Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture

Sachin Sharma, Kamal Kumar Ghanshala, Seshadri Mohan*
Graphic Era Deemed to be University, Dehradun, UK, India
*University of Arkansas at Little Rock, Little Rock, Arkansas, USA
{sxsharma88, kamalghanshala}@gmail.com
*sxmohan@ualr.edu

***Abstract*—With the transformation of connected vehicles into the Internet of Vehicles (IoV), the time is now ripe for paving the way for the next generation of connected vehicles with novel applications and innovative security measures. The connected vehicles are experiencing prenominal growth in the auto industry, but are still studded with many security and privacy vulnerabilities. Today's IoV applications are part of cyber physical communication systems that collect useful information from thousands of smart sensors associated with the connected vehicles. The technology advancement has paved the way for connected vehicles to share significant information among drivers, auto manufacturers, auto insurance companies and operational and maintenance service providers for various applications. The critical issues in engineering the IoV applications are effective to use of the available spectrum and effective allocation of good channels an opportunistic manner to establish connectivity among vehicles, and the effective utilization of the infrastructure under various traffic conditions. Security and privacy in information sharing are the main concerns in a connected vehicle communication network. Blockchain technology facilitates secured communication among users in a connected vehicles network. Originally, blockchain technology was developed and employed with the cryptocurrency. Bitcoin, to provide increased trust, reliability, and security among users based on peer-to-peer networks for transaction sharing. In this paper, we propose to integrate blockchain technology into ad hoc vehicular networking so that the vehicles can share network resources with increased trust, reliability, and security using distributed access control system and can benefit a wider scope of scalable IoV applications scenarios for decision making. The proposed architecture is the faithful environment for information sharing among connected vehicles. Blockchain technology allows multiple copies of data storage at the distribution cloud. Distributed access control system is significantly more secure than a traditional centralized system. This paper also describes how important of ad hoc vehicular networking in human life, possibilities in real-world implementation and its future trends. The ad hoc vehicular networking may become one of the most trendy networking concepts in the future that has the perspective to bring out much ease human beneficial and secured applications.**

Keywords: IoV, smart city, blockchain, intelligent sensors, security, privacy.

I. Introduction

Due to explosive growth in multimedia applications and the new innovations in the area of human-machines interaction technologies, the powerful engagement is happening for connectivity in the world. The IoV applications networking are also dramatically evolving and creating various new connectivity methodologies. An IoV networking ideally connect vehicles to other vehicles via physical devices that embed with various new intelligent sensors. The Internet-connected devices produce and exchange an enormous amount of data to beneficial human services. Many initiatives have been taken to provide human friendly advanced technology platforms and it is a challenge to turn IoV applications networking platform into economic ecosystems [1]. The main challenge of IoV networking implementation is a variety of application modules, diversity in data sources, and a trust among different intelligent systems. In [2], the authors proposed how the new technology and real-time data communication may impact on different phases of human lifestyles. In general, there are two types of data communication happens. First, communication among diversified data sources in various domains. Second, communication among various sensors in local system. We discuss the issue of how to consolidate the two communication platforms including multiple senses of human and establish consistency.

The IoV sensors information delivery could be a variety of digital distribution of multimedia system contents. However, on-line knowledge delivery medium like the web-based mostly cloud services [3] or peer-to-peer communication establish high network performance with the economic scheme. A data communication network (DCN) is an optimized distributed network for consistent data communication in IoV application platform. In [4], the authors proposed a new approach of generating, distributing and multiple transmission file format. However, none of those solutions convergence on the data security and integrity of the multiple transmission file format delivered contents. The communication of various multimedia files collected from various types of sensors over wired or wireless network in case of tampering do not consider secure. In this paper, we propose a secured Ad hoc vehicular networking architecture based on the blockchain. The blockchain is a sophisticated technology [5] that has the potential transparency and trust to shield ad hoc vehicular networking architecture

and validate transactions. A secured computing network architecture easily retrieves the data communication transaction or the modification histories. The architecture consists of the following information; a hash consists of data transaction histories (blockchain transactions log) and an impression copy of original data content. After the impression copy is retrieved,the rest is transferred to a administer ledger that can retrieve the communication data history and restructure the tampered regions.

The remaining of this paper consists of the following sections. Section II consists of generic architecture of IoV networks. Section III demonstrates the IoV applications. Section IV consists of security and privacy concerns in IoV applications. Section V consists of the overview of the blockchain. Section VI consists of implementation and performance analysis. Section VII consists of blockchain use case and analysis. Finally, section VIII includes conclusion and future work.

II. Generic Architecture of IoV Networks

The network protocol performs a major role in data communication. IoV networks establish communication among an extensive number of physical devices and variety of sensors. Moreover, IoV networking will face innumerable challenges in security issues. So, a generic architecture of IoV networking consists of requisite characteristics such as sustainability, reliability, scalability, availability, Quality of Service (QoS), socio-economic viability, confidentiality, security, privacy, authenticity and integrity. IoV networks are connecting everything and everyone to communicate data with each other expanding the network traffic with storage capacity. The IoV network facilitates improvement in existing user-friendly new advanced technology, applications and business models. The architecture consists of the following layers. Each layer is briefly described below:

Concept Layer: This layer consists of the various varieties of sensors to acknowledge user. This layer collects specific information by individual sensor devices with location and securely broadcasts to convolution layer.

Convolution layer: This layer consists of the delicate data collected from various sensor devices, transmit to the control layer through wired or wireless communication.

Control layer: This layer consists of control on various IoV services, applications, and database. It has control over smart computational process, results and service management.

Utility layer: This layer consists of IoV applications management in various domains such as smart city, smart heath, smart vehicle, smart home and intelligent transportation etc. It may also develop utility graphs, utility models and utility analysis report, etc. depends upon the data retrieved from concept layer which may help to business enterprise managers to develop an efficient and service oriented business strategies.

III. IoV Applications

IoV applications might be used in several domains like smart city, smart lifestyle, smart retail, smart transportation, smart home, smart agriculture, smart business, smart healthcare, smart culture and tourism, smart environment, smart forestry and smart energy.

Smart transportation: Various transportation systems such as rail, road, waterways and airways consist of smart huge infrastructure, various sensors, actuators and powerful processors, which may facilitate smart services to drivers and/or passengers such as smart navigation services and passenger safety services etc. The numerous business enterprises and government authorities would get benefit from real-time information collected by sensor about traffic patterns and route optimization information. Deployed sensors may facilitate passengers by sharing useful information in a single platform such as tickets access, seat availability, arrival or departure details, boarding process, freight services availability with cost and travelling fare comparisons etc. We will briefly explain few application domains below:

Smart health: Health monitoring IoV sensors networking are more reliable compare to traditional sensors networking especially in very sensitive information collection about patient health. Using these sensors, remote patient diagnosis system may be deployed to facilitate any patient anywhere in the world due to it's reliability and authenticity in efficient data collection strategies.

Smart home: The smart sensors and actuators deployed in home helps to make peoples daily life more comfortable in many aspects such as auto room cooling or heating adaptation as per the human body demands; auto room lighting as per human body activity such as read mode and sleep mode etc. In case of an accident such as fire, short circuits may be evaded with the suitable alert system.

Smart energy: The various sensors deployed in the home, and offices help in efficient energy consumption by automatically inactive/turned off the electrical or electronic appliances such as television, air condition, refrigerator, light bulbs, kitchen appliances and so on, when not in use.

Smart city: The various sensors deployed in the smart city enable efficient management services such as traffic management, waste management, smart parking, smart street lighting, water management, smart surveillance, and smart building. The services operation management will be done in real-time objects based on human body interaction inputs. Furthermore, applications perform user-defined events and record human senses oriented predefined conditions.

IV. Security and Privacy concerns in IoV Applications

The security and privacy of data collected from various sensors under IoV applications provide confidentiality, integrity, availability, authenticity, reliability and authorization. In future, IoV will be a most remarkable network of the global economy. Therefore, the security and privacy concerns are the need in IoV.

In the initial phase, most of the researches are emphasised on evolving the human senses sensors to machine communication protocols. Though it generates the needs of security

and privacy of gathered data. The sensors collect data from human senses then transmit data to the central system using sensors to machine device. Various sensors are deployed in the system create vulnerabilities to attack from the malicious attackers such as phishing attacks, acknowledgement message attack, message modeling attack, malware attacks, Denial-of-Service (DoS) attack, active level attack, service message attack, message mutation attack, message voiding attack, and sybil attack [6], [7]. IoV networking facilitates sensors to machine communication management and reliable quality of service (QoS) [8], [9]. Extensive traffic of data and sensor devices in the concept layer may cause of malicious attacks. Convolution, control and utility layers are critical parts of IoV network architecture consisting of high data traffic security necessity and efficient cost-effective real-time data analysis with management. In IoV networking architecture, the smart sensors are connected with the Internet or external network for collecting data via transmission [10], [11] . Privacy of specific sensors senses information is one of the critical challenges in IoV networking. Another concern is privacy at the concept layer which may cause to expose of private information in the occurrence of hardware and software design flaws. An attacker may take control of any physical device at the concept layer and manipulate the sharing information. Therefore, physical device reliability is one of the major impact on keeping the collected data secured. Many steps can be taken to keep sensitive information secured and private such as encryption methods, hide the basic user details, and hide the current location etc. Encryption technique can be implemented to maintain data integrity and transmission reliability in IoV networking. Secure well-defined communication protocols are the one of the best ways to solve these issues. However, for reliance secured operations require certified and high powered devices.

V. Overview of Blockchain

Blockchain [12] is an incipient technology based on distributed ledger which accounts all transaction details called as blocks. Each block has it's own time-stamp and linked with older block make this technology enabled transaction more trustworthy and efficient among two organizations. In recent years, many financial institutions adopted this technology to facilitate a secured trustworthy transaction model. For example, Bitcoin [13], a recent innovative digital payment network and kind of money, utilizes blockchain technology. Multiple points verify the transaction validity. As a blockchain principle, where a transaction proceeds from point P to Q while other points verify and validate the transaction. If an invalid transaction occurs, the acknowledgement doesn't proceed. Ultimately all points suppose to verify, validate and attach the transaction copy to their ledger. Fundamentally it works by attaching blocks or chaining blocks concerning the transactions and reserve them in a very successive order known as blockchain. The blockchain is a decentralized database with resistant of the data modification [14]. The database is validated through the collaboration of many organizations. The following is a brief idea of how blockchain executes multiple tasks: Assume that John needs a favour from Alex in exchange for virtual currency. Once an agreement over, John's virtual wallet begins the transaction. In outcome, there will be a deduction in virtual currency in John's virtual wallet and an addition in Alex's virtual wallet. For validation purpose, any associated users would check John's virtual wallet current fund worth. After validation, the node miners will initiate to build a new block which will be added to the chain. This method will generate an associate upgraded blockchain. The hash value; associated with every transaction stored in the ledger with a time stamp; a node miner does the mining and creates the new blockchain.

In this paper, we propose the use of the open-source nature of blockchains for a secure IoV application message transaction. In our proposed scheme, every human senses data transaction is verified and validated, then stored within a block. The new block is associated to the previous block to build a chain. Each block document the transactions of millions of users in a way that the stored blocks cannot be amended by malicious attackers. The characteristics of blockchains are as follows:

Distributed: Distributed nature of database is malicious attacks resistant. A centralized database system may be one of the drawbacks in case of malicious attack but blockchain has no centralized system and every transaction by any user has to validate by each user.

Universal: Universal nature of this technology; considering there is no single authority to control this system; helps to make system more translucent nature without compromise with security.

Secure: The distributed database is secured via two steps verification process i.e., non-public and public keys generation and hash value validation.

Authority-less: Due to no single authority, many services can be performed without the approval of other users.

In the blockchain, human senses enable sensors data as blocks can be stored in a distributed manner among several thousands of servers all over the world [15], [16]. Any user of that network could have free access to the current version of the block, which is crystal clear methods to all users. The IoV application network is separated into following categories:

The first category involves the users who are allowed to build new blocks and the miners. The second category involves the users who are allowed to build and distribute only online available data. Node miners gather data, analyze them and move into blocks of blockchains [17], [18]. It is based on a chain of consecutively connected blocks. New blocks are always accumulate rigorously to the tail of the chain. The block resides a header and a body containing data [19]. The blocks are attached with keys which ensure security in the IoV applications. The key of each block requisites the security rules and regulations. The hash value, part of encryption is executed by different servers on the same network worldwide. If the outcome matches then a unique signature has been assigned

to that block which can not be altered and deleted. Node miners can only check the existing distributed data and add a request of the new block. If a node miner is looking for the specific key then he has to do an enormous amount of data recalculation. Once it's identified then he has to dispatch to other members for verification and validation. Once it's validated then it's difficult to alter. The data used in IoV applications communication may be secured by blockchain. Each new data record encompasses a reference to the previous source record rules and regulations. The enormous data experience genius rules and regulations among physical devices and sensors, which creates the prerequisites for blockchain-based IoV technology where contents can be viewed openly; which makes it more secured. This innovative approach allows users to secure human senses personal data, because the hash value process is inevitable. In case of original data is changed, it receives a unique digital signature as an outcome.

VI. Implementation and performance analysis

In this section, we illustrate the implementation and the performance analysis using the following steps: inception, encryption and data migration, block preparation, decryption and data uploading in proposed scheme algorithm (Fig. 1).

Inception: At this step, IoV network randomly issue a unique user ID U_{ID} every user. This U_{ID} consists of the secondary key, primary key, hash value, R is a number; generated once and seen by the user only, and time stamp of key generation.

$Key_{secondary}$ = Hash value $(Key_{primary}||R||Timestamp)$

The secondary key keeps all the record of the data transaction. If this key is forbidden, the user will be lost his privacy. The secondary key can be retrieved back by using R.

Encryption and data migration: When a user in IoV network wants to migrate data, then an encryption process takes place. In our proposed scheme, we prefer an encryption mechanism to encrypt data using the secondary key. The user generates unique sequential ID with the time stamp for the specific database encryption.

$Seqential_{ID}$ = Hash value $(Key_{primary}||Timestamp)$

The hash value to ensure data authenticity and integrity can fix any length of the binary value. If a malicious attacker alters the stored information in IoV network, by checking the hash value, attacks can be identified and the malicious attacker can be blocked by broadcasting his information in IoV network. Once the primary key matches, then the encryption process will be completed and data will be migrated to the destination.

Block preparation: In this step, the block can be prepared and add into the blockchain. In the initial, a node miner is selected by a few users in the network by voting process and that node miner has authority to mine the blocks. A new generated block consists of primary key; which has hash value associated. IoV network system will broadcast new block addition confirmation after verification and validation of node miner and a hash value. All the user in IoV network should accept the new block in their blockchain.

Decryption and data uploading: In this step, the decryption process takes place. As the blockchain technology has transparency and any user may retrieve the contents. However, users can obtain the corresponding decryption key by satisfying rules on the public blockchain ledger access. If the user in IoV network requires some information with sequential ID then the user has to raise a request to node miner. After verification of request user by node miner, it will share the request information with verified and validated the user in IoV network. This two-step verification implemented to enhance the security. The IoV can exclusively modify the future communication methods and enormous scope for research and development worldwide.

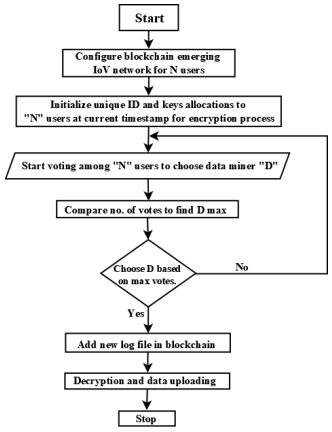

Fig. 1: Proposed scheme algorithm.

Trustworthy communication: The IoV application network may consist of billions of sensors, physical devices and other objects to exchange enormous of gathered data and facilitates various beneficial services. The wireless networks usually establish non-secure connections; which allow malicious attackers to steal sensitive data from the network. Consequently, the blockchain-based IoV provide a beneficial mechanism to restrict malicious users, illegitimate access, and external intrusion. The proposed encryption and decryption scheme address the security and privacy issues. Another way is to facilitate trustworthy communication over the network is to develop security policies and regulations for data transmission across the wireless network.

Security analysis: The security analysis in IoV applications network referred to the avoidance of malicious attacks. Using the proposed scheme, any user in the network get data access successfully after he fulfils the regulations set by other users and node miner. We assume that any user in IoV network not et all reveals his U_{ID} to others such as secondary key, primary key, and sequential ID. Once the user reveals his U_{ID} then it will be unsecured or public.

The malicious attackers may try to attack any information stored on the IoV network, for that activity he needs to get decryption key to decrypt the encrypted data. If attackers succeed then unlimited secured data can be uploaded and altered in IoV network. In our proposed scheme, the blockchain emerges with IoV network which protects data integrity and secured reliability of information. A malicious attacker may try to

demolish the blockchain-based IoV network. In case, if the attacker is a legitimate user of IoV network and attempts to encrypt irrelevant data and deliver data transactions to node miners to affect network traffic. Our proposed scheme can confront such attacks. Those attackers can easily identify by comparing the hash value. Even if a legal user attempts to upload irrelevant data in IoV network, without secondary key he can't.

Privacy analysis: Our proposed scheme in blockchain-based IoV network facilitates secured QoS to their users. We used the data encryption to ensure data security and rules facilitates to reliability in data encryption. This mechanism facilitates data privacy to the data. Privacy of users in IoV network is a key of our proposed scheme. Users need to keep their U_{ID} safe and $Key_{secondary}$ help them to retrieve his data transaction in case they lost. The key management process in the proposed scheme is very simple and faster encryption and decryption process.

VII. Blockchain Use Case and Analysis

This section provides several use cases illustrating the applicability of blockchain to IoV. In a traffic situation involving a set of vehicles that are networked, each vehicle functions essentially a mobile router. The vehicles within the network transmit messages among them and establish trust based on their transaction history.

This section discusses the IoV components in vehicular ad hoc networking architecture.

Transactions: Communication messages among vehicles in the IoV architecture are known as transactions. In the blockchain-based IoV, each transaction initiated by a vehicle is intended for a selected operation. Store transaction is used by vehicles to store data. A generated access key by a vehicle owner is used to access the cloud storage. A monitor transaction is periodically to observe a gadget info. All transactions to or from the vehicles are put away in a community blockchain.

Community Blockchain: Associated with each IoV is a community blockchain that monitors transactions and has an administration header to implement clients administrative strategy for approaching and active transactions. Beginning from the genesis transaction, each gadget's transactions are affixed together as an permanent ledger in the blockchain. Each block in the community blockchain contains two headers that are indicated as block header and administrative approach header. The block header has the hash of the previous block to keep the blockchain unchanging. The administrative approach header is utilized for approving gadgets and upholding proprietor's control policy over his home.

On-vehicle Miner: On-vehicle miner is a gadget that centrally processes all transactions to and from the vehicle. The miner could coordinate with the vehicle's Internet gateway or a different independent gadget, could be set between the gadgets and the vehicle gateway. Like existing central security gadgets, the miner verifies, approves, and reviews transactions. The miner gathers all transactions into a block and attaches the full block to the blockchain. To give extra limit, the miner deals a local storage.

On vehicle local Storage: On vehicle local storage is a storing gadget, for example, a backup drive, that is utilized by gadgets to store information locally. This storage can be incorporated with the miner or it tends to be a different gadget. The capacity utilizes a First-in-First-out (FIFO) strategy to store information and stores each gadget's information as a ledger affixed to the gadget's beginning stage.

Evaluation and Analysis: This section gives a total discourse on the security, privacy, and performance of the blockchain based IoV.

Security Analysis: There are three principle security necessities that should be addressed by any security plan, in particular: privacy, trustworthiness, and accessibility. Privacy suggests that just the approved client can peruse the message. Trustworthiness infers that the sent message is gotten at the goal with no change, and accessibility implies that each administration or information is accessible to the client when it is required. Next, we analyze the viability of our proposed solution to avoid basic security attacks that are especially applicable for IoV. The Denial of Service (DoS) attack in which the aggressor utilizes a few tainted IoT gadgets to overpower a specific objective node. The proposed design has a various levelled resistance against this attack. All transactions must be checked by the miner. Assume that the attacker by one way or another still figures out how to taint the gadgets. The second degree of protection originates from the way that all outgoing traffic must be approved by the miner by looking at the administration header. Since the solicitations that comprise the DoS attack traffic would not be approved, they would be obstructed from leaving the vehicle.

Performance Evaluation: Blockchain-based IoV architecture causes computational and packet overhead on the IoV gadgets and the miner for giving improved security and privacy. To assess these overheads, we simulated an IoV scenario in a Cooja simulator. To compare about the overhead of the blockchain-based IoV architecture, we simulated another scenario that handles transactions without encryption, hashing, and blockchain. We allude to this baseline method as the "base method". We utilized IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) as the basic correspondence for a vehicle setting. We simulated three z1 mote sensors (that mimick IoV gadgets) which send information straightforwardly to the local available vehicle miner every 2 seconds. Each simulation went on for one minute and the outcomes displayed are averaged over this span (TABLE I). A cloud storage is straightforwardly associated with the miner for storing information and restoring the block-number.

Fig. 2 demonstrates the outcomes for the time overhead.

TABLE I: Packet Overhead Evaluation

Packet Flow	Base (Bytes)	Blockchain based (Bytes)
From devices to the miner	10	25
From the miner to the cloud	10	48
From the cloud to the miner	10	28

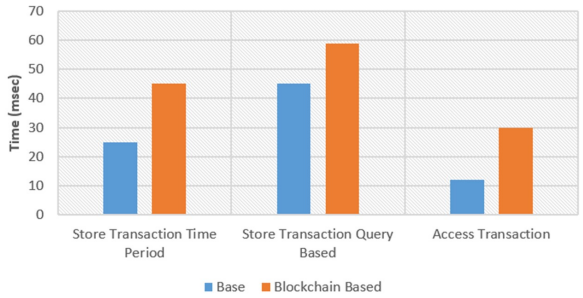

Fig. 2: Time Overhead Evaluation.

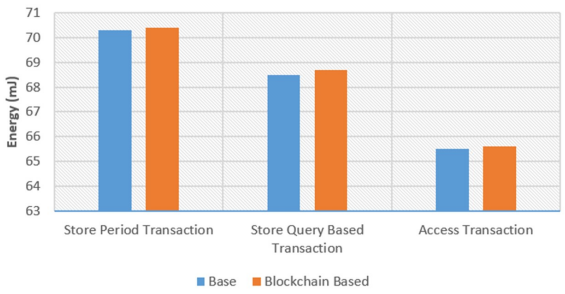

Fig. 3: Energy Consumption Evaluation.

The blockchain based design expands more opportunity to process packets contrasted with the base method, which can be ascribed to the extra encryption and hashing tasks. In the most pessimistic scenario for the query-based store transaction the extra overhead presented by proposed strategy is 20ms.

Fig. 3 outlines the energy consumption results. As is apparent, the blockchain technique expands the energy utilization by 0.1 (mj). The table frameworks the energy utilization for the 3 center errands performed by the miner, namely: CPU, transmission (T_x), and listening (L_x). The energy utilization by CPU expanded generally 0.1 (mj) in our design because of encryption and hashing. Transmitting longer information packets multiplied the transmission energy utilization of our strategy in contrast with the base method. In synopsis, the low overheads presented by our blockchain-based IoV pale given the noteworthy security and privacy advantages to be gained.

VIII. Conclusion and Future Work

We have proposed an efficient and secured scheme for blockchain-based IoV to facilitate user's privacy in his sharing data in the network. We describe the evolution and how important of IoV applications in the daily life of a human being in future communication, the generic architecture, numerous possible applications, and implementation of the blockchain technology in IoV network; which verify each stage process to ensure the privacy of the user's personal data. The blockchain technology emerging in IoV is a revolution on the level of the new innovative invention. Through analysis, we show that the proposed scheme is secure and efficient and also facilitate data integrity, confidentiality to attain user privacy. This emerging technology will impact over worldwide to redesign business models. The innovation of blockchain-based IoV will drive the future of innovative research, technology and design development of imaginative products.

References

[1] Ning, Zhaolong, Xiping Hu, Zhikui Chen, MengChu Zhou, Bin Hu, Jun Cheng, and Mohammad S. Obaidat*" A cooperative quality-aware service access system for social Internet of vehicles,"* IEEE Internet of Things Journal 5, no. 4 (2018): 2506-2517.

[2] Y. Mizuno and N. Odake, *"Current Status of Smart Systems and Case Studies of Privacy Protection Platform for Smart City in Japan,"* in 2015 Portland International Conference on Management of Engineering and Technology (PICMET), Aug 2015, pp. 612 - 624.

[3] A. Hefnawy, et al.*"Lifecycle Management in the Smart City Context: Smart Parking Use-Case,"* The 13th IFIP PLM16 International Conference, Columbia 11-13 July, 2016.

[4] A. U. A. A. Butt, S. R. Bramwell, and B. T. Fudge*"Multimedia distribution system,"* Jun. 25 2013, US Patent 8,472,792.

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander,*"Where is current research on blockchain technology? A systematic review,"* PloS one, vol. 11, no. 10, 2016.

[6] Sachin Sharma and Seshadri Mohan,*"Cognitive Radio Adhoc Vehicular Network (CRAVENET): Architecture, Applications, Security Requirements and Challenges,"* Advanced Networks and Telecommunications Systems (ANTS), IEEE International Conference, pp. 1-6, 2016.

[7] Sachin Sharma, Awan Muhammad, and Seshadri Mohan, *"Smart vehicular hybrid network systems and applications of same,"* March 29, 2018, U.S. Patent 15/705,542.

[8] Sachin Sharma, Ghanshala Kamal Kumar, and Seshadri Mohan, *"A Security System Using Deep Learning Approach for Internet of Vehicles (IoV),"* In 2018 IEEE 9th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Nov. 8 âĂŞ Nov. 10, 2018, Columbia University, New York, USA.

[9] Kamal Kumar Ghanshala , Sachin Sharma, Seshadri Mohan, and R. C. Joshi, *"Cloud-Based Cognitive Radio Adhoc Vehicular Network Architecture: A Next-Generation Smart City,"* In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 145-150. IEEE, 2018.

[10] Sachin Sharma, M. Baig Awan, and Seshadri Mohan, *"Cloud enabled cognitive radio adhoc vehicular networking (CRAVENET) with security aware resource management and internet of vehicles (IoV) applications,"* In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6. IEEE, 2017.

[11] Sachin Sharma, Awan Muhammad, and Seshadri Mohan, *"Cloud enabled cognitive radio adhoc vehicular networking with security aware resource management and internet of vehicles applications,"* U.S. Patent Application 16/058,488, filed December 6, 2018.

[12] W. Mougayar,*"The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology,"* John Wiley & Sons, 2016.

[13] *"https://bitcoin.org/en/,"* accessed on 18 June 2018.

[14] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou,*"Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,"* in Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016, pp. 839 - 858.

[15] M. Pilkington,*"Blockchain Technology: Principles And Applications,"* In Research Handbook On Digital Transformations, O. F. Xavier, Z. Majlinda, And E. Edward, Eds., Ed, 2016, P. 225.

[16] K. Kotobi and S. G. Bilen,*"Blockchain-Enabled Spectrum Access In Cognitive Radio Networks,"* In Wireless Telecommunications Symposium (WTS), 2017, Chicago, Il, Usa, 2017, pp. 1-6.

[17] LI Yang, XIN Yonghui, HAN Yanni, LI Weiyuan, Xu Zhen,*" A survey of DoS attack in content centric networking,"* J. Journal of Cyber Security. 2017, 2(1):91-108.

[18] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang,*"The blockchain as a decentralized security framework,"* IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18 - 21, 2018.

[19] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram,*"Blockchain for IoT security and privacy: The case study of a smart home,"* in Proc. IEEE Int. Conf. Pervasive Computing and Communications Workshops, 2017, pp. 618 - 623.