“THEME ARTICLE”, “FEATURE ARTICLE”, or “COLUMN” goes here: The theme topic or column/department name goes after the colon.

Realization of Blockchain in Named Data Networking-based Internet-of-Vehicles

Farhan Ahmad*, Chaker Abdelaziz Kerrache, Fatih Kurugollu*, Rasheed Hussain*****
*Cyber Security Research Group, College of Engineering and Technology, University of Derby, United Kingdom

** Department of Mathematics and Computer Science, University of Ghardaia, Algeria

*** Institute of Information Systems, Innopolis University, Russia

The revolution of Internet-of-vehicles (IoV) has stimulated a substantial response from academia, research and industry due to its massive potential to improve overall transportation. Current IoV faces huge challenges due to its reliance on the IP-based network architecture. Therefore, Named Data Networking (NDN) is proposed as a promising architecture to solve issues posed by IP-based systems. Recently, Blockchains (BCs) are utilized within IoV to increase network security. However, the integration of BC within NDN-enabled IoV is still an open research problem. In this study, we proposed a novel tier-based architecture known as “Blockchain in NDN-enabled Internet-of-Vehicles (BINDN)” which can support BC within NDN-enabled IoV. BINDN can be used as a reference architecture to design security solutions in NDN-enabled IoV using BC. Further, it provides an extensive set of applications including IoV security, trust management and privacy enhancements. Moreover, we highlighted major challenges and issues when integrating BC within NDN-enabled IoV.

INTRODUCTION

Internet-of-things (IoT) has emerged as a ground-breaking technology over the past decade which enabled every device with communication, computing and storage capability to connect to the Internet, thus, presenting a plethora of applications including smart cities, smart grids, smart e-healthcare and smart transportation

[1]. In the domain of transportation, IoT has evolved into Internet-of-Vehicles (IoV) where smart vehicles are equipped with a wide range of sensing, computing and storing capacities to ensure safer transportation, better fuel utilization, infotainment and efficient journey times. This technology broadens the vision of vehicles and enables them to take right decisions under such time-sensitive and critical circumstances.

One of the main driver of IoV success relies on the successful delivery of messages among vehicles in a secure and trusted environment. Current IoV follows a point-to-point (P2P) communication paradigm where messages are propagated from source to destination based on the IP addresses of the vehicles. However, IoV applications mostly follows a point-to-multi point (P2M) communication pattern where messages broadcasted by one vehicle is shared with all the neighbouring vehicles.

To address this issue, Named Data Networking (NDN) is proposed as an innovative Internet architecture, which follows a principle that content (data) itself is more vital than content provider [2]. NDN fits with the philosophy of IoV as every participating vehicle has the opportunity to get desired data, thus, enabling them to take timely decisions on the road to ensure traffic safety. NDN incorporates two types of messages, i.e., "'Interest" and "Data" packets. First, the source vehicle generates *interest* packet in search of the content, which NDN core disseminates across the network to share with the respective vehicles in specific region. Any vehicle having the requested content shares it with the source vehicle by issuing *data* packets, which then propagates over the same NDN network. This efficient technique makes NDN a suitable solution to support large-scale IoV.

As mentioned earlier, IoV mostly constitutes safety content in the network that must be shared with the source vehicle without any alteration. However, as IoV is a large-scale and decentralized network, the probability of attacker presence cannot be ruled out completely. Recently, Blockchain (BC) is proposed as a decentralized and auditable network where every participating node can add or modify data only after solving a complex puzzle, thus, providing a security-by-design architecture. BC, originally designed for financial industry, is already revolutionizing the IoT industry including healthcare [3], supply chain [4] and logistics [5]. However, for a highly mobile network like IoV, BC is still in its early stage of research such as [6], where BC is used to manage user's reputation within VANET.

In BC-based IoV, vehicles can only modify the block data after solving Proof-of-Work (PoW) consensus algorithm, which enables them to disseminate legitimate content throughout the network. For NDN-enabled IoV, BC can be a revolution as it provides security by design architecture due to its decentralized nature. However, to the best of our knowledge, BC is not utilized within NDN-enabled IoV for this specific purpose. Therefore, in this study, we integrated BC within NDN-enabled IoV for secure message dissemination among the participating vehicles. The major contributions of this study are two-fold:

- We propose a new architecture to support BC in NDN-enabled IoV **(BINDN)**, and
- We highlight several open research challenges to tackle the integration of BC within NDN-enabled IoV.

BACKGROUND OVERVIEW

Unlike classical vehicular networks (VANETs) from which IoV has recently evolved, as illustrated in Figure 1, each vehicle is considered as a smart object (smart vehicle) equipped with multiple communications technologies, a powerful multi-sensor platform, computation units, IP-based connectivity to the Internet and to the other vehicles either directly or indirectly. Further, every vehicle in IoV is equipped with multi-communication modules that enable them to interact with various in-vehicle components (sensors, on-board units), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-people (V2P) to provide different applications [7]. However, majority of IoV applications are information-centric [8], where vehicles seek specific information with time and location constraint without taking into account who is the owner/producer of this information. This is exactly the principle of Named Data Networking.

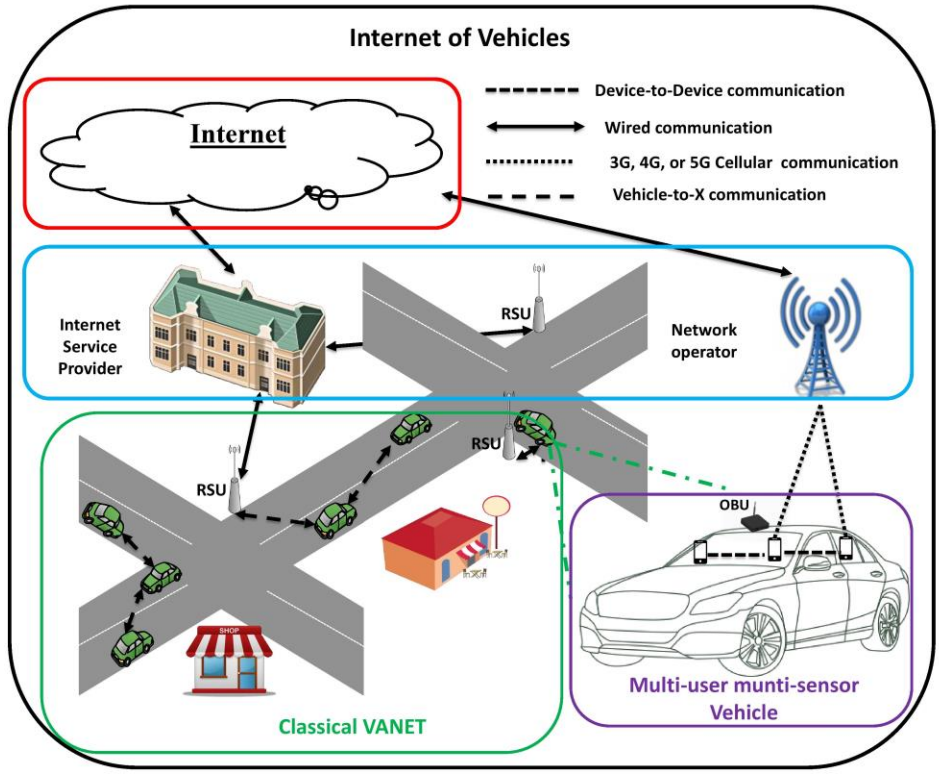

Fig. 1. Internet of Vehicles

In conventional TCP/IP, nodes must get an IP address prior communication. NDN is a clean-slate future internet architecture that names the data, not the hosts [9]. It incorporates two types of packets, a broadcasted "Interest" packet and as response a unicasted "Data" packet. One of the main advantages of NDN is that the routers in addition to the pending Interest Table (PIT) and the list of interfaces represented by the Forwarding Information Base (FIB), they also store copies of the delivered data in their caches called Content Store (CS). Thus, a new data requester may receive the data directly from the nearest intermediate router. Since most of IoV applications are data-centric, efficient transportation system should be realized over this data-centric networking vision [10]. However, besides the heterogeneity of IoV technology, the realization of IoV over NDN will cause many other security challenges.

To address this question, Blockchain can be utilized which is recently proposed as an innovative solution to ensure the desired security level in the network [11]. It was the reason behind the cryptocurrency. However, BC has many other applications besides financial industry [11]. The idea of BC was to transform from a centralized, costly and slow information systems to alternative systems that are fully distributed and efficient in response time, with low-cost. The main concept in BC is the "open ledger" representing a publically shared ledger containing all the information transfer divided into chained blocks. Thus, the open ledger content is distributed across all the nodes in the network. These nodes are called "Miners" [12]. To ensure the synchronization among the distributed copies of the open ledger, a node 'A' willing to transfer an information to another node 'B' broadcast this 'invalidated transfer' to the networks. Afterwards, the miners will compete among themselves to tackle the invalidated transfer and be able to validate and record it into the ledger. The first miner will get a 'reward' for the successful transaction within the BC. To complete the transfer, a miner should be able to validate it and then find the special key that enable the miner to take the previous transfer and lock with it the new transfer. As the search for the key is random, BC requires every miner to invest intensively in terms of computation power and time. The wining miner will then publish the validated transfer together with the found lock so that all other miners will add it to the copies of the ledger. All validated transfers are grouped in chained blocks with a fixed capacity [13].

In the following, we present our architecture called 'BINDN' for the realization of Blockchain in NDN-based IoV.

INTEGRATION OF BLOCKCHAIN IN NDN-BASED IOV

"BINDN"' which is based on BC within NDN-enabled IoV is depicted in Figure 2. It is a five-tier architecture, which consists of five distinct levels, spanning over both mobile vehicles and static infrastructure.

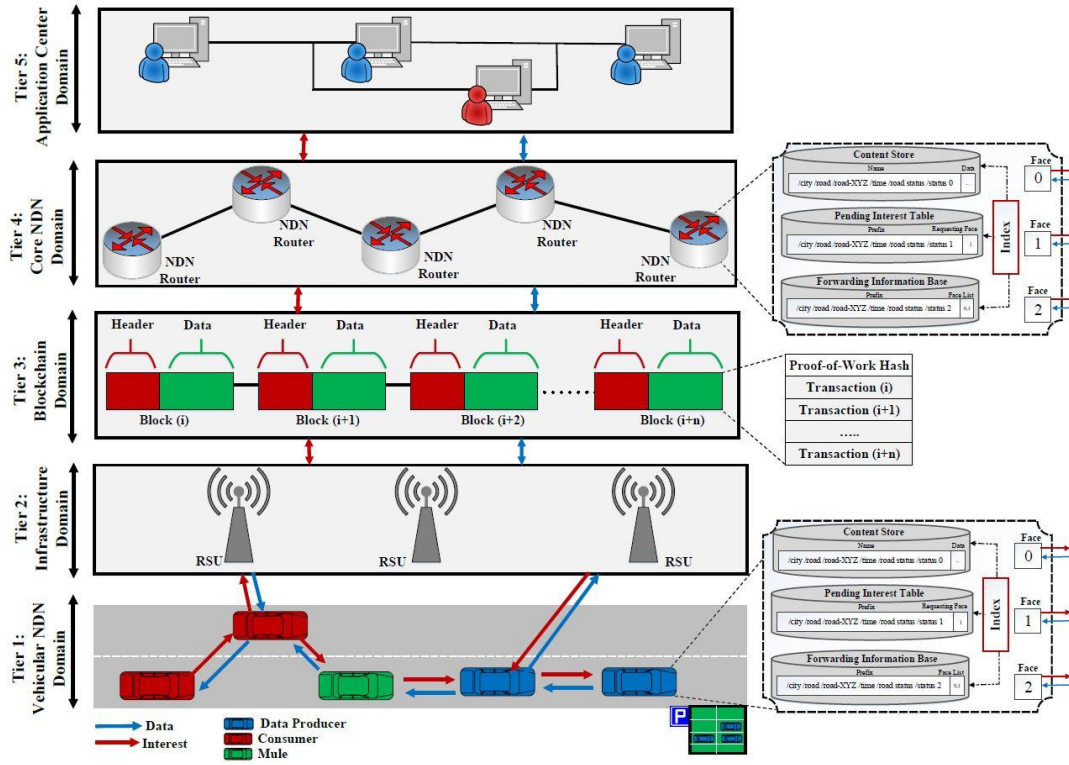

Fig. 2. Proposed Architecture for Blockchain-enabled NDN-IoV

Vehicular NDN (VNDN) Domain

This tier represents the mobile aspect of BINDN, where, information generated by the vehicles are shared using V2V communication. This tier constitutes three types of vehicles, i.e., Consumer, Producer, and Mule [14]. The consumer generates an *Interest* packet in search of information (such as, parking space in the neighbourhood) which is shared with neighbouring vehicles via V2V communication, where every vehicle first checks its "'Content Store (CS)". If the requested information is present in CS, then the *Data* packet is sent back to the requesting consumer. If the data is missing in the CS, then Interest packet is forwarded to "Pending Interest Table (PIT)". If the requested information is missing in PIT, then, the requested information is not present at this vehicular node. Thus, the "Forwarding Information Base (FIB)" of the vehicles forwards the Interest packet towards other nodes and creates a PIT entry to keep track of the packets. The producers generate *Data* packets if they have the requested information, which follows the same route towards the consumer using PIT entries. The mules in the network acts opportunistically and are used to exchange packets between source and destination [15]. This tier is helpful for infotainment applications such as parking information where the vehicles can share the information using V2V mode of communication.

Infrastructure Domain

This second tier of BINDN constitutes the static units of the network, i.e., Roadside units (RSUs). This tier is responsible for sharing information for bandwidth and data hungry applications such as on-demand videos which is achieved via V2I communication. In this tier, RSUs act as message gateways, where the information provided by the vehicle is shared with tier-3 to record data within the BC. As IoV includes both legitimate and malicious nodes due to its large-scale nature, , the information provided by the malicious RSU will be identifiable as the miners at the back-end will identify the compromised content during its verification process, while, data provided by the legitimate RSU will be able to append within BC after verification by the miners.

Blockchain Domain

This tier lies between infrastructure domain and the core NDN domain, and is responsible to perform all the BC related tasks. In this domain, the *Miners* are elected first which are responsible to add transactions in the BC. These miners are elected after solving a complex consensus algorithm, which can be either proof-of-work (PoW) or proof-of-stake (PoS) etc. When the information is transmitted from vehicle via RSU, the *Miners* validates and adds the information to the BC. The block in BINDN has two major components, i.e., (1) Block header, and (2) Block data. *Header* contains the Proof-of-Work Hash, which includes control related information such as version number, nonce value, previous block, time stamps and merkle trees. On the other hand, *Data* field constitutes the list of transactions, which are recorded by the miners after validating the received information.

Core NDN Domain

This domain represents the core structure of traditional NDN that mostly constitutes of NDN routers and lies in the back-end wired networks. As mentioned earlier, every NDN router is equipped with three distinctive data structures, i.e., CS, PIT and FIB. This domain continuously collaborate with tier-3 where blocks created by the miners are forwarded and routed via this core NDN domain in search of the data. This tier is very helpful for delay-tolerant applications including on-demand and YouTube videos [16]. The node possessing the requested data is transmitted back to the requesting vehicle via BC and RSU.

Application Center (AC) Domain

This is the final tier of the BINDN, which resides in the deep back-end networks. This contains the service providers, which are providing different applications to the users in order to improve their transportation experience, such as on-demand videos, online-banking and traffic information etc. Since, the data is encapsulated using BC, therefore resulting in a security-by-design architecture. When an Interest is received at the AC domain, the data is provided back to the requesting vehicle via BC.

In short, BINDN provides a reference architecture, where a wide range of IoV applications can be realized using NDN and BC. Specifically, BINDN follows a security-by design approach, thus, it can provide security applications for IoV such as trust and reputation management.

RESEARCH CHALLENGES AND OPEN ISSUES

In this section, we discuss various research challenges, which could surface as a result of integrating BC within NDN-based IoV.

Cross-platform Authentication and Authorization

Multi-layer authentication is at the core of this architecture and the fact that the architecture uses different communication paradigms, make it more challenging. For instance, IoV use distinct authentication mechanisms for safety and non-safety applications. In case of NDN-enabled BC-based IoV, the authentication at vehicular level can be different from authentication at a BC level. The same argument holds for authorization and access control as well. Therefore, a seamless authentication and authorization mechanism is essential for this architecture. One way could be a private BC with restriction and special privileges for the subscribed nodes and implementation of single sign-on like mechanism. More investigation is needed in this direction.

Revocation

Revocation is the pinnacle of the conditional privacy protection. In the NDN-enabled BC-based IoV, revocation is not only identity revocation, but also privileges and access rights. With the heterogeneity of different communication paradigms, the revocation must take into account the role of revokee in these environments. To this end, an efficient, scalable and robust revocation mechanism is required in IoV. It is worth noting that the revocation functionality is usually distributed between the entities of the network. As a result, the revocation management could be distributed among different stakeholders of the IoV management.

Fairness in Miner Election

One of the inherent problems from the BC is the mining. Miners are the entities that get a specific portion of the transaction, and therefore the role of miners must be regulated according to the application requirements. Furthermore, the selection of miners must take all the requirements from IoV application into account such that tolerable delay, cost, bandwidth, and so forth. Economic investigation is also necessary in this case, to discuss the Return on Investment (RoI) of the IoV applications. We regard this as a future work.

Optimization of Consensus and PoW Algorithms

The interconnection time among vehicles in IoV is unpredictable due to the ephemeral nature of communication. As a result, the consensus mechanisms for BC will be adversely affected if there is not enough time for the nodes to be in contact. Furthermore, the setup of consensus and then PoW for each node should also be both efficient and fair. Furthermore, it is also important to look into emerging BC mechanisms that are more suited for resource-constrained environments. We believe that research investigation in this direction will answer the pending questions.

Reputation and Trust Management

Sharing right information is of paramount importance in IoV. Trust is one way to make sure that right information is shared by the nodes. Each node establishes and manages trust with its neighbors. For efficient and robust trust management, the participating nodes must have communication with the neighbors for a considerable time. On the other hand, for intermittent networks such as IoV, recommendation is established based on neighbors. However, in the current heterogeneous environment, trust management must take into account the other enabling technologies as well (for instance IoT and BC). The trust management should be formalized as focal point taking into account the integrating communication mechanisms. More in-depth research is needed in this direction.

Public Key Infrastructure Management

NDN-enabled BC-based IoV use cryptographic primitives for different purposes such as authentication, confidentiality, communication security and so on. Keeping in mind different security requirements across different platforms, both key establishment and Public Key Infrastructure (PKI) management is required. The PKI management is an inherent issue in IoV and in case of its integration with other technologies; it will need thorough investigation and optimal solutions to reap the advantages of NDN, IoV, and BC. On the other hand, each node may have to manage multiple keys for different kinds of communications; therefore, it is of utmost importance to have a robust PKI mechanism that can function efficiently in highly mobile and heterogeneous IoV.

CONCLUSION

NDN is a promising Internet architecture, which can improve both the safety and non-safety aspects of the IoV. In this article, we introduced blockchain as a security parameter to secure the overall NDN-enabled IoV. Specifically, we proposed a novel tier-based architecture, which relies on three distinct technologies including BC, NDN and IoV. Particularly, we envisioned the advantages offered by BC within NDN-enabled IoV to increase the network efficiency in terms of security and information dissemination among the vehicles.

In a nutshell, the integration of NDN-enabled IoV with BC is ambitious and is poised to solve the existing problems of the IoV security as well as increase the spectrum of services and applications. However, the aforementioned challenges must be solved beforehand.

REFERENCES

1. Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran and S. Guizani, “Internet-of-Things-Based Smart Cities: Recent Advances and Challenges”, in *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16-24, Sept. 2017. doi: 10.1109/MCOM.2017.1600514
2. Named Data Networking. NDN Project Overview. Available online: *https://named-data.net/project/* (Accessed: 28th November, 2018)
3. H. Wu and C. Tsai, “Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing*”, IEEE Consumer Electronics Magazine*, 7(4):65–71, July 2018.
4. D. Miller, “Blockchain and the Internet of Things in the Industrial Sector”, *IEEE IT Professional*, 20(3):15–18, May 2018.
5. G. Perboli, S. Musso, and M. Rosano, “Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases”, *IEEE Access,* 6:62018–62028, 2018
6. H. Khelifi, S. Luo, B. Nour, H. Moungla and S. Hassan Ahmed, "Reputation-Based Blockchain for Secure NDN Caching in Vehicular Networks," *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, Paris, 2018, pp. 1-6.
7. J. Contreras, S. Zeadally, and J. A. Guerrero-Ibañez, “Internet of Vehicles: Architecture, Protocols, and Security”, *IEEE Internet of Things Journal*, 2017.
8. P. TalebiFard, V. CM Leung, M. Amadeo, C. Campolo, and A. Molinaro, “Information-centric Networking for VANETs” *In Vehicular ad hoc Networks*, pages503–524. Springer, 2015.
9. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, KC Claffy, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang, “Named Data Networking”, *ACM SIGCOMM Computer Communication Review*, 44(3):66–73, 2014.
10. S. H. Bouk, S. H. Ahmed, D. Kim, and H. Song, “Named-Data-Networking-based ITS for Smart Cities” *IEEE Communications Magazine*, 55(1):105–111, 2017.
11. M. Pilkington, “11 Blockchain Technology: Principles and Applications”, *Research Handbook on Digital Transformations*, page 225, 2016.
12. A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, “Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards.” *Overview report The British Standards Institution (BSI),* 2017
13. N. Z. Aitzhan and D. Svetinovic, “Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams” *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852, 2018.

14. G. Grassi, D. Pesavento, G. Pau, L. Zhang, and S. Fdida, "NAVIGO: Interest Forwarding by Geolocations in Vehicular Named Data Networking", *IEEE 16th Inter-national Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–10. IEEE, 2015.
15. M. Chowdhury, A. Gawande, and L. Wang, "Secure Information Sharing among Autonomous Vehicles in NDN", *IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 15–26, April 2017.
16. S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, " Recent Advances in Information-Centric-Networking based Internet of Things (ICN-IoT)" *IEEE Internet of Things Journal (EarlyAccess)*, pages 1–1, 2018.

AUTHORS BIOGRAPHY

Farhan Ahmad completed his Ph.D. in Computer Science from University of Derby, UK in 2018. Currently, he is working as Post-Doctoral Research Fellow at the Cyber Security Research Group, University of Derby, UK. His research focuses on Trust Management in Vehicular Networks and M2M communication, Blockchain in Internet-of-Things, Named Data Networking and Cyber Security. He can be contacted at f.ahmad@derby.ac.uk.

Chaker Abdelaziz Kerrache is an Associate Professor at the department of mathematics and computer science, University of Ghardaia, Algeria. He received his Ph.D. degree in Computer Science at the University of Laghouat, Algeria, in 2017. In 2015, he joined the Computer Networks Group (GRC) as a visiting PhD student. His research focuses on Trust and Risk Management, Secure Multi-hop Communications, Vehicular Networks, Named Data Networking (NDN), and UAVs. He can be contacted at kr.abdelaziz@gmail.com.

Fatih Kurugollu is working as Professor of Cyber Security at the University of Derby, UK, where, he is also leading the Cyber Security Research Group. Prof. Kurugollu received his Ph.D. from Istanbul Technical University, Turkey in 2000. He also worked at Queen's University, Belfast, U.K, and Marmara Research Center, Kocaeli, Turkey. His research focuses on Cyber Security, Multimedia Security, and hardware architectures for image and video applications. He can be contacted at f.kurugollu@derby.ac.uk.

Rasheed Hussain is currently working as Associate Professor at Innopolis University, Innopolis Russia. His research interests include information security, privacy, vehicular networks, vehicular clouds and social networks, blockchain, and future internet architecture. He received his Doctoral degree in computer science and engineering from Hanyang University, South Korea. He can be contacted at r.hussain@innopolis.ru.