wallet, presumably to store digital identities or credentials. The process is relatively fast, indicating an efficient setup phase for new users or devices in the IdNet ecosystem. *Id Verification Time* is the time it takes to verify an identity. Compared to the wallet creation time, verification takes significantly longer period. This discrepancy is possible due to the high complexity and security measures involved in verifying an identity, such as checking cryptographic proofs or consulting a decentralized registry. *Id Presentation Time* is the duration, which is more than twice as long as the time for identity verification. It indicates the process of presenting the identity to a verifier or service, possibly including the time for collecting, packaging and submitting the required credentials. The longer time indicates a more complex interaction, possibly involving multiple network hops or interactions with external systems.

Id Metadata Reading Time is for reading metadata associated with an identity and is faster than verification or presentation, but still takes a few seconds. This process can involve accessing detailed information about the identity, such as permissions, attributes or history, which is important for making decisions about access control or customizing services. *OpenDaylight configuration time* is the time for configuring the network settings with the OpenDaylight SDN controller is very short. This indicates that changes to the network configuration re-

TABLE II
AVERAGE TIME FOR IDNET OPERATIONS
AND SERVICE CONFIGURATIONS.

Performance Indicator	Value
Wallet Creation Time	≈ 200 ms.
Id Verification Time	≈ 5 sec.
Id Presentation Time	≈ 11 sec.
Id Metadata Reading Time	≈ 3 sec.
OpenDaylight Configuration Time	≈ 100 ms.
Kubernetes Deployment Time	≈ 40 ms.
E2E Service Creation Time	≈ 3.100 sec.
Id Revocation Time	≈ 19 sec.

quired for proper IdNet operation or policies can be performed efficiently, minimizing the impact on network performance. *Kubernetes Deployment Time* is similar to the OpenDaylight configuration and provisioning of a Flutter service in Kubernetes environment is remarkably fast. This value is obtained by measuring the time between the service request and the deployment of the service in Server-1. This short deployment time is crucial for dynamic environments where services need to be scaled or updated frequently based on identity-driven policies.

E2E service creation time is the end-to-end time to create a service, including setup, configuration and provisioning of required resources, is relatively fast, although not instantaneous. This indicates a good balance between thoroughness (in terms of identity verification and policy application) and efficiency. This value is by measuring the time between the service request and the deployment of the service in Server-1, Server-2 and configuration of all OVSS. *Id revocation time* represents the revocation of an identity, which is the longest of the processes listed. During this time, an identity is not only marked as invalid, but this status is also applied to the entire system to ensure that access rights are immediately restricted. The process includes a dynamic reconfiguration of the network, such as updating access control lists, routing policies and firewall rules, as well as the potential redeployment of services to enforce new access restrictions. In addition, the system must deal with different access restrictions in different domains, which requires customised policy updates and secure inter-domain communication.

C. Comparisons and Implications for IdNet

Numerical results in Table II illustrate the operational efficiency and responsiveness of the IdNet system across a range of tasks, from network and service configuration

to the more complex and security-related processes of identity management. The wallet creation and service deployment processes are observed to be remarkably fast, demonstrating IdNet’s ability to rapidly provision services and customise network configuration. However, the processes of identity verification, presentation and revocation are much more lengthy, highlighting the complexity and critical security considerations involved in managing digital identities. Some conclusions from results are as follows: (i) *Trade-off between efficiency and security*: The longer times for identity verification, presentation, and revocation reflect a trade-off between security and efficiency. These processes are inherently complex and critical to maintaining the integrity and security of the IdNet system. (ii) *Fast configuration changes*: The short times for OpenDaylight and Kubernetes configurations show that the system is able to quickly adapt network and service configurations based on identity-driven policies, which is crucial for dynamic and automated environments. (iii) *Operational effects*: The different times for the various operations indicate that while IdNet can perform routine configurations and deployments quickly, identity management operations, especially those that ensure security and compliance, require more time. This balance is crucial to the design and management of IdNet systems as it affects usability and system security.

D. Discussions

The experimental results provide a clear illustration of the trade-off between operational efficiency and stringent security protocols within the IdNet framework: While the system excels in rapidly executing configurations and deployments, the critical security processes of identity verification, presentation, and revocation inherently took longer. This trade-off is essential for ensuring that while the network remains agile and responsive, it does not compromise on security standards crucial for protecting digital identities. The quick configuration times for both OpenDaylight and Kubernetes suggest that IdNet is well-suited to environments requiring rapid adaptability. These capabilities are especially beneficial in dynamic application scenarios where network conditions or service requirements can change frequently [13]. The variation in the time required for different operations highlights important considerations for the deployment and management of IdNet systems. While routine tasks can be managed efficiently, operations central to security and compliance demand more resources and time, impacting

overall system performance and user experience.

E. Observed Challenges

There are also some challenges for IdNet’s real-world applications in IoT security, edge computing and multi-cloud environments such as the following. (i) *Privacy considerations*: When developing and implementing IdNet systems, a careful balance must be struck between the need for security and identity verification and the need to protect user privacy, possibly through the use of privacy-enhancing technologies such as zero-knowledge proofs [14] and encrypted identity tokens [15]. (ii) *Potential for creating more user-centric network services*: IdNet could facilitate the development of new business models and services that use identity information to offer users greater added value. For example, network operators could offer identity-based security services, IDaaS (Identity-as-a-Service) offerings or personalized network experiences that go beyond traditional connectivity services. (iii) *Interoperability with existing network infrastructures*: To achieve seamless integration, transition strategies and compatibility layers must be developed that can bridge the gap between IdNet and traditional networking approaches. For example, the deployment complexity that can arise from integrating IdNet into traditional IP networks can be effectively addressed through approaches such as hybrid network models, overlay networks, gateway solutions, standardized interfaces, pre-deployment testing using digital twin environments, and cost-benefit optimization that balances initial effort with long-term benefits. (iv) *Scalability*: The scalability of IdNet in large networks can be achieved through distributed processing, edge-based identity verification, caching, digital twin simulations and incremental deployment strategies to ensure stable and efficient performance under high traffic conditions. The performance overhead in large scenarios can be effectively mitigated by strategies such as distributed processing, caching, efficient cryptographic techniques, incremental updates, edge computing and predictive analytics to maintain scalability and responsiveness. (v) *Resource Consumption*: Blockchain-based identity management systems may require additional computing and storage resources, which can increase the hardware requirements for the network infrastructure. On the other hand, IdNet can mitigate these challenges through optimizations such as lightweight blockchain protocols, hybrid storage, edge-based identity verification, caching, and selective updates.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we have introduced and explored the concept of IdNet, highlighting its potential to revolutionize network management and security through the integration of digital identities. Through its focus on identity, integration with blockchain technology and compatibility with digital twins, IdNet provides a framework for secure, efficient and adaptable networking. Our experimental analysis revealed a balanced trade-off between operational efficiency and security. Processes such as wallet creation and service provisioning were executed swiftly, demonstrating IdNet's ability to adapt quickly. Conversely, identity verification and revocation were more time consuming, reflecting the complexity and critical nature of these processes in ensuring network integrity and user privacy. Future work could focus on optimizing strategies such as load balancing, edge computing and decentralized identity management and performing large-scale simulations to validate the performance of IdNet in such environments.

REFERENCES

- [1] D. M. Manias and A. Shami, "The need for advanced intelligence in NFV management and orchestration," *IEEE Network*, vol. 35, no. 1, pp. 365–371, 2020.
- [2] M. El Rajab, L. Yang, and A. Shami, "Zero-touch networks: Towards next-generation network automation," *Computer Networks*, p. 110294, 2024.
- [3] R. Li, Z. Wang, L. Fang, C. Peng, W. Wang, and H. Xiong, "Efficient blockchain-assisted distributed identity-based signature scheme for integrating consumer electronics in metaverse," *IEEE Transactions on Consumer Electronics*, 2024.
- [4] W. Wang, Z. Han, T. R. Gadekallu, S. Raza, J. Tanveer, and C. Su, "Lightweight blockchain-enhanced mutual authentication protocol for uavs," *IEEE Internet of Things Journal*, 2023.
- [5] D. B. Rawat, R. Doku, A. Adebayo, C. Bajracharya, and C. Kamhoua, "Blockchain enabled named data networking for secure vehicle-to-everything communications," *IEEE Network*, vol. 34, no. 5, pp. 185–189, 2020.
- [6] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pp. 342–345, 2020.
- [7] R. Kapudasu and K. Jain, "Network device identity management using cryptography," in *Inventive Computation and Information Technologies: Proceedings of ICICIT 2022*, pp. 951–963, Springer, 2023.
- [8] E. Zeydan, J. Mangues, S. S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity for routing in inter-domain networks," *IEEE Communications Magazine*, pp. 1–7, 2023.
- [9] E. Zeydan, L. Blanco, J. Mangues, S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity for federated learning in vehicular networks," in *2023 19th International Conference on Network and Service Management (CNSM)*, pp. 1–7, IEEE, 2023.
- [10] V. Stafford, "Zero trust architecture," *NIST special publication*, vol. 800, p. 207, 2020.
- [11] S. Yiliyaer and Y. Kim, "Secure access service edge: A zero trust based framework for accessing data securely," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0586–0591, IEEE, 2022.
- [12] Y. Wu, K. Zhang, and Y. Zhang, "Digital twin networks: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13789–13804, 2021.
- [13] N. a. Slamnik-Kriještorac, "AI-empowered management and orchestration of vehicular systems in the beyond 5G era," *IEEE Network*, vol. 37, no. 4, pp. 305–313, 2023.
- [14] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A survey on zero-knowledge proof in blockchain," *IEEE network*, vol. 35, no. 4, pp. 198–205, 2021.
- [15] C. Adams, "Security analysis of a privacy-preserving identity-based encryption architecture," *Journal of Information Security*, vol. 13, no. 4, pp. 323–336, 2022.

VI. BIOGRAPHIES

Engin Zeydan is currently a Senior Researcher at Centre Tecnològic de Telecomunicacions de Catalunya.

Josep Mangues-Bafalluy is currently a Senior Researcher and the Head of the Services as Networks Research Unit, Centre Tecnològic Telecomunicacions Catalunya (CTTC).

Suayb S. Arslan holds the position of Professor of Computer Engineering and Director of the Institute for Artificial Intelligence and Data Science at Bogazici University and is also a research affiliate at the Massachusetts Institute of Technology in Boston, MA, USA.

Yekta Turk is with Aselsan Corp. working in the areas of networking and security.

Kapal Dev is with Munster Technological University, Ireland working in the areas of security and privacy of next generation networks.