



**Graphic Era**  
Deemed to be University  
Accredited by NAAC with Grade A  
Approved by AICTE, Ministry of HRD, Govt. of India



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

AUTHORS: DR. SACHIN SHARMA & DR. SESHADRI MOHAN  
PRESENTER : DR. SESHADRI MOHAN

WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

5

## Outlines

- Introduction
- Generic architecture for IoV networks
- Applications of IoV
- Security and privacy in IoV applications
- Overview of Blockchain
- Implementation and performance analysis
- Conclusion and future work

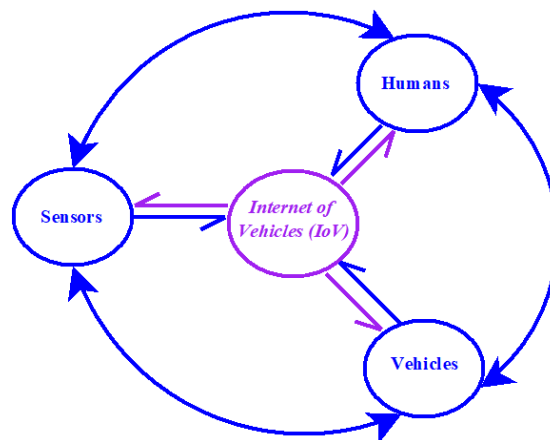
WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

6

## Introduction

- 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.
- 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.
- Blockchain technology facilitates secured communication among users in a connected vehicles network.
- The proposed architecture provides a reliable and secure environment for information sharing among connected vehicles.

## IoV architecture



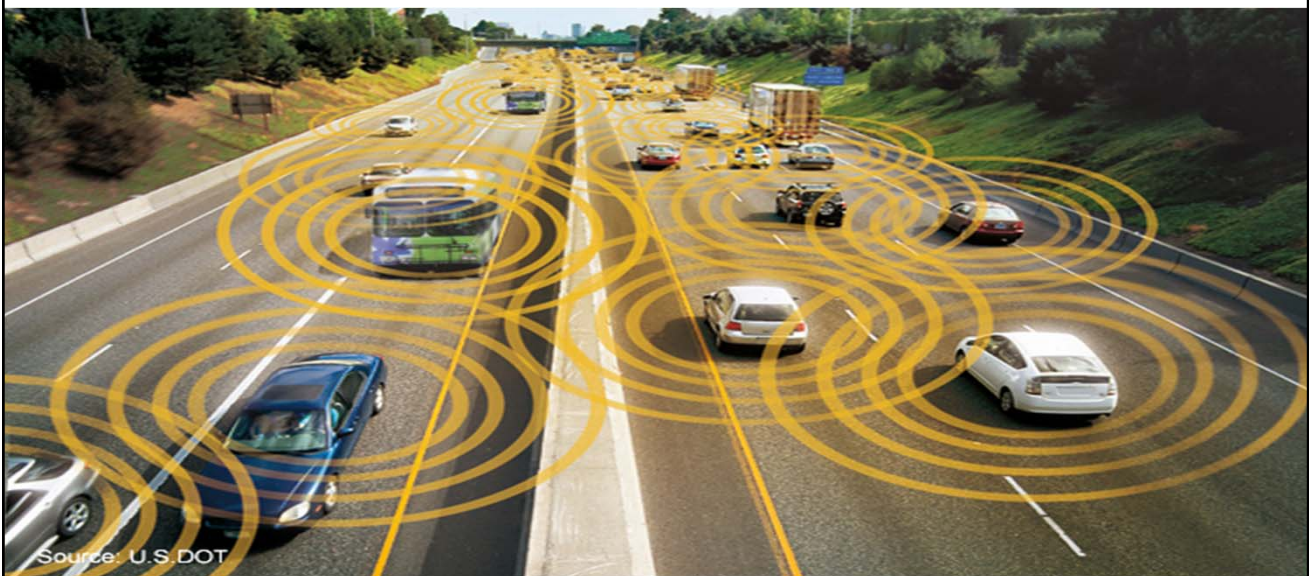
## Generic architecture of IoV networks

- IoV networks establish communication among an extensive number of physical devices and variety of sensors.
- 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.
- The IoV network facilitates improvement in existing user-friendly new advanced technology, applications and business models.

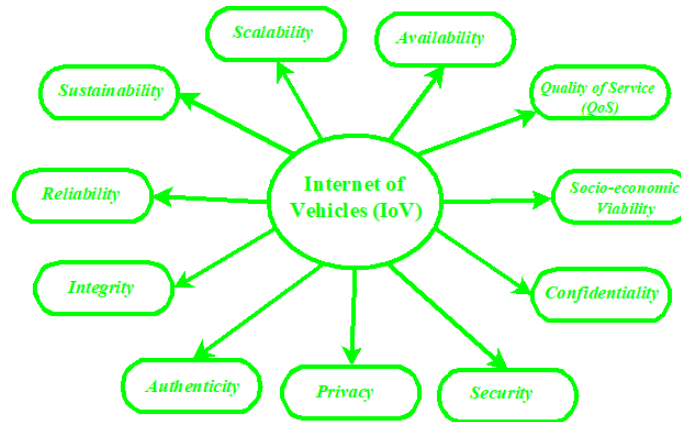
WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

9

## SmArT VehiculAr Network Techbox (SAVANT)



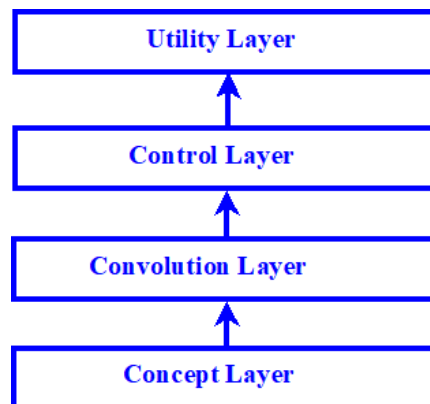
## Characteristics of IoV architecture



WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

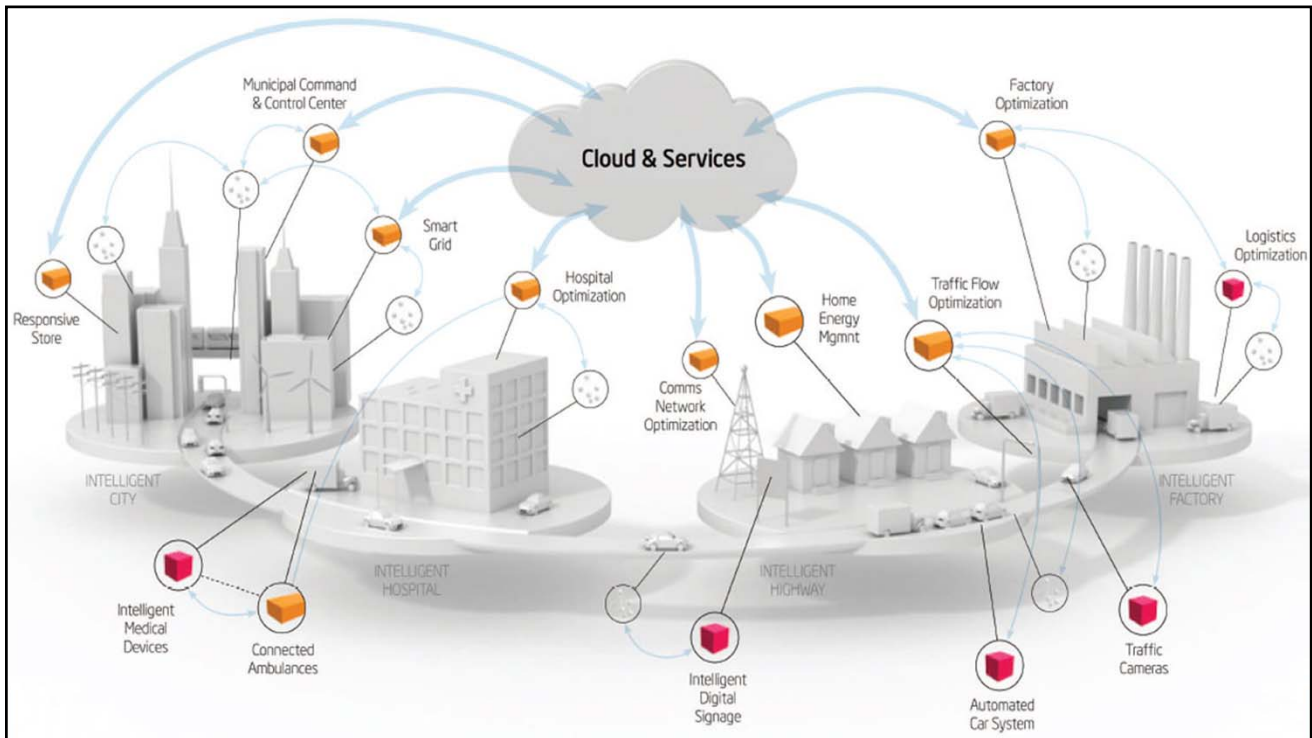
7

## Layers of IoV Network architecture

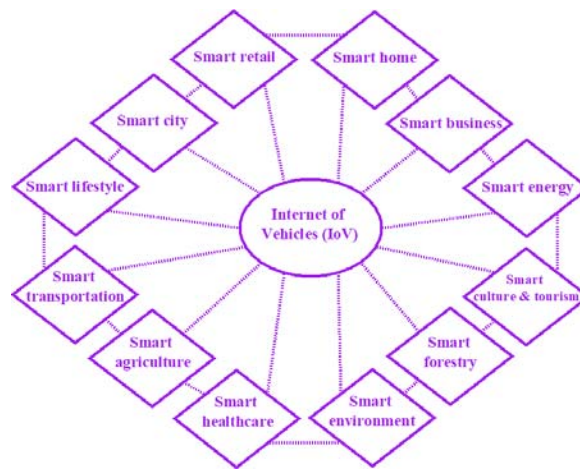


WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

<



# Applications of IoV



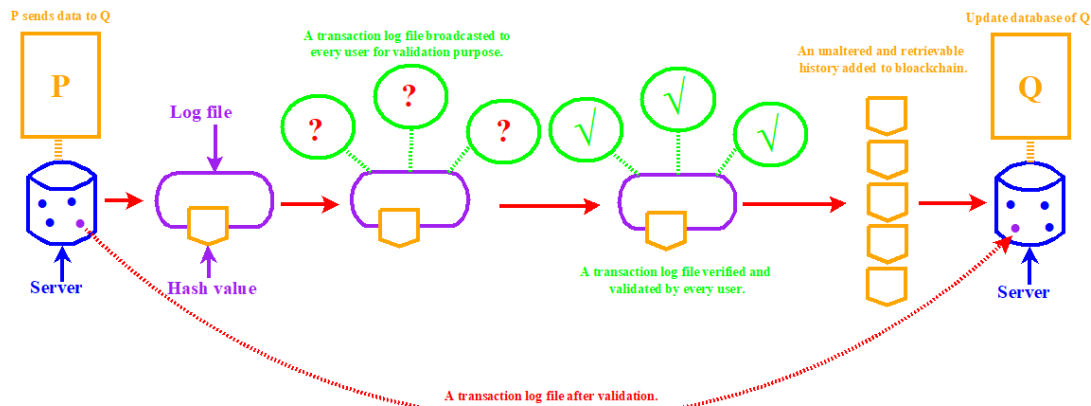
## Security and privacy in IoV applications

- The security and privacy functionality must provide confidentiality, integrity, availability, authenticity, reliability and authorization of data collected from various sensors under IoV applications networking .
- In the future, IoV will be a most remarkable network of the global economy.
- In IoV networking architecture, the smart sensors are connected with the Internet or external network for collecting data via transmission.
- Guarding the privacy of information sensed by specific sensors is one of the critical challenges in IoV networking.

## Overview of Blockchain

- Blockchain is an incipient technology based on distributed ledger which accounts all transaction details called as log files.
- Each log file has it's own time-stamp and linked with older log file 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.

## Basic Blockchain architecture



WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

57

## Implementation

The implementation and the performance analysis process includes the following steps: inception, encryption and data migration, log file preparation, decryption and data uploading.

- **Inception:** At this step, IoV network randomly issues a unique user ID (UID) to every user. This UID 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.
- **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.

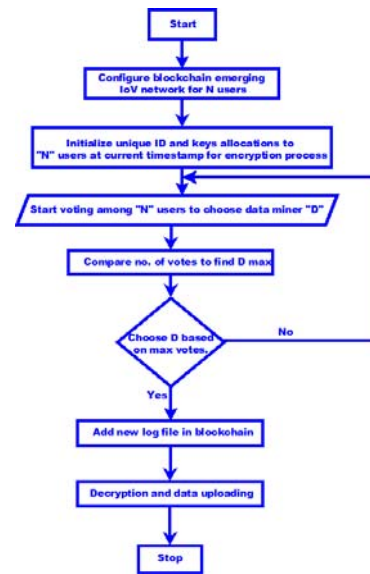
WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

58



➤ *Log file preparation:* In this step, the log file can be prepared and added into the blockchain. Initially, a data miner is selected by a few users in the network by a voting process and that data miner has authority to mine the log files.

➤ *Decryption and data uploading:* In this step, the decryption process takes place. As the blockchain technology has transparency, any user may retrieve the contents. However, users can obtain the corresponding decryption key by satisfying rules on the public blockchain ledger access.



WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

15

## Security and Privacy

**Security:** The security analysis in IoV applications network referred to the avoidance of malicious attacks. 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 data miners to affect network traffic, our proposed scheme can confront such attacks. Those attackers can easily be identified by comparing the hash value. Even if a legal user attempts to upload irrelevant data in the IoV network, without the secondary key, uploading will fail.

**Privacy:** Our proposed scheme in blockchain based IoV network facilitates secured QoS to their users. We used the data encryption to ensure data security and the Blockchain rules ensure the reliability in data encryption. Users need to keep their UID safe and utilize the secondary key to help them to retrieve the data transaction. The key management process in the proposed scheme is very simple and faster encryption and decryption process.

WIRELESS WORLD RESEARCH FORUM MEETING 41, 30 OCT. – 1 NOV., 2018, HERNING, DENMARK

5 :



## Blockchain Versus IoV Blockchain

- Trust
  - Trust among automotive industry (Tier – I/II vendors).
- Security
  - Security of useful data transmission among various types of sensors in connected vehicles.
- Smart Contracts
  - Smart contracts development among multiple IoV application service providers
- Fair Access
  - Fair access to IoV applications user data.

## Conclusion and future work

- We apply blockchain technology to efficient and secured scheme for blockchain-based IoV to facilitate user's privacy in sharing data with the network.
- The blockchain technology will emerge in IoV as the technology to ensure privacy and security.
- Through analysis, one can show that the proposed scheme provides security and also facilitates data integrity, confidentiality so as to ensure privacy of user data.
- This emerging technology will impact businesses worldwide and motivate them to redesign business models.
- The innovation of blockchain-based IoV will drive the future of research, technology and design and development of novel and innovative products.

# Thank You !