2022 International Conference on Computer Communications and Networks (ICCCN) | 978-1-6654-9726-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCN54977.2022.9868843

# A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems

Ronghua Xu[a], Yu Chen[a], Xiaohua Li[a], Erik Blasch[b]

[a]Dept. of Electrical and Computer Engineering, Binghamton University, Binghamton, USA
[b]The U.S. Air Force Research Laboratory, Rome, USA
Emails: {rxu22, ychen, xli}@binghamton.edu, erik.blasch@us.af.mil

***Abstract*—The fast integration of 5G communication, Artificial Intelligence (AI), and Internet-of-Things (IoT) technologies is envisioned to enable Next Generation Networks (NGNs) for diverse smart services and user-defined applications for Smart Cities. However, it is still challenging to build a scalable and efficient infrastructure that satisfies the various performance, security, and management demands by heterogeneous IoT applications across multiple administrative domains. This paper presents a dynamic edge resource federation architecture, which integrates the concept of network slicing (NS) and blockchain to improve scalability, dynamicity, and security for multi-domain IoT applications. A NS-enabled dynamic edge resource federation framework adopts intelligent mechanisms to support efficient multi-domain service coordination that satisfies diverse Quality of Service (QoS) and security requirements. We propose a Hierarchical Integrated Federated Ledger (HIFL), which aims to guarantee decentralized security and privacy-preserving properties in multi-domain resource orchestration and service re-adjustment. As a secure-by-design solution, HIFL is promising to support efficient, trust and secured end-to-end IoT services. A preliminary proof-of-concept prototype has been implemented for comparing intra- and inter-domain performance expectations.**

***Index Terms*—Next-Generation Networks (NGNs), Smart Cities, Internet of Things (IoT), Edge Network, Network Slicing, Blockchain.**

## I. Introduction

The rapid evolving fifth-generation (5G) communication networks combined with Internet of Things (IoT) and edge-cloud computing technologies brings the concept of *Smart Cities* into practice. A plethora of novel smart applications improve the quality of our lives through enhancing health, safety, and convenience, including intelligent transportation [8], smart e-health care [18], distributed data markets [26], smart agriculture [25], intelligent edge surveillance [13], and more. Meanwhile, smart cities highly rely on an efficient and secure infrastructure, which has to meet various performance, security, and management demands through heterogeneous IoT applications across multiple administrative domains [30].

It becomes more evident that the existing homogeneous network infrastructure is not able to handle scalability and extensibility due to the rapid growth of IoT connections [11], [20]. In addition, it is difficult for a traditional centralized service framework to facilitate dynamic and heterogeneous IoT ecosystems that need optimal resource utilization and diverse Quality-of-Service (QoS) requirements [24]. Furthermore, unifying sensitive information among geographically scattered devices that belong to different domains also brings increasingly concerns on security and privacy.

As one of the key enabling technologies in the context of 5G, Network Slicing (NS) utilizes virtualization and softwarization to divide the physical network into multiple isolated logical networks (i.e, slices) with different network characteristics [24]. Through dynamic resource allocation among dedicated slices for heterogeneous IoT applications, NS is a promising method to improve scalability and dynamicity in a large scale of IoT network that satisfies various QoS demands [6], [10], [21]. Moreover, the isolation property of NS ensures performance and security guarantees [2]. Thus, NS facilitates mitigating impact of attacks like Distributed Denial-of-Service (DDoS) and protecting sensitive information collected by IoT devices.

Blockchain, a distributed ledger technology (DLT) [12], has demonstrated great potential to revolutionize various aspects of economy and society. Blockchain utilizes a decentralized architecture to securely store and verify data without relying on a centralized trust authority [29]. The decentralization of blockchain is promising to improve performance and reduce a single point of failure caused by a centralized service architecture. Moreover, leveraging consensus protocols to verify and record transactions on a immutable and transparent public distributed ledger, blockchain guarantees availability, correctness, and provenance for resource sharing (i.e, computing, storage and networking.) among untrusted participants in a multi-domain IoT system.

To improve scalability, dynamicity and security for multi-domain IoT applications, this paper proposes a

978-1-6654-9726-8/22/$31.00 ©2022 IEEE

secure-by-design and dynamic edge resource federation architecture based on NS and blockchain technologies. Integrating NS-enabled dynamic edge resource orchestration with federated ledger fabric [26], the Hierarchical Integrated Federated Ledger (HIFL) solution aims at an organic mutual reinforced networking service infrastructure. All physical edge resources are converted to virtual resources that are managed by domain specific slices. The multi-domain coordination federates these isolated slices that are dynamically designed, deployed and optimized according to service requirements and operating conditions. The federated ledger allows for a decentralized security fabric to enhance security and privacy-preserving properties in intra-slice and inter-slice resource orchestration and service inter-operations.

The remainder of this article is organized as follows. Section II introduce the background knowledge and related work of integrating NS and blockchain into IoT systems. In Section III, the system architecture of HIFL and main procedures are explained followed with descriptions of the main components and procedures in multi-domain orchestration. Section IV presents the preliminary prototype implementation and evaluation along with discussions on the open questions yet to be addressed. Section V concludes this paper.

## II. Background and Related Work

### A. Network Slicing for IoT

Network slicing concept in 5G is introduced by NGMN (Next Generation Mobile Network) in [4]. To assure service customization, isolation and multi-tenancy support, NS can divide a common physical network infrastructure into multiple logic networks called slices or subnets. Each NS slice is a unification of virtual resources, which run a set of virtual network functions and software defined network (SDN) settings for a specific communication service and business model. NS builds on top of key principles, like isolation, elasticity, automation and customisation, which are promising to improve scalability and dynamicity of heterogeneous IoT systems [2].

To support the intelligent allocation and dynamic adjustment of virtual resources in NS networks, adaptive virtual network slices for diverse IoT services is proposed to achieve vertical, horizontal and internetwork scaling purposes [10]. Given real-time resource utilization and performance requirements, adaptive resource adjustment algorithms can produce the output of new optimal values to re-allocate resources. NS may combine resources from different administrative domains. Thus, a multi-domain network slicing management and orchestration architecture is designed to enable efficient and dynamic federated resources allocation across domains [21]. Each domain uses sub-domain controllers to orchestrate and manage resources and Network Slice Subnet Instances (NSSI), while an global end-to-end slice coordinator unifies the management of federated domains. By using a brokering layer that relies on a graph-based resource database, a brokering architecture for network slicing is proposed to federate IT and edge resources owned by multiple third-party actors [6]. The proposed architecture [6] is implemented for the federation of a stadium infrastructure resources, and an author evaluates the time for resource federation, slice provisioning and slice activation.

### B. IoT-Blockchain Considerations

*Blockchain* initially was implemented as an enabling technology of Bitcoin [12], which aims to provide a cryptocurrency to record and verify commercial transactions among trustless entities in a decentralized manner. In a blockchain network, a large amount of miners or validators execute a consensus protocol under a Peer-to-Peer (P2P) network to ensure integrity, consistence and total order of data on the distributed ledger. Thanks to the decentralized network architecture and cryptographic security mechanisms, all trust-less participants in a blockchain system cooperatively maintain a security and trust framework instead of relying on a centralized third party trust authority. Emerging from the intelligent property, a *smart contract* (SC) encapsulates self-executing procedures recorded on the distributed ledger, Thus, a SC introduces programmability into blockchain to support various customized transaction logic rather than simple cash transactions [30].

Combining blockchain and a smart contract enables a secured and trust-free framework to facilitate data sharing and the federation of resources from third party actors. However, resources intensive consensus algorithms, like Proof-of-Work (PoW) and its variants, are not affordable for IoT devices that are strictly constrained by computation and storage capacity. Using a Practical Byzantine Fault Tolerance (PBFT) [7] protocol can achieve high throughput, lower latency and limited computation overhead; however, it cannot scale up to a large consensus network. Moreover, IoT devices are managed by different administrative domains with diverse performance and security requirements. Therefore, a monolithic blockchain network cannot perfectly ensure decentralization, scalability and security for dynamic and heterogeneous IoT systems across multiple domains.

### C. Lightweight Distributed Ledgers for Edge Networks

The inherent security guarantees of blockchain provide the foundations of a serverless record-keeping without the need for centralize trusted third-party authorities [3]. Transparency, immutability and auditability ensure resilience, correctness, and provenance for all data sharing among untrusted participants. Many efforts try to leverage blockchain to support security features required in IoT systems. IoTChain [5] proposes a three-tier blockchain-based IoT architecture, which allows regional nodes to perform any lightweight consensus, like Proof-of-Stake (PoS) and PBFT. IoTChain only provides simulation results on communication cost of transactions; however key metrics in the consensus layer, like computation, storage and throughput, are not considered. FogBus [22] proposes a lightweight framework for integrating blockchain into fog-cloud infrastructure, which aims to ensure data integrity as transferring confidential data over IoT-based systems. In FogBus, master nodes deployed at the fog layer are allowed to perform PoW mining, while IoT devices send transactions to master nodes as trust intermediates to interact with blockchain. However, using PoW as the backbone consensus protocol still results in high energy consumption and low throughout.

HybridIoT [19] proposes a hybrid blockchain-IoT architecture to improve scalability and interoperability among sub-blockchains. In HybridIoT, a BFT interconnector framework works as a global consortium-blockchain to link multiple PoW sub-blockchains. However, using PoW consensus in sub-blockchain networks still brings computation and storage overhead on IoT devices if they are deployed as full nodes. IoTA [9] aims to enable a cryptocurrency designed for the IoT industry, and it leverages a directed acyclic graph (DAG), called tangle [17], to record transactions rather than chained structure of the ledger. IoTA provides a secure data communication protocol and zero fee micro-transaction for IoT/machine-to-machine (M2M), and it demonstrates high throughput and good scalability. However, existing IoTA networks still rely on hard-coded coordinators, which employ PoW to finalize path of recorded transactions in DAG.

Unlike the above mentioned IoT-Blockchain solutions, which either adopt computation intensive PoW as their backbone consensus mechanism or rely on a intermediate fog layer to execute consensus protocol, HIFL aims at a partially decentralized, lightweight hierarchical blockchain network fabric that is customized for a dynamic network slice in a highly heterogeneous edge computing environment. In addition, HIFL will form an organic network fabric of the network slices, not merely taking advantage of blockchain as a time-stamped series of data records, but can also serve as network slice brokers [15], [23], [31].

## III. HIFL: Rationale and Design

### A. System Architecture Design

Aiming at a self-adaptive, secure-by-design and partial decentralized networking service architecture, the HIFL solution takes advantage of NS and blockchain technologies to enable efficient and scalable edge resources federation and orchestration under heterogeneous multi-domain IoT environments. The proposed HIFL architecture is depicted in Figure 1 with two distinct sub-frameworks.

(1) *Multi-domain Coordination*: adopts a dynamic edge resource federation paradigm with NS as an enabling technology. The virtualization layer abstracts all physical edge resources to virtual resources according to functionalities, like computing, storage and network connectivity. Each domain specific slice manages virtual resources within a domain and provides interfaces to upper level multi-domain coordination. A software-defined network (SDN) controller provides network connectivity and service chaining among allocated Virtual Networ Functions (VNF). VNF Management and Orchestration (MANO) manages the VNFs along with required virtual computing and storage resources. Dynamic resource orchestration depends on customer/user requirements and system performance monitoring. By federating virtual resources managed by different domain specific slices, multi-domain orchestration relies on intelligent algorithms to achieve fast resource deployment and efficient services re-adjustments with diverse QoS and security requirements.

(2) *Federated Ledger*: provides a decentralized security fabric to guarantee security and privacy-preserving in data and resource sharing across different domains. In a specific domain, a random elected committee executes an efficient BFT-based consensus protocol to verify and record data on a private intra-domain ledger. Because each domain is a permissioned network, only authorized users are allowed to access data on an intra-domain ledger. Moreover, running BFT consensus protocol by a small scale validator committee can achieve low latency and high throughput of transactions. Such an intra-domain ledger blockchain network supports partial decentralization at the network of edge with performance and privacy-preserving guarantees. At the multi-domain level, a public inter-domain ledger network federates fragmented intra-domain ledger networks, and it uses a scalable PoW consensus to secure cross-domain operations. For multi-domain operations, the public inter-domain ledger only records checkpoints data that indirectly refer to raw data on private intra-domain ledgers. Therefore, the NIFL federated ledger structure is promising to ensure scalability and security without sacrificing performance and privacy requirements of individual domains [26].

### B. Dynamic Resource Orchestration

The dynamic resource orchestration uses federated NS Instances (NSIs) to support end-to-end connectiv-

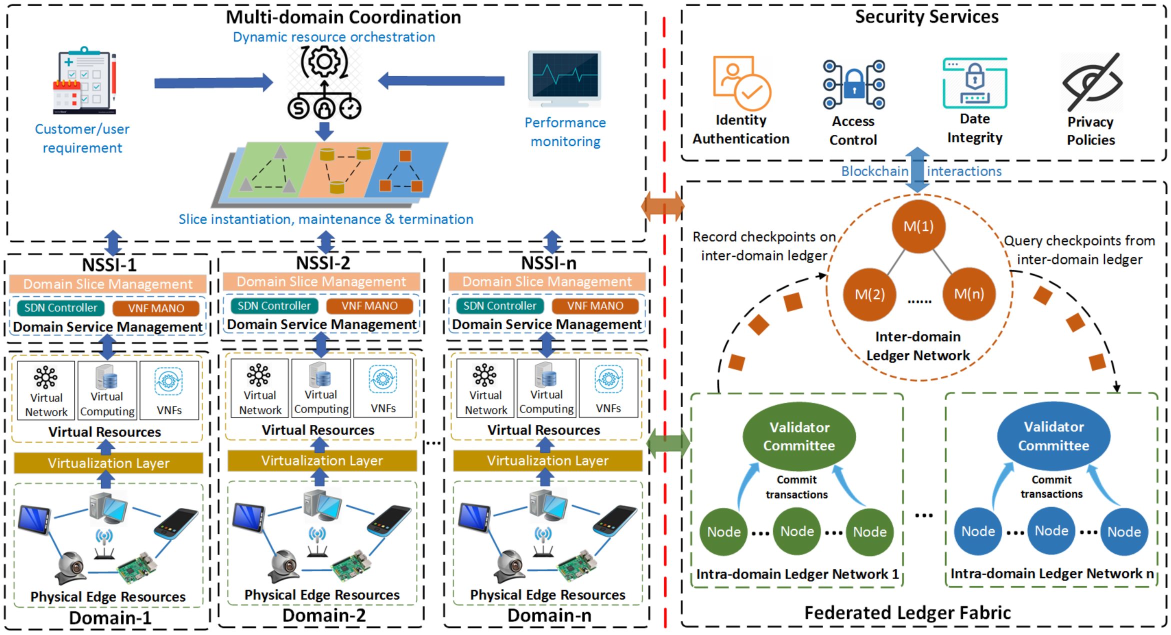

Fig. 1. Illustration of system architecture consisting of multi-domain service coordination and federated ledger fabric.

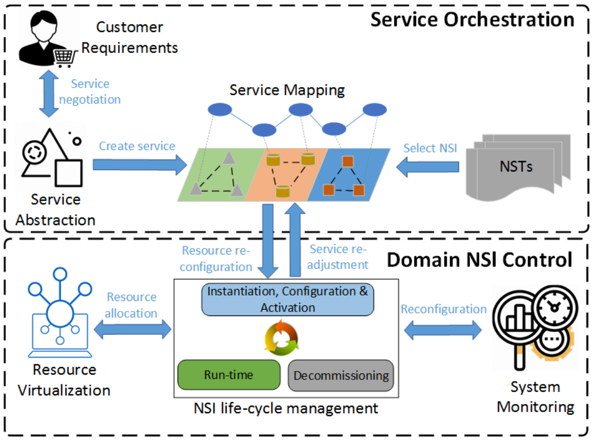

Fig. 2. The dynamic resource orchestration mechanism.

ity for multi-domain applications. Given continuously analyzing service and monitoring performance, NSIs carry out resource allocation and service re-adjustment to ensure desired requirements. An overview of multi-domain service orchestration and domain NSI control is shown in Figure 2. The dynamic resource orchestration happens if 1) customers/users launch service requests; or 2) running services with allocated resources cannot fulfill desired performance.

1) After receiving customer requirements, Service Orchestration (SO) firstly negotiates with verticals and service providers on admission control and charging. Then, SO decomposes and abstracts services toward different administrative domains. Given current unified resources of the system, service mapping process selects appropriate NS templates (NSTs) to create a service graph that is sent to domain NSI control for resource configuration. The domain NSI control allocates virtual resources for new NS instantiation. After configuration and activation, an NSI becomes run-time that supports functionalities of service and reports performance.

2) When system monitoring detects performance degradation due to insufficient resource or service configurations, domain NSI's control will send service re-adjustment requests to service orchestration. The service mapping process may modify service specific parameters, and/or allocate more topology, links and computing resources. Then it sends resource re-configuration to domain NSI control, which is responsible for instantiating, modifying or decommissioning NS to meet on-demand requirements in service providing time.

## C. Blockchain based Security Mechanism

The identified threads and probable points of attack for network slicing can be categorized as: life-cycle security, intra-slice security and inter-slice security [16]. Figure 3 summarizes the representative threats and explains how blockchain can be used to enhance security proprieties of dynamic edge resource federation framework.

*Slice life-cycle Attack*: An adversary can modify NS templates in preparation phase or change configuration when new slices are instantiating given on-demand service requests. The access violation may happen in slice run-time phases such that unauthorized entities can

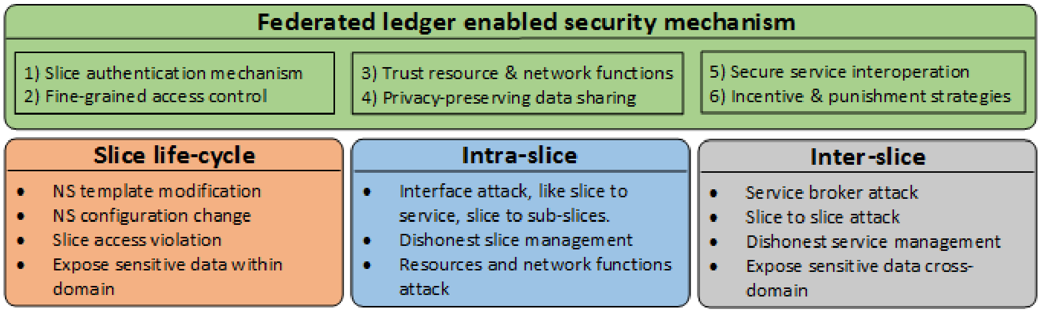
Federated ledger enabled security mechanism
1) Slice authentication mechanism
2) Fine-grained access control
3) Trust resource & network functions
4) Privacy-preserving data sharing
5) Secure service interoperation
6) Incentive & punishment strategies
Slice life-cycle
• NS template modification
• NS configuration change
• Slice access violation
• Expose sensitive data within domain
Intra-slice
• Interface attack, like slice to service, slice to sub-slices.
• Dishonest slice management
• Resources and network functions attack
Inter-slice
• Service broker attack
• Slice to slice attack
• Dishonest service management
• Expose sensitive data cross-domain

Fig. 3. Blockchain based security mechanism for dynamic edge resource federation.

conduct performance and DoS attacks by changes in configuration or even deactivation of slices. Moreover, improper decommissioning handles may expose sensitive data of resource providers within a domain.

For each domain assuming that the domain administrator is a trust oracle, a dedicated intra-domain ledger network relies on permissioned management to provide flexible authentication primitives, like identity verification [28] and access control [27]. It is promising to prevent against unauthorized access to data and resource as well as performing malicious operations under a dynamic network condition. Moreover, slice template and instance information can be recorded on an immutable and auditable intra-domain ledger storage. Thus, a decentralized data integrity scheme [14] supports authenticity and integrity verification for slices, to prevent fake or modified slice instances when new resources join or leave the system.

*Intra-slice Attack*: Slices within a domain also expose vulnerabilities on interfaces between services and sub-slices. Moreover, a slice manager collects resources and network functions shared by different providers. Thus, it needs audit participants' behaviors to identify dishonest activities. The intra-domain ledger provides a trust free platform that all authorized participants can verify data on the distributed ledger without relying on any third-party agency. By properly designing authentication and access control strategies, the intra-domain ledger can guarantee privacy-preserving data and resource sharing among untrusted providers.

*Inter-slice Attack*: Considering inter-slice scenarios, an adversary can compromise service brokers to interrupt multi-domain coordination, or use authorized slices to gain access to other unauthorized slices. Moreover, it may leak sensitive data during inter-slice operations. The HIFL federated ledger leverages a cryptographic secure inter-ledger transaction (tx) protocol to guarantee auditability and provenance of multi-domain tasks without exposing sensitive data on intra-domain ledgers. Moreover, incentives and punishment strategies by blockchain motivate more honest participants to join the system and gain benefits in data and resources sharing.

TABLE I
CONFIGURATION OF EXPERIMENTAL DEVICES.

| **Device** | Dell Optiplex-7010 | Raspberry Pi 4 (B) |
|---|---|---|
| **CPU** | Intel Core TM i5-3470 (4 cores), 3.2GHz | Broadcom ARM Cortex A72 (ARMv8), 1.5GHz |
| **Memory** | 8GB DDR3 | 4GB SDRAM |
| **Storage** | 350G HHD | 64GB (microSD card) |
| **OS** | Ubuntu 16.04 | Raspbian GNU/Linux (Jessie) |

## IV. PROOF-OF-CONCEPT PROTOTYPE EVALUATION

To study the feasibility of proposed HIFL solution, we implemented a conceptual prototype of resource federation that simulates a video surveillance system including two administrative domains. Table I shows configuration of devices for prototype setup. Each domain consists of 10 Raspberry Pi-4 (RPi) devices that provide edge resources and a Dell Optiplex-7010 desktop as a domain manager. We use Tendermint core [1] to build a intra-ledger network for each domain, and all RPis within a domain also act as validators to execute an efficient BFT protocol and maintain its intra-domain ledger. A private Ethereum network is used to simulate a inter-domain ledger network, where 4 miners are deployed on separate desktops and each has Intel(R) Core(TM) 2 Duo CPU E8400 @ 3 GHz and 4 GB of RAM. All desktops and RPis are connected through a local area network (LAN).

### A. Numerical Results

Table II provides a set of comparative numeral results by querying or recording data on intra-domain and inter-domain networks separately. 100 test runs have been conducted for each test scenario and we use the average value to show performance. Because querying data from an inter-domain ledger uses smart contract as enable technology, such that it needs more processing time than intra-domain ledger does. In addition, the HIFL

TABLE II
COMPARATIVE EVALUATION OF COMMITTING TRANSACTIONS ON FEDERATED LEDGER NETWORKS.

| | Intra-domain | Inter-domain |
|---|---|---|
| **query data (ms)** | 18 | 110 |
| **record data (s)** | 1.6 | 4.5 |
| $tx$ **throughput (tx/s)** | 625 | 127 |
| **CPU usage (%)** | 100 | 32 |
| **Memory usage (MB)** | 1,200 | 80 |
| **Gas/**$tx$ **(Ether)** | 0.001 | × |

intra-domain ledger relies on an efficient BFT consensus protocol, which achieves lower latency and higher transaction throughput as recording data on distributed ledger. Thus, HIFL is able to satisfy time sensitive and high throughput requirements in specific domain networks. Moreover, the inter-domain ledger is mainly to guarantee scalability, auditability and global security for cross-domain operations. Therefore, 4.5 s transaction latency and 127 tx/s transaction rate is acceptable for majority of inter-domain scenarios.

To evaluate resource consumption as validators and miners run on host machines, we use "top" command to monitor CPU and memory usages by consensus processes on desktop and RPi. The Ethereum miner uses a computation intensive PoW mining algorithm such that needs full capacity of a CPU core and consumes about 1.2GB memory. As a result, miners can only be deployed on the powerful platforms, like edge or fog servers. Due to lightweight BFT consensus algorithm that achieves efficiency in CPU and memory usage, it's affordable for IoT devices to work as validators in intra-ledger networks. Ethereum network requires gas fees that are used to reward miners who commit transactions on the inter-ledger. It introduces extra financial cost on inter-ledger transactions, which is \$1.23/$tx$ according to Ether price of the public Ethereum market at Jan 22, 2021. However, intra-ledger transactions do not require transaction fees, and each domain can design their own rewarding strategies for participants.

### B. Discussions

This paper focuses on the design rationale and principles of the HIFL solution. In terms of completeness, it is an introduction of a work-in-progress. There are a lot of open questions yet to be answered and limitations of the current proof-of-concept prototype.

Basically, HIFL takes advantages of properties of NS and blockchain to achieve multi-domain dynamic edge resources orchestrations and service re-adjustments on a physically distributed infrastructure. Actually HIFL still relies on a partially decentralized network framework owing to a logically centralized administrative management for domain-specific NS and VNF.

In addition, HIFL is a promising basic abstract architecture to address issues in distributed, dynamic and heterogeneous cross-domain IoT systems. Because of the high diversity in the smart cities application domain and the design of NS itself is highly application dependent, implementations based on certain specific real-life applications are necessary to gain deeper insights and demonstrate practical benefits of using HIFL. On top of a preliminary proof-of-concept prototype that is built leveraging our earlier work on intelligent public safety surveillance, we have obtained some numerical results that evaluate general performance in terms of network latency and processing overhead. Due to limited efforts, however, we have not validated security and privacy properties given possible attack scenarios. We leave aforementioned issues to future work.

## V. CONCLUSIONS

This paper proposes HIFL - a partially decentralized and secure-by-design dynamic edge resource federation architecture atop of multi-domain IoT systems. Experimental results based on a proof-of-concept prototype demonstrate the feasibility of applying the HIFL solution in smart cities scenarios, like smart video surveillance systems. While the HIFL experimental results are encouraging, what we have presented in this paper is merely an initial conceptual design and some preliminary study results. There are many open questions are yet to be solved before the HIFL architecture becomes applicable in real-world smart cities applications. Our current ongoing efforts mainly focus on the design of an efficient dynamic edge resource orchestration mechanism and an approach for the evaluation on the performance and security features in a large scale IoVT network.

## ACKNOWLEDGEMENT

This work is supported by the U.S. National Science Foundation (NSF) via grant CNS-2141468 and the U.S. Air Force Office of Scientific Research (AFOSR) Dynamic Data and Information Processing Program (DDIP) via grant FA9550-21-1-0229. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U. S. Air Force.

## REFERENCES

[1] "Tendermint core," https://docs.tendermint.com/master/.

[2] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[3] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[4] N. Alliance, "5g white paper," *Next generation mobile networks, white paper*, vol. 1, 2015.

[5] Z. Bao, W. Shi, D. He, and K.-K. R. Chood, "Iotchain: A three-tier blockchain-based iot security architecture," *arXiv preprint arXiv:1806.02008*, 2018.

[6] A. Boubendir, F. Guillemin, C. Le Toquin, M.-L. Alberi-Morel, F. Faucheux, S. Kerboeuf, J.-L. Lafragette, and B. Orlandi, "Federation of cross-domain edge resources: a brokering architecture for network slicing," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 415–423.

[7] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999, pp. 173–186.

[8] N. Chen and Y. Chen, "Anomalous vehicle recognition in smart urban traffic monitoring as an edge service," *Future Internet*, vol. 14, no. 2, p. 54, 2022.

[9] IOTA Foundation, "IOTA Data Marketplace," https://data.iota.org, accessed: Jan. 2, 2020.

[10] V. P. Kafle, Y. Fukushima, P. Martinez-Julia, T. Miyazawa, and H. Harai, "Adaptive virtual network slices for diverse iot services," *IEEE Communications Standards Magazine*, vol. 2, no. 4, pp. 33–41, 2018.

[11] W. Kassab and K. A. Darabkh, "A–z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, p. 102663, 2020.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[13] S. Y. Nikouei, Y. Chen, S. Song, B.-Y. Choi, and T. R. Faughnan, "Toward intelligent surveillance as an edge network service (isense) using lightweight detection and tracking algorithms," *IEEE Transactions on Services Computing*, vol. 14, no. 6, pp. 1624–1637, 2019.

[14] S. Y. Nikouei, R. Xu, D. Nagothu, Y. Chen, A. Aved, and E. Blasch, "Real-time index authentication for event-oriented surveillance video query using blockchain," in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–8.

[15] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5g services," *IEEE Networking Letters*, vol. 1, no. 3, pp. 99–102, 2019.

[16] R. F. Olimid and G. Nencioni, "5g network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99 999–100 009, 2020.

[17] S. Popov, "The tangle," *cit. on*, p. 131, 2016.

[18] A.-M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen, "Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems," in *2015 12th annual IEEE consumer communications and networking conference (CCNC)*. IEEE, 2015, pp. 826–834.

[19] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1007–1016.

[20] N. Srinidhi, S. D. Kumar, and K. Venugopal, "Network optimizations in the internet of things: A review," *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 1–21, 2019.

[21] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," *IEEE Network*, vol. 33, no. 5, pp. 242–252, 2019.

[22] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "Fogbus: A blockchain-based lightweight framework for edge and fog computing," *Journal of Systems and Software*, vol. 154, pp. 22–36, 2019.

[23] K. Valtanen, J. Backman, and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5g network slice brokering case," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2018, pp. 185–190.

[24] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[25] Y. Xing, S. Lei, C. Jianing, F. M. Amine, W. Jun, N. Edmond, and H. Kai, "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273–302, 2021.

[26] R. Xu and Y. Chen, "Fed-ddm: A federated ledgers based framework for hierarchical decentralized data marketplaces," in *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–8.

[27] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot," *Computers*, vol. 7, no. 3, p. 39, 2018.

[28] R. Xu., Y. Chen, E. Blasch, and G. Chen, "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," *Optical Engineering*, vol. 58, no. 4, p. 041609, 2019.

[29] R. Xu, D. Nagothu, and Y. Chen, "Decentralized video input authentication as an edge service for smart cities," *IEEE Consumer Electronics Magazine*, 2021.

[30] R. Xu, S. Y. Nikouei, D. Nagothu, A. Fitwi, and Y. Chen, "Blendsps: A blockchain-enabled decentralized smart public safety system," *Smart Cities*, vol. 3, no. 3, pp. 928–951, 2020.

[31] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "Nsbchain: A secure blockchain framework for network slicing brokerage," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–7.