Name: Muhammad Faisal ID# 15139 Section: FALL-18

Sessional Assignment

Q. Write an introduction of a five research papers don't copy paste write in your own words. Choose your own area. All research papers are in the same Area and different from each other.

Answer.

1. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks

Introduction

The drastically increasing volume and the growing trend on the types of data have brought in the possibility of realizing advanced applications such as enhanced driving safety, and have enriched existing vehicular services through data sharing among vehicles and data analysis. Due to limited resources with vehicles, vehicular edge computing and networks (VECONs) i.e., the integration of mobile edge computing and vehicular networks, can provide powerful computing and massive storage resources. However, road side units that primarily presume the role of vehicular edge computing servers cannot be fully trusted, which may lead to serious security and privacy challenges for such integrated platforms despite their promising potential and benefits. We exploit consortium blockchain and smart contract technologies to achieve secure data storage and sharing in vehicular edge networks. These technologies efficiently prevent data sharing without authorization. In addition, we propose a reputation-based data sharing scheme to ensure high-quality data sharing among vehicles.

With rapid development of vehicular telematics and applications, vehicles generate a huge amount and several different types of data. For example, a self-driving vehicle can create 1 GB data per second from cameras, radar, GPS, etc. [1]. Moreover, vehicles can cooperatively collect and share data of common interest [2], [3]. Data collected by the vehicles consists of objective and subjective information. The objective information mainly includes traffic-related data, such as road and weather conditions, and parking lot occupancy. The subjective information includes things such as rating of a hotel and quality of vehicular services [4]. Sharing of data has made it possible to realize goals such as improved driving safety, and to obtain higher service quality during travelling. Due to resource constraints, vehicles cannot support massive data storage and large-scale data sharing. Vehicle-generated data becomes increasingly fine-grained and complex, which increases the burden on data transmission.

To address these challenges, mobile edge computing is a promising paradigm that can be embedded at the network edge infrastructures, e.g., roadside units (RSUs), to support massive data storage, computing and sharing close to the vehicles [2], [5]. Vehicular networks integrated with mobile edge computing are evolving toward vehicular edge computing and networks (VECONs) [6].

Security and privacy issues are critical challenges for VECONs. RSUs in VECONs play an important role to temporally store and manage vehicular data. But the RSUs are semi-trusted as

they are usually distributed along the road without any strong security measures, thus making them vulnerable to being compromised by attackers.
Vehicles therefore may not be willing to upload their data to the RSUs because of privacy concerns. Likewise, peer to peer (P2P) data sharing among vehicles raises the issues such as data access without authorization and the need of ensuring security in a decentralized manner. These challenges influence the sharing of vehicular data, and thus hinder the pace for development of VECONs [9].
Recently, blockchain technology has attracted growing attention and research work in the context of vehicular networks because of its characteristics of decentralization, anonymity and trust. Blockchain can facilitate establishing a secure, trusted and decentralized intelligent transport ecosystem, to address data sharing problems thus contributing in creating better usage of the transport infrastructures and resources.
The main contributions of this paper are summarized as follows.
1) We propose to utilize consortium blockchain to establish a secure and distributed vehicular blockchain for data management in VECONs.
2) We deploy smart contracts on the vehicular blockchain to achieve secure and efficient data storage on RSUs, and data sharing among vehicles.
3) We develop a reputation-based data sharing scheme with three-weight subjective logic (TWSL) model to choose more reliable data source to improve data credibility.

REFERENCES

[1] W. Xu *et al.*, "Internet of Vehicles in big data era," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 19–35, Jan. 2018.
[2] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.
[3] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: A content-centric framework," *IEEE Wireless Commun.*, vol. 24, no. 1, pp. 60–66, Feb. 2017.

2. Blockchain based trust & authentication for decentralized sensor networks

Introduction

Sensor networks and Wireless Sensor Networks (WSN) are key components for the development of the Internet of Things. These networks are subject of two kinds of constraints. Adaptability by the mean of mutability and evolutivity, and constrained node resources such as energy consumption, computational complexity or memory usage.
We propose a new security model and its protocol based on the blockchain technology to ensure validity and integrity of cryptographic authentication data and associate peer trust level, from the beginning to the end of the sensor network lifetime.
SENSOR Networks and Wireless Sensor Networks (WSN) are two main components involved in the development of the Internet of Things (IoT). Security and privacy handling for Sensor Networks present new issues due to specific constraints. Low resources on computation, hardware functionalities and energy consumption in WSNs. The research work is divided into two categories: security and privacy for the data being sent over the network on one side, and node authentication and trust management on the other side. Both have been actively explored the last ten years, and some solutions have been brought by researchers. However, from our

knowledge none of these works propose a complete model for both content access, security, privacy and trust management. In this paper, we focus on addressing authentication and trust management issues.

REFERENCES

[1] C. M. Medaglia and A. Serbanati, An Overview of Privacy and Security Issues in the Internet of Things, D. Giusto, A. Iera, G. Morabito, and L. Atzori, Eds. New York, NY: Springer New York, 2010.

[2] Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks." vol. 2006, pp. 1–13, 2006.

3. Blockchain Technology, Cognitive Computing, and Healthcare Innovations

Introduction

Blockchain enables more agile value chains, faster product innovations, closer customer relationships, and faster integration with the Internet of Things (IoT) and cloud technology. Now with Cloud and Blockchain technologies providing high computing power and network capabilities, cognitive systems are available tools to deepen the relationship between humans and the world. Many problems that have been with our society for a long time can be solved. Cognitive systems are the tools to accomplish that ambitious goal. The study concluded with discussing opportunities and challenges of the application of two intrahorizons of Blockchain technology, Cognitive Computing and Healthcare.

Blockchain was firstly introduced as the computational infrastructure of Bitcoin, a digital currency, but has tremendously found much interest in a variety of industrial application domains. The proposal of blockchain was to distribute electronic transactions rather than maintain dependency on centralized institutions for the exchange. Blockchain is essentially a simplified payment verification system. Blockchain keeps evolving in a number of industrial domains as the body of research grows [3]. Researchers are working to apply a number of use cases included smart contracts, such as supply chain, and healthcare. The scalability feature and distributed implementation of Blockchain technology makes it a powerful tool to improve the supply chain process where Ecopreneurs were given the option to make informed decisions toward improving global economy and sustainability of the project where supply chain is implemented [4]. The flow initiated from raw material to the final product until they are handed to the end consumer could gain benefit from this distributed implementation of scalable ledger platform, Blockchain technology, to track the supply chain elements, ranging from raw materials to the transportation equipment to the human resources. Authors predict the utility of Blockchain technology in the novel supply chain managements could place companies in a higher level of competition for enhanced socio-economic, socio-environmental and eco-efficiency[4].

REFERENCES

[1] W. J. Sutherland *et al.*, "A 2017 horizon scan of emerging issues for global conservation and biological diversity," *Trends Ecol. Evol.*, vol. 32, no. 1, pp. 31–40, Jan. 2017.

[2] S. Nakamoto. (2008). Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: www.bitcoin.org, p. 9.

[3] M. Pilkington, *Blockchain Technology: Principles and Applications*.

4. Smarter City: Smart Energy Grid based on Blockchain Technology

Introduction

The improvement of the Quality of Life (QoL) and the enhancement of the Quality of Services (QoS) represent the main goal of every city evolutionary process. It is possible making cities smarter promoting innovative solutions by use of Information and Communication Technology (ICT) for collecting and analysing large amounts of data generated by several sources, such as sensor networks, wearable devices, and IoT devices spread among the cityIn the Smart City context, this paper intends to investigate the Smart Environment pillar, and in particular the aspect related to the implementation of Smart Energy Grid for citizens in the urban context. The innovative characteristic of the proposed solution consists of using the Blockchain technology to join the Grid, exchanging information, and buy/sell energy between the involved nodes (energy providers and private citizens), using the Blockchain granting ledger.

A Smart City is conceived as an idealistic city, where the quality of life for citizens is significantly improved by combining ICT [1], [2], new services and new urban infrastructures, The main innovation in the Smart City evolutionary process consists of considering a user-centric vision, and accounting urban issues from the perspective of the citizen's needs, engaging the citizens in the city management. In other words, the Smart City concept may be defined as an integrated system in which human and social capital heavily interacts, using technology-based solutions. The application of the Internet of Things (IoT) paradigm to urban scenarios is of special interest to support the smart city vision [3]–[5] [6]. This vision aims to efficiently achieve sustainable and resilient development and a high quality of life on the basis of a multi-stakeholder, municipality-based partnership.

The Italian architect Carlo Ratti confers a very important role to modern city, affirming that this "occupies 2% of the land surface, hosts 50% of the global population and consumes 75% of the total energy, being cause of the 80% of emission of CO2"1.

For all these reasons, it is necessary promoting city transformation processes to obtain a better use of renewable resources, reducing wastes and safeguarding the environment [7], [8], while at the same time promoting the cohesion between citizens that are to be joined to obtain shared benefit in terms of quality of life. The eco-sustainable approach has to be applied in several aspects and at several layers of the evolutionary process, such as mobility, environment, social services, as well as in the urban requalification.

The paper, furthermore, describes the mobile application that has been implemented in order to enable the citizens access to the Blockchain network.

REFERENCES

[1] A. Pieroni and G. Iazeolla, Engineering QoS and energy saving in the delivery of ICT services. 2016.

[2] A. D'Ambrogio et al., "Use of integrated technologies for fire monitoring and first alert," in Application of Information and Communication Technologies, AICT 2016 - Conference Proceedings, 2017.

[3] A. Pieroni, N. Scarpato, M. Brilli, "Performance Study in Autonomous and Connected Vehicles a Industry 4.0 Issue," J. Theor. Appl. Inf. Technol., vol. 96, no. 2, 2018.

5. Consortium Blockchains: Overview, Applications and Challenges

Introduction

The Blockchain technology has recently attracted increasing interests worldwide because of its potential to disrupt existing businesses and to revolutionize the way applications will be built, operated, consumed and marketed in the near future. In this context, consortium blockchains emerged as an interesting architecture concept that benefits from the transactions' efficiency and privacy of private blockchains, while leveraging the decentralized governance of public blockchains. Ethermint is performed in order to highlight its main advantages and limitations. Finally, various research challenges and opportunities are discussed.

The blockchain technology has attracted increased interests worldwide in recent years, with emerging applications in key domains, including finance, energy, insurance, logistics and mobility. Indeed, this technology is expected to disrupt businesses and markets on a global scale. A blockchain is essentially a trustless, peer-to-peer and continuously growing database (or ledger) of records, aka. blocks, that have been verified and shared among the participating entities [1]. Each block typically contains a timestamp,

A cryptographic hash value of the previous block, and a set of transactions data. Once a new block is validated by consensus and written to the ledger, transactions cannot be altered retroactively without the collusion of the network majority. Blockchain is secure by design and relies on well-known cryptographic tools and distributed consensus mechanisms to provide key characteristics, such as persistence, anonymity, fault-tolerance, auditability and resilience.

the blockchain technology is foreseen as the core backbone of future smart cities and enterprises by enabling the interoperability and collaboration between organizations, while enhancing their security, data and process management.

Indeed, several challenges will need to be addressed to unlock the tremendous potential of blockchains especially before this paradigm shift becomes technically, economically and legally viable in enterprises environments. These challenges concern the technical aspects of blockchains, including its architecture, deployment, governance, scalability and data privacy. Private and consortium blockchains emerged from this perspective as appropriate architecture concepts for business environments, where restrictions are applied on who is allowed to participate to the network. While the former approach assumes that the network is operated by a single entity, a consortium blockchain operates under the leadership of a group of entities, thus enabling collaborative business transformation among organizations and innovative business models

REFERENCES

[1] E. Ben Hamida, K. L. Brousmiche, H. Levard, and E. Thea, "Blockchain for Enterprise: Overview, Opportunities and Challenges," in The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017), Nice, France, Jul. 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, accessed: 2017-05-25. [Online]. Available: https://bitcoin.org/bitcoin. pdf

[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, 2016, pp. 2292–2303.