Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing

Hong Liu, Yan Zhang, and Tao Yang

Abstract

EVCE computing is an attractive network paradigm involving seamless connections among heterogeneous vehicular contexts. It will be a trend along with EVs becoming popular in V2X. The EVs act as potential resource infrastructures referring to both information and energy interactions, and there are serious security challenges for such hybrid cloud and edge computing. Context-aware vehicular applications are identified according to the perspectives of information and energy interactions. Blockchain-inspired data coins and energy coins are proposed based on distributed consensus, in which data contribution frequency and energy contribution amount are applied to achieve the proof of work. Security solutions are presented for securing vehicular interactions in EVCE computing.

Introduction

Electric vehicles cloud and edge (EVCE) computing is an attractive network paradigm involving seamless connections in heterogeneous vehicular contexts to aggregate distributed electric vehicles (EVs) into a common resource pool, and to invoke the EVs for locally flexible usage [1]. In EVCE computing, information flow and energy flow are dynamically exchanged during the vehicle-to-anything communications, including vehicle-to-grid (V2G), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V), to achieve collaborative data sensing, information analyzing, and energy sharing. Due to the data sensitivity and context complexity, vehicular applications confront serious security issues.

The emergence of autonomous vehicles promotes the popularity of the combination of distributed vehicular resources. EVs constitute a noteworthy portion of connected services with energy, communication, and computation resources to perform processing at the network edge. Meanwhile, EVs' idle resources may be aggregated to establish a mobile resource pool for collaborative utilization [2]. Thus, a vehicular ecosystem will be established based on the distributed and aggregated EVs through their activity cycles, in which information and energy interactions are achieved among EVs, sensors, roadside units (RSUs), and local aggregators (LAGs) for interactive applications.

The coexistence of hybrid cloud computing and edge computing is becoming the trend of future vehicular applications, which have the following three characteristics.

Centerless Trust: There is no center node in peer-to-peer communications, in which data exchange is performed without pre-assigned trust relationships.

Collaborative Intelligence: An EV makes a limited contribution to specific processing; the coordinated EVs will jointly address problem solving for crowd intelligence.

Spatio-Temporal Sensitivity: An EV's exchanged information and energy are sensitive data with obvious spatio-temporal attributes for the data provenance requirement.

Unlike traditional system infrastructures, the EVCE confronts serious security challenges due to the legal entities and attackers being equipotent participants owning equal privilege. For instance, an EV provides dynamic traffic information and idle energy as distributed resources. An attacker could receive omni-bearing messages via open interfaces and wireless communication channels. In order to address the security issues, blockchain is introduced as a potential solution with two main features. *Decentralization* means that the data accounting, storage, maintenance, and transmission are performed based on distributed computing capabilities, and there is no core node for centralized management; *Co-participation* means that all the participants will join in block transactions based on consensus algorithms.

Toward the blockchain, cryptographic algorithms are applied to establish mutual or multi-party trust relationships. Mass collaboration is performed by collective self-interests, and the possible data uncertainty is regarded as a marginal element. Any block records and stores a receipt to a link with the previous block, and a new block is attached to the ledger only if the corresponding messages pass authentication by the majority of participants [3]. This special data structure provides better robustness under a single point of failure, and avoids tampering attack with data traceability. Currently, blockchain-based key management [4], anonymous multi-signatures [5], and secure software defined network architecture [6] have been proposed and leveraged to enhance security. In this article, the blockchain is applied during information and energy interactions to achieve enhanced security protection.

The remainder of this work is organized as follows. The next section introduces the network architecture and context-aware vehicular applications. Following that, we present security requirements and distributed consensus. Then we

Digital Object Identifier:
10.1109/MNET.2018.1700344

Hong Liu is with East China Normal University and Shanghai Trusted Industrial Control Platform Co., Ltd.; Yan Zhang (corresponding author) is with University of Oslo; Tao Yang is with The Third Research Institute of the Ministry of Public Security.

0890-8044/18/$25.00 © 2018 IEEE

present the security solutions for both information and energy interactions. The final section draws a conclusion.

Network Architecture and Context-aware Applications

Network Architecture

Figure 1 illustrates the network architecture of EVCE computing, in which there are two computing modes for extending mobile cloud infrastructures to the EVs as the network edges.

EV Cloud Computing: The EVs' idle energy, computation, and communication resources can be aggregated into a common pool. The EVs are regarded as mobile cloudlets based on vehicular ad hoc networks (VANETs) and other networks. The connected EVs are gathered for providing cooperative services while moving round different areas or spending hours in parking lots. The cloud computing mode highlights extending traditional cloud infrastructures into flexible connected EVs to establish interactions with RSUs, LAGs, and other entities [7, 8].

EV Edge Computing: The EVs act as distributed units to perform a substantial amount of data processing and analysis during collaborative operations, in which sensors are geographically dispersed to establish interactions [9]. Flexible computing is achieved instead of establishing direct communications with the remote cloud. This edge computing mode provides higher accuracy on measurement, and emphasizes the proximity to sensors, dense geographical distribution, latency reduction, and support for mobility to enhance the quality of services [10, 11]. The moving EVs could enhance the network connectivity and capability with high-speed data transmission and low communication latency.

This hybrid network architecture is fundamentally different from that of the traditional system paradigm. It is established based on distributed vehicular cloudlets and units, and highlights the performance of local information and energy processing with the collaboration of nearby vehicular resources.

Vehicular Information and Energy Interactions

In the network structure, both information and energy interactions (e.g., exchanging, collaboration, and reallocation) are achieved to support the Internet of Vehicular Energy.

Vehicular Information Interactions: During information interactions, an EV establishes wireless communications with multiple sensors for distributed perception and cooperative processing, including traffic updates monitoring and road environment detection. The sensing data is gathered by EVs for satisfying diverse functional requirements. Much vehicular data temporarily exists or entirely remains on the EVs, while some may be transmitted to and from other entities.

The EVs are distributed computing nodes to aggregate data together, and the associated data is applied for cooperative services, including traffic query, driving assistance, and entertainment sharing. The EVs realize resource reallocation to satisfy specific individual demands. Here, information interactions are generally based on V2I and V2V communications. For instance, an EV communicates with fixed surrounding infrastructures, communicates with parking lots to provide assistant information servers, and exchanges messages with a LAG during V2G communications.

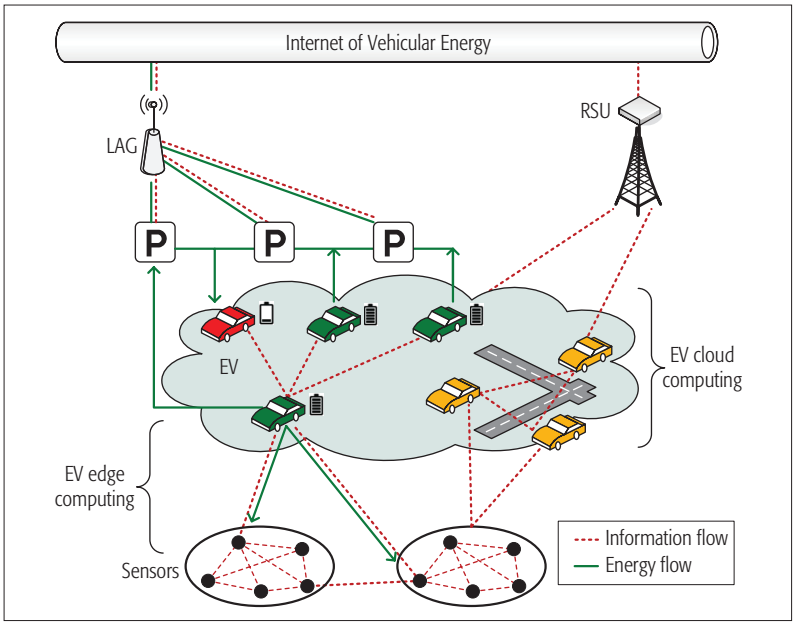

FIGURE 1. The network architecture of EVCE computing.

Vehicular Energy Interactions: During energy interactions, an EV performs changing and discharging operations during V2G communications with the roles of energy demand, energy storage, and energy supply. A LAG acts as an agent between the power grid and the gathered EVs for aggregating distributed batteries.

The EVs own potentially available batteries to interact with a LAG for energy exchanging. The aggregated EVs jointly establish a large and flexible energy pool, and the size of the energy pool continually varies according to EVs' arrivals and departures within an area [12, 13]. Meanwhile, an EV interacts with multiple sensors, and also supplies redundant energy to surrounding and dispersed sensors based on the emerging wireless charging technology for creating a perpetual energy source to provide power over distance, one-to-many charging, and controllable wireless power. Considering an EV's activity cycle perspective, it moves around different area networks along with distributed energy support.

Note that 4G LTE cellular telecommunication, WiFi, and IEEE 802.11p/wireless access for vehicular environments (WAVE) are available broadband wireless communication technologies for vehicular data transmission [14]. Both in-band spectrum and the 5.9 GHz dedicated short-range communications (DSRC) spectrum are popular for ubiquitous vehicular applications. The International Standards Organization/International Electrotechnical Commission (ISO/IEC) 15118 standard is particularly designed to support V2G communication interfaces.

Context-Aware Vehicular Applications

Figure 2 illustrates context-aware vehicular applications, in which there are four scenarios referring to information and energy interactions. The first two scenarios (shown by the red areas) refer to

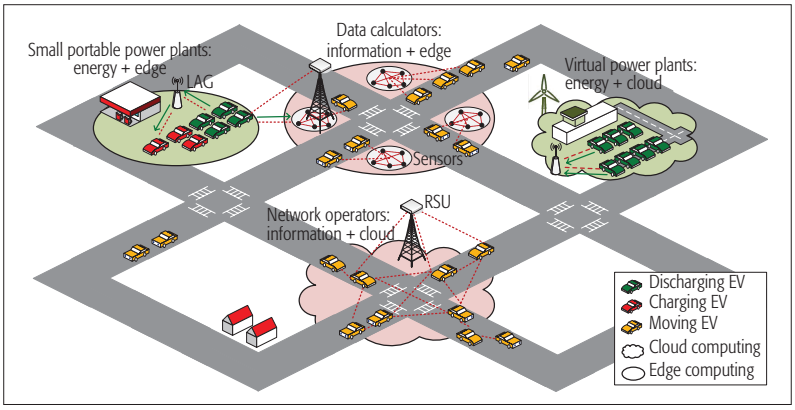

FIGURE 2. The contexts-aware vehicular applications based on the information and energy interactions.

information interactions, which consider the moving EVs as infrastructures to enhance computation capability for the vehicular cloud and edge. The other two scenarios (shown by the green areas) refer to energy interactions, and involve employing the discharging EVs as infrastructures for distributed energy support for the vehicular cloud and edge. Note that the energy interactions are performed along with the information interactions, and the EVs are assigned the following four main roles.

Spontaneous Network Operators: During the cloud-computing-based information interactions, slowly moving EVs act as spontaneous network operators to perform a substantial amount of communications with neighboring EVs and RSUs for establishing robust connectivity [11]. The vehicular networking forms a core component by carrying and forwarding data packets to other EVs, and is achieved through the combination of V2I and V2V communications. The EVs establish interactions with the RSUs to exchange information by monitoring roadside infrastructures, and also interacts with other EVs within a certain range. Data-driven interactions provide network connectivity for enabling data transmission. Collaborative networking is achieved considering high mobility and localized scattering from the neighboring EVs and RSUs.

Mobile Data Calculators: During the edge-computing-based information interactions, the EVs act as mobile data calculators to provide local data processing by integrating various sensing data to extract available information for transportation management. The moving EVs are traffic probes, integrated with private sector probe data for directly linking roadside sensors to physical surroundings. For instance, road detection and traffic optimization of automated vehicles are performed based on the cooperation of proper sensors. The EVs approach network boundaries with dense geographical distribution and collaborative computing capability.

Virtual Power Plants: During the cloud-computing-based energy interactions, the EVs act as virtual power plants to provide flexible energy aggregation with a cluster of scattered energy. Assume that there are many fully charged EVs during a long period of working time and nighttime, and the EVs are potentially available to feed energy back into the power grid or other neighboring entities. Moreover, an EV may play the role of mobile energy transporter to balance energy pools among different areas.

Small Portable Power Plants: During the edge-computing-based energy interactions, the EVs act as small portable power plants to share energy with roadside infrastructures (e.g., sensors and RSUs). Energy consumption of sensors and RSUs is one of the most important constraints; it will influence the network reliability and lifetime. Energy connectivity is crucial for enabling energy flow among different entities. The EVs are expected to be applied for wireless discharging to transmit idle energy to nearby sensors along with the development of wireless charging technology. Long-staying EVs become abundant and convenient power plants for energy sharing.

Security Requirements and Distributed Consensus

Security Requirements

Traditional security requirements including the data confidentiality, integrity, and availability (CIA triad), authentication, authorization, and accounting (AAA), privacy preservation (e.g., location, charge status, and identity) should also be addressed. Due to the limitations of wireless communication channels, data tampering, identity impersonation, and privacy violation related security issues become severe in EVCE computing.

Considering the characteristics of centerless trust, collaborative intelligence, and spatio-temporal sensitivity, traceability and transparency should be highlighted.

Traceability: refers to data provenance to identify data lineage tracing for collaborative EVs and other entities. It is required that the origins and intermediate flow of information and energy be traced during interactions. Due to attackers and legal entities being equally privileged and equipotent participants, the interactive data may be maliciously utilized or tampering.

Transparency: refers to an entity (e.g., an EV) knowing which other entity (e.g., a LAG) obtains its related data, when and where the entity has used the data, and how the entity realizes a specific function. Transparency has limited visibility during interactions based on the software defined security model (e.g., zero-trust model), and private data should be confused by scrambling mechanisms to avoid the data being resolved by irrelevant entities.

In EVCE, there are dissimilar security challenges.

Toward EV Cloud Computing: EVs establish information interactions along with computation resource sharing, and it is challenging to achieve data access control and traceability during dynamic participation. EVs establish energy interactions with energy resource sharing, and it is challenging to achieve aggregated energy transmission with identity privacy preservation.

Toward EV Edge Computing: EVs communicate with neighboring sensors, and it is challenging to achieve anonymous data transmission and batch authentication. EVs and LAGs establish direct energy interactions, EVs and sensors establish indirect energy interactions via RSUs, and it is challenging to achieve centralized and distributed energy allocation with energy status privacy preservation.

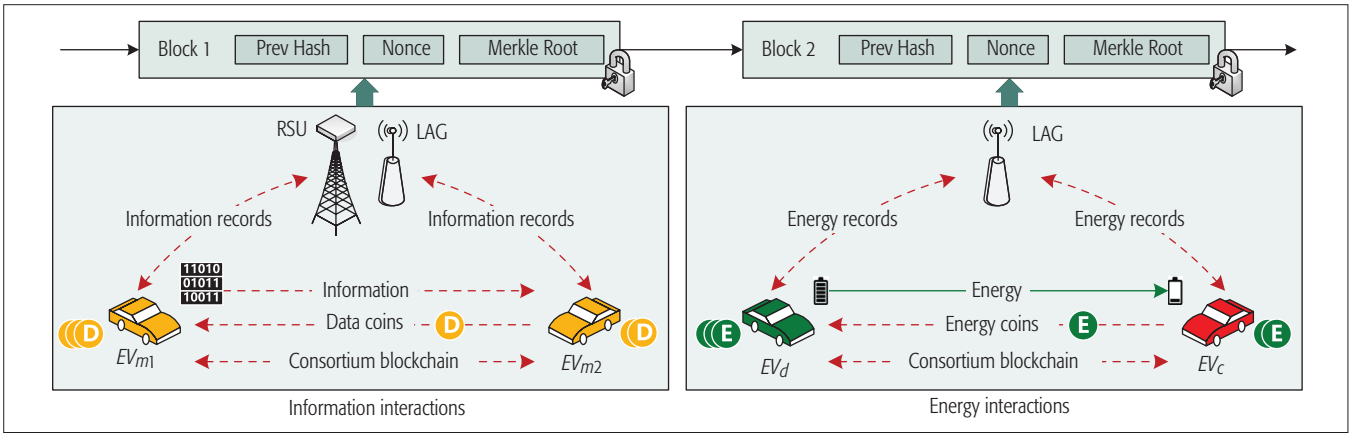

FIGURE 3. The structure of distributed consortium blockchain.

For instance, an EV performs computations based on dispersive data, which will be further processed for a certain purpose. Note that spatio-temporal attributes should be considered as critical parameters, for which timestamps and position information (e.g., latitude and longitude) could be jointly applied for sequence recordings. Each item of data should be assigned a lineage flag for further identifying its origins. Meanwhile, the EVs have dynamic positions, which will be applied for determining the location relationships for the interactive entities, and the RSUs and LAGs are regarded as having static positions to assist location identification.

Distributed Consensus

EVCE computing has similar features (e.g., centerless trust and collaborative intelligence) as the blockchain, in which all the participants collectively validate new blocks for collaborative management [15]. Blockchain establishes distributed consensus before transaction records are written into a digital ledger. It is executed by the collaborative participants based on timestamps and Merkle hash tree algorithms. The proof of work (PoW) and proof of stake (PoS) are two typical consensus algorithms. The PoW is absolutely dependent on the computing power, and the participants compete to obtain correct data writing with relatively random and low probability. The PoS is based on a deterministic approach and probability, and an account is chosen depending on its total stakes.

Here, *data coins* and *energy coins* are defined as new cryptocurrency for vehicular applications. During information and energy interactions, vehicular records are stored in a consortium blockchain, and the blockchain-inspired distributed consensus mechanisms are achieved. The vehicular records will be encrypted and structured into the blocks based on the pre-defined distributed consensus mechanisms, and RSUs and LAGs respectively audit the vehicular records and add them in a linear chronological order in a blockchain for verification.

Figure 3 shows the structure of a consortium blockchain, and each block contains a cryptographic hash value to the prior block. The traditional PoW in Bitcoin is available for the distributed consensus, which is achieved based on data contribution frequency and energy contribution amount.

Proof of Data Contribution Frequency: During information interactions, data coins are defined based on the proof of EVs' data contribution frequency. A consensus process is performed by authorized RSUs or LAGs for audit, and a new block will be formed for verification during a consensus process. If the EV has the highest data contribution frequency in a certain period, it will be rewarded by data coins as incentive to encourage other EVs to contribute information.

Proof of Energy Contribution Amount: During energy interactions, energy coins are defined based on the proof of EVs' energy contribution amount, which is directly related to the periodic energy interactions. A consensus process is performed by the authorized LAGs, and the amount of discharged energy is measured by smart meters. If an EV has the most energy contributions in a certain period, it will be rewarded by energy coins for encouraging other available EVs to participate in the discharging operations.

The data coins and energy coins are only exchanged among EVs, and are allowed to be circulated and traded. During the information interactions, the sensors will not obtain data coins due to their inherent functions for data distribution. During the energy interactions, the sensors and RSUs will not obtain any energy coins since they have no redundant energy to perform discharging operations.

The proof of data contribution frequency and the proof of energy contribution are defined for determining representation in majority decision making. The established data coins and energy coins can be applied for vehicular resources allocation. If an EV contributes more frequently for collaborative intelligence, it will obtain more data coins. It will be assigned higher priority to access the resource pool, and its data may be assigned higher credibility for decision assistance. If an EV feeds more energy back into the grid or other entities, it will own more energy coins, and will be assigned with higher priority or lower price for energy utilization.

Security Solutions for EVCE Computing

In EVCE computing, there are moving EVs (i.e., EV_m), discharging EVs (i.e., EV_d), charging EVs (i.e., EV_c), RSU, LAG, and multiple sensors. The data coins and energy coins are considered during the EVs' interactions; anonymous data transmission

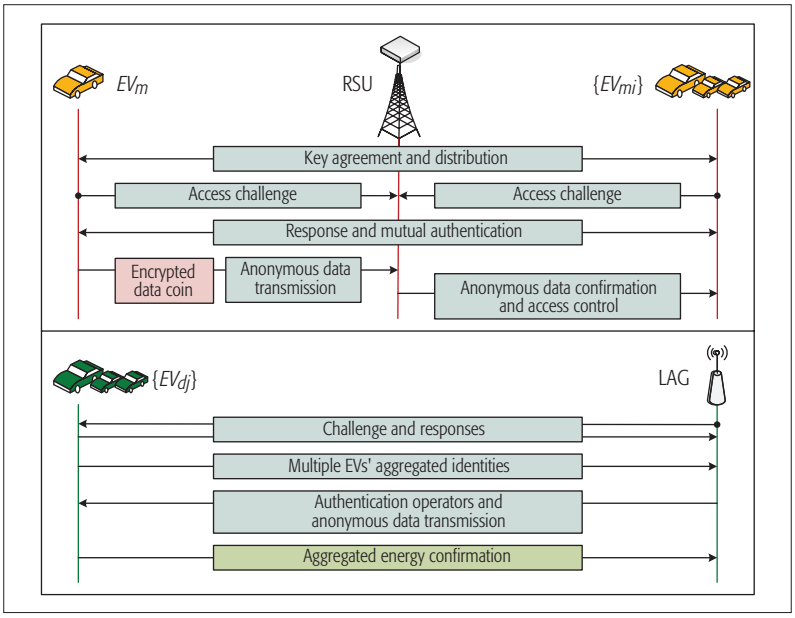

FIGURE 4. The security scheme in EV cloud computing.

and aggregated energy transmission are achieved during heterogeneous interactions.

Securing Interactions in Cloud Computing

Figure 4 shows secure interactions in cloud computing, involving EVs (i.e., EV_m and EV_d), an RSU, and a LAG, and the distributed EVs' resources are aggregated for more flexible allocation and usage.

Information-Driven Security Scheme: The moving EVs act as network operators to establish V2V communications. EV_m interacts with its neighboring EVs $\{EV_{m1}, EV_{m2}, ..., EV_{mi}\}$ ($i \in \mathbb{N}^*$) for collaborative operations. These moving EVs jointly perform cooperations in which data-coin-based anonymous data confirmation and access control should be particularly considered for data exchanging and sharing.

In the initialization, the moving EVs perform key agreement and distribution based on the peer-to-peer networks; temporary session keys could be established based on lightweight symmetric encryption. The shortest path tree routing and multi-path key mode could be applied for group key agreement. Thereafter, the moving EVs and the RSU establish interactions via access challenges and responses. Here, the moving EVs jointly complete cooperation for data exchanging, the signed data could be broadcast to neighboring EVs, and mutual authentication could be established based on homomorphic encryption and secure multi-party computation.

The encrypted data coins directly influence resource allocation among different moving EVs. Moreover, spatio-temporal attributes could be applied for access control, and conditional proxy re-encryption could be used to address data sharing and data hiding issues among different EVs.

Energy-Driven Security Scheme: The multiple discharging EVs $\{EV_{d1}, EV_{d2}, ..., EV_{dj}\}$ ($j \in \mathbb{N}^*$) act as virtual power plants to establish an aggregated energy resource pool via the LAG. These discharging EVs' energy should be aggregated during transmission with privacy considerations.

$\{EV_{d1}, EV_{d2}, ..., EV_{dj}\}$ generate pseudo random numbers as access challenges to be transmitted to the LAG for launching a session. When the EVs and LAG establish interactions, the EVs' aggregated identifiers are transmitted to the LAG for mutual authentication. The LAG extracts its local values to compute authentication operators based on lightweight cryptographic primitives for identification and authentication. Here, elliptic curve digital signature algorithm (ECDSA)-based signature (e.g., ring, group, and blind signatures) could be applied for anonymous data transmission.

The EVs have diverse energy preferences for the discharging request. An EV supplies its idle energy back into the power grid for aggregating distributed energy. During energy interactions, the energy is regarded as a non-differential resource for reallocation. The discharging EVs jointly establish a flexible energy pool, which can be shared by the EVs around the same LAG. The Merkle-hash-tree-based selective disclosure mechanism could be applied for protecting the sensitive data fields. Such data structure avoids storing all the data fields to realize efficient and secure verification of a large data structure.

Securing Interactions in Edge Computing

Figure 5 shows secure interactions in edge computing, involving the EVs (i.e., EV_m, EV_d, EV_c), an RSU, a LAG, and sensors, and the distributed EVs' resources are applied for local computing and processing.

Information-Driven Security Scheme: The moving EV_m acts as a mobile data calculator during information interactions in edge computing. Batch authentication should be established by ultra-lightweight algorithms.

The sensors constantly broadcast omni-bearing queries, and EV_m gives a response upon receiving a periodic query. Thereafter, a key agreement and distribution scheme could be established to support dynamic participation and authentication. EV_m and sensors perform mutual authentication based on the permutation, symmetric encryption, or hash/hash-based message authentication code (HMAC). The multicast message authentication and batch authentication become efficient for secure interactions among multiple sensors.

Here, EV_mfirst obtains the raw sensing data $Data_0$, and further performs processing and computing to obtain the advanced data $Data'_0$. Thereafter, EV_m transmits $Data'_0$ to an RSU for data integration. Other neighboring EVs also perform similar authentication operations, and further transmit $\{Data'_1, Data'_2, ..., Data'_x\}$ to the RSU. Based on the distributed consensus, $Data'_*$ will be written into the digital ledger, and data coin will be assigned to the appropriate EV.

Energy Driven Security Scheme: The discharging EV_d acts as a small portable plant to establish communications with EV_c, LAG, RSU, and sensors during energy interactions in the edge computing.

For one aspect, the LAG generates pseudo-random numbers as access challenges, and respectively transmits them to surrounding EV_c and EV_d. After the LAG and EVs establish mutual authentication, EV_d is requested to perform discharging operation to feed a local vehicle EV_c. Upon EV_d receiving the discharging request, it could wrap its energy status into

ciphertexts and transmit the encrypted energy status to EV_c. The delivery of energy coins is performed based on pseudonym, avoiding sensitive privacy disclosure.

For the other aspect, the sensors perform similar operations, and establish challenges and responses with EV_d. The sensors transmit energy requests to EV_d via an RSU for local energy access. EV_d's energy status will be transmitted to the sensors for energy confirmation.

EV_c and sensors will be charged by the wired and wireless charging technology, and energy coins are exchanged between EV_d and EV_c based on the distributed consensus. The concealed data aggregation can be applied for privacy preservation, and hierarchical data access control can be applied intra-network (e.g., V2G communications) and inter-networks (e.g., V2G and V2I communications).

In EVCE computing, the data coins and energy coins are applied as authentication operators for EVs. The access priority, credibility, and price could also be related to data coins and energy coins. Data traceability and transparency could be achieved by the inherent characteristics of blockchain.

Conclusion

This article focuses on security issues for both information and energy interactions in EVCE computing. The context-aware vehicular applications are presented according to the EVs' different roles; blockchain-inspired data coins and energy coins are defined to achieve distributed consensus; and data contribution frequency and energy contribution amounts are applied for proof determination. Security schemes are proposed for cloud and edge computing to launch perspectives on vehicular applications.

Acknowledgment

This work is funded by the National Key R&D Program of China (2017YFB0802302, 2017YFB0801701) and the National Natural Science Foundation of China (61601129). This work is partially supported by projects 240079/F20 funded by the Research Council of Norway.

References

[1] S. K. Datta *et al.*, "Vehiclesas Connected Resources: Opportunities and Challenges for the Future," *IEEE Vehic. Tech. Mag.*, vol. 12, no. 2, 2017, pp. 26–35.
[2] H. Li *et al.*, "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP," *IEEE Wireless Commun.*, vol. 22, no. 4, Aug. 2015, pp. 74–80.
[3] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" *IT Professional*, vol. 19, no. 4, 2017, pp. 68–72.
[4] A. Lei *et al.*, "Blockchain-Based Dynamic Key Management for HeterogeneousIntelligent Transportation Systems," *IEEE Internet of Things J.*, 2017.
[5] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and AnonymousMessaging Streams," *IEEE Trans. Dependable and Secure Computing*, 2017.
[6] P. K. Sharma *et al.*, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Commun. Mag.*, vol. 55, no. 9, Sept. 2017, pp. 78–85.
[7] K. Zhang *et al.*, "Mobile Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Offloading," *IEEE Vehic. Tech. Mag.*, vol.12, no. 2, 2017, pp. 36–44.
[8] Z. Zhou *et al.*, "Software Defined Machine-to-Machine Communication for Smart Energy Management," *IEEE Commun. Mag.*, vol. 55, no. 10, Oct. 2017, pp. 52–60.

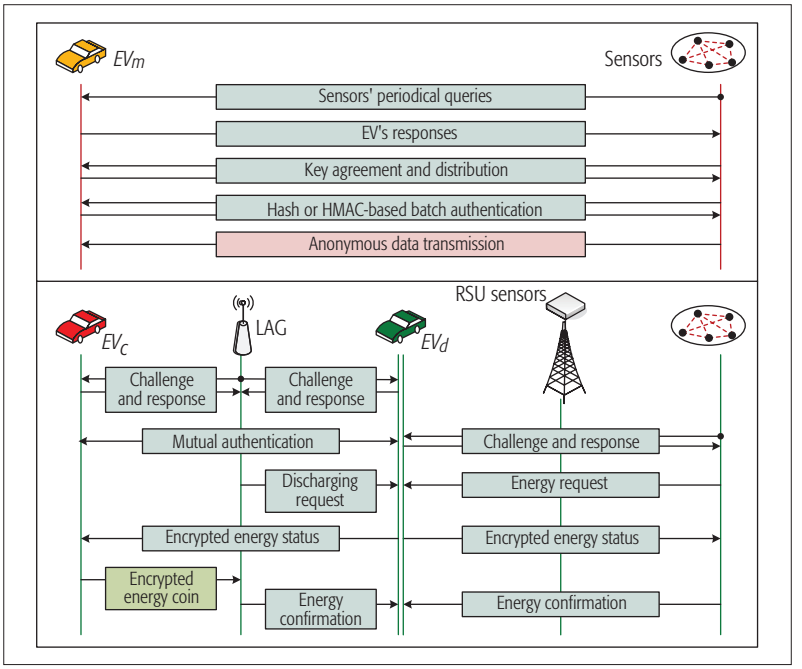

FIGURE 5. The security scheme in the EV edge computing.

[9] X. He *et al.*, "A Novel Load Balancing Strategy of Software-Defined Cloud/Fog Networking in the Internet of Vehicles," *China Commun.*, vol. 13, Supplement 2, 2016, pp. 140–49.
[10] K. Sasaki *et al.*, "Vehicle Control System Coordinated Between Cloud and Mobile Edge Computing," *Proc. 55th Annual Conf. Society of Instrument and Control Engineers of Japan*, 2016, pp. 1122–27.
[11] X. Hou *et al.*, "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 6, 2016, pp. 3860–73.
[12] Y. Zhang *et al.*,"Securing Vehicle-to-Grid Communications in the Smart Grid," *IEEE Wireless Commun.*, vol. 20, no. 6, Dec. 2013, pp. 66–73.
[13] J. Kang *et al.*, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Trans. Industrial Informatics*, 2017.
[14] J. Ren *et al.*, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Network*, vol. 31, no. 5, Sept./Oct. 2017, pp. 96–105.
[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.

Biographies

Hong Liu is an associate professor in the School of Computer Science and Software Engineering, East China Normal University. She received her Ph.D. degree from the School of Electronic and Information Engineering, Beihang University, China. She focuses on security and privacy issues in edge computing. She has published more than 30 SCI papers, and 1 ESI Highly Cited Paper. She has served as a Program Committee member and Workshop Chair in several conferences.

Yan Zhang is a full professor in the Department of Informatics, University of Oslo, Norway. He received a Ph.D. degree from the School of Electrical & Electronics Engineering, Nanyang Technological University, Singapore. He serves as an Editor of IEEE journals, and serves in Chair positions for a number of conferences. His current research interests include next-generation wireless networks leading to 5G, and green and secure cyber-physical systems. He is an IEEE Vehicular Technology Society Distinguished Lecturer.

Tao Yang is an associate professor at the Third Research Institute of the Ministry of Public Security. He received his Ph.D degree from the School of Computer Science, Fudan University. He focuses on security issues in information networks and digital forensics. He has presided over three national key scientific research projects. He was awarded the Science and Technology Progress award and the Three Grade Merit of the Ministry of Public Security.