IOT STANDARDS

IoT Standards Matters will look at different segments of the IoT market as it relates to implementation and use of standards. Each column will select a particular vertical, and lay out the relevant standards and technologies that affect the evolving IoT hyperspace. The pace of the columns will start broadly with the vision of narrowing the subject of subsequent articles toward more specific applications of standards, whether in the development, application, test, or commissioning of IoT technologies.

INTRODUCTION

Internet of Things concept's pervasiveness has overshadowed every application domain, be it consumer, industrial, enterprise, strategic or infrastructure. Across industry verticals, applications of the IoT continue to expand, and a shift has occurred from clusters of siloed IoT devices to interconnected IoT environments. This is especially apparent in settings such as factory floors and automotive vehicles. However, the IoT hasn't yet scaled as quickly as expected, and the IoT industry hasn't achieved a genuinely seamless experience in which devices pass into and out of physical environments and are identified, trusted, and managed without a need for separate (and at times manual) authentication steps. And, Internet of Vehicles (IoV) is another such an IoT environment which is yet to come of age and meet the users expectations. A systems approach in addressing the Security, Privacy & Trustworthiness concerns through appropriate standards can help realize this vision sooner than envisaged...

MENTOR'S MUSINGS ON THE ROLE OF STANDARDS IN IMPROVING THE PRIVACY, TRUST AND REPUTATION MANAGEMENT IN INTERNET OF VEHICLES (IOV)

by N. Kishor Narang
Technology Philanthropist, Innovation & Standardization Evangelist

INTERNET OF VEHICLES

Internet of vehicles (IoV) is a network of vehicles equipped with sensors, software, and the technologies that mediate between these with the aim of connecting & exchanging data over the Internet according to agreed standards. IoV evolved from Vehicular Ad Hoc Networks ("VANET," a category of mobile ad hoc network used for communication between vehicles and roadside systems) and is expected to ultimately evolve into an "Internet of autonomous vehicles." It is expected that IoV will be one of the enablers for an autonomous, connected, electric, and shared (ACES) Future Mobility.

Road vehicles as a product category depend upon numerous technology categories from real-time analytics to commodity sensors and embedded systems. For these to operate in symphony the IoV ecosystem is dependent upon modern infrastructure and architectures that distribute computational burden across multiple processing units in a network. In the consumer market, IoV technology is most typically referenced in discussions of smart cities and driverless cars. Many of these architectures depend for their functionality upon open-source software & systems.

IoV is revamping the automotive system into a large and diverse car network, which has many benefits, including changes

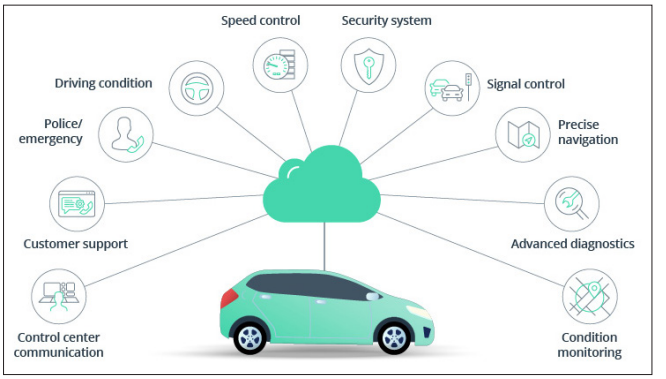

FIGURE 1. Internet of Vehicles.

in information services, intelligent vehicle management, increased productivity, reduced traffic congestion, and car accidents. The IoV promotes automobiles and information technology, highlighting applications in terms of efficiency, safety, infotainment, connected devices, safety, and everything else. The Internet of Vehicles aims to fundamentally improve transportation by connecting vehicles, drivers, passengers, and service providers together. Several new services such as parking space identification, platooning and intersection control, to name just a few, are expected to improve traffic congestion, reduce pollution, and improve the efficiency, safety and logistics of transportation. The IoV is expected to enable a number of applications essential for self-driving vehicles such as collision detection, lane change warning, traffic signal control, intelligent traffic scheduling, fleet management, remote diagnostics or infotainment. By talking to each other, vehicles can, for example, avoid collision, one of the requirements that must be met for automotive vehicles to become fully autonomous.

SHIFTING PERSPECTIVES – V2X TO VANET TO IOV:

Vehicles are undoubtedly becoming smarter and in-vehicle technology is getting better. One aspect receiving significant attention is the smart vehicle's ability to communicate with occupants as well as with its surroundings. Thus far, communication in vehicles had primarily focused on the occupants by serving them consumable content from remote servers or the cloud. This content delivery is commonly referred to as infotainment — where the occupants are served with information related to their journey (such as maps, weather, attractions, places of interest, congested roads, and nearby accidents) or with entertainment options (such as satellite radio, music, internet connectivity, and social networking applications). Vehicle connectivity also enables services such as emergency communication in the event of an accident or a breakdown of the vehicle. The vehicle's on-board diagnostics (OBD)-II (2nd Generation) port is a rich avenue for procuring messages on the performance and health of the vehicle, and providing them to the driver or a service technician for improved troubleshooting. The Vehicle performance Data extracted through the OBD port is being leveraged to even optimize the Insurance Premium for vehicle as the driving habits of the driver are inferred through the vehicle operational data.

Over the past several years, inter- vehicle communication has received a lot of interest, especially in the context of safety, where it has been subject to a significant amount of research. It is now fairly well-recognized that inter- vehicle communication could potentially help in the reduction of traffic-related fatalities.

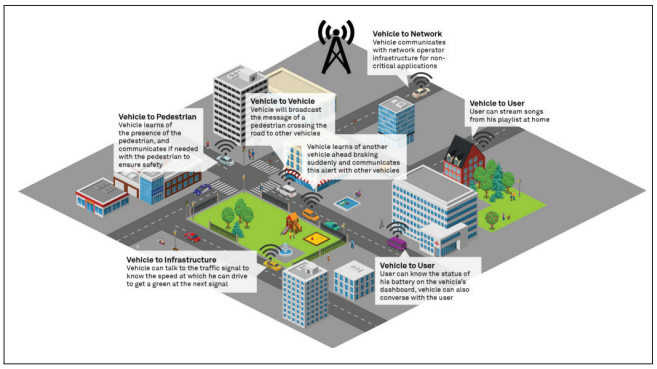

FIGURE 2. Various communication systems for connected vehicles.

With the rapid increase in vehicular technology, the vehicular ad hoc network is slowly converting into the Internet of Vehicles (IoV). VANET turns every vehicle to join other vehicles by wireless communications. However, it comes with the limitations of covering a small network that limits the flexibility and the number of connected vehicles. Further, few points like driver's behavior, challenging roads, and jams are the hindrances of VANET communication. Hence, it would be right to mention that in VANET; the involvement of objects is unstable and random. Therefore, the VANET was not enough to provide the services or the applications to its customers, and these reasons initiated the inception of IoV. The IoV majorly has two technologies that are vehicle intelligence and vehicle networking. Vehicle networking combines VANET (Interconnection of Vehicles) + Vehicle Telematics (Connected Vehicles) + Internet of Devices. Vehicle intelligence emphasizes the combination of various applications which support artificial intelligence, deep learning, and swarm computing, etc. to improve the safety of the driver and to achieve enhanced safety in vehicular technology.

Hence, the IoV is a combination of vehicles, an intelligent environment, humans, smart things, and a vast network that provides services in large cities. IoV is considered an integrated system with features like high conformity, controllability, validity, and numerous vehicles, networks, users, and smart devices. IoV is the deep integration of the user-vehicle-device-environment that extends to provide an efficient service level to the users as per their expectations and satisfaction. It is also called VANET, which is like a subset of IoV. IoV has telematics, defined as a technology based on wireless networks, that helps send, receive, and store the data, including speed, times, faults, consumption, and more. Also, from the past years, an enormous number of users have been included in the evolution of IoT, Big Data, and cloud computing. IT companies have published many applications or services, but VANET lacks the capacity to process complete information; hence, it can be used on small-scale applications, which generally reduces the number of users. Therefore, the traditional VANET, telematics, and other connected vehicle networks need something on a large scale. Hence, the Internet of Vehicles (IoV) came into existence.

It is required to highlight why it is impossible to achieve the same with the usage and application-level support of IoT. The reason behind this is that some aspects of IoV are distinctive from IoT. IoT majorly targets the objects and provides the data for connecting things, whereas the Internet targets the user and serves the utility for the users. IoT is a platform for connecting the things that we use daily and embedded with sensors, software, and electronics to the Internet and enabling them to gather and exchange information. Information can be anything or everything; however, IoV majorly concentrates on integrating users and vehicles wherein users and vehicles can interchangeably act as an intelligence of each other. The network models in IoV are also quite different from the IoT and Internet.

Currently, most of the researchers are working on V2V (Vehicle) and V2I (Infrastructure) communication, as it provides safety-related information well in advance to the driver of the vehicle, which helps save lives and time. Furthermore, Intelligent Transportation System (ITS) focuses primarily on safety and latency-sensitive services like collision detection, route navigation, traffic management, or emergency alert-related information that are supported via V2V and V2I communication. The Intelligent Transportation System (ITS) is an application that provides services related to transportation and traffic management to make lives better and provide safety to drivers and passengers. The main reason for the development of ITS was various road accidents, pollution, and traffic congestion, mainly in the metro cities. Road accidents are a significant concern for the driver and the passengers. ITS is the backbone for the development of next-generation technologies. It incorporates various fields like management of transportation, control of the traffic, and different policies. Wider areas of the ITS are information management, incident and emergency systems, Electronic Toll Collection, traffic management, etc. Recently, India has successfully implemented automatic toll gates, equipped with sensors that sense the vehicle, scan the QR code associated with the vehicle, and automatically collect the toll cost.

Taxonomy of IoV

In taxonomy of IoV communication, essentially, IoV has the foundation in five types of network communication. Vehicle-to-Vehicle (V2V) communication supports the exchange of information with outside vehicles. With the help of V2V, each vehicle acts as a node and tries to connect to the other moving vehicles. The network created by V2V is of a wide range. The information like the crash event on the route can quickly be passed from one vehicle to another vehicle with the help of V2V communication. The communication shall be quick enough without much delay so that the other vehicle receives the information without any delay.

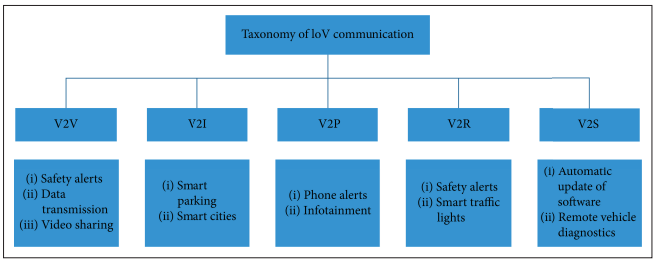

FIGURE 3. Taxonomy of Internet of Vehicles.

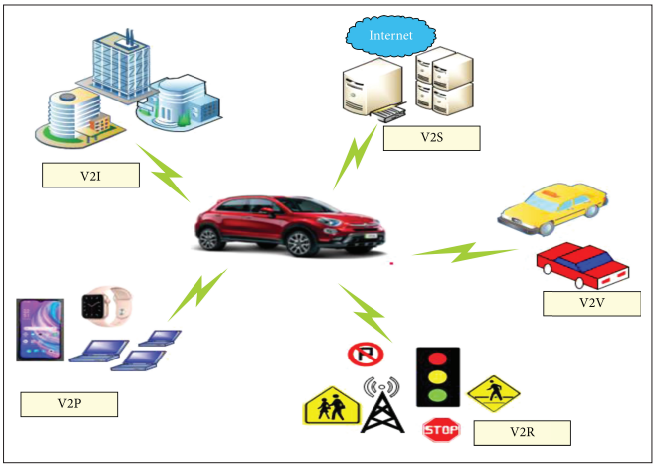

FIGURE 4. Internet of Vehicles ecosystem.

Vehicle-to-Personal devices (V2P) bring attention to applications like Carplay and android auto support in vehicles. In this era, when the hands-free profile is in use, with the help of Android and iOS platform, it is easy to connect personal devices to the infotainment unit of the vehicle and communicate with the personal devices. The phone application can be replicated over the infotainment display, and the usage of applications like call, music, navigation, SIRI, and Google assistant can be made available for the driver to use without taking phones in the hands. Vehicle-to-Server (V2S) supports the additional information accessible from the APIs with the help of the Internet. Now, it is possible to update the vehicle software by Over the Air (OTA) communication using V2S-based network communication. This is essential for the communication from the servers and any information update. Vehicle-to-Infrastructure (V2I) supports the communication with the building or infrastructure of the city. In this type of application, drivers can easily be aware of the parking space availability in the malls and other scenarios like the availability of tables for food in some malls. Vehicle-to-Roadside unit (V2R) is used to communicate with roadside units like traffic signals or warning signs for the road walk. Also, while communicating between the vehicles in a dense network packet loss is the problem; considering the use of RSU, the communication between the vehicles can be maintained effectively.

Layered Architectures of IoV

The main inclinations of the IoV environment are to solve the problem of the connection between multiple devices in multiple fields (traffic management, security and entertainment, and information). However, due to privacy, usability, and accessibility issues, the interaction of these applications has limitations, so they usually act as independent entities. To reduce such problems, attempts are being made on the development of cross interoperability platforms, elements, and devices from different vehicles that can collaborate in the environment of IoV.

The architectures are still eveloving as new needs, use cases and concerns are being identified by various stakeholders of the IoV ecosystem, which itself is expanding with the onslaught of disruptive innovations like AR/VR/XR, Metaverse, Web 3.0...

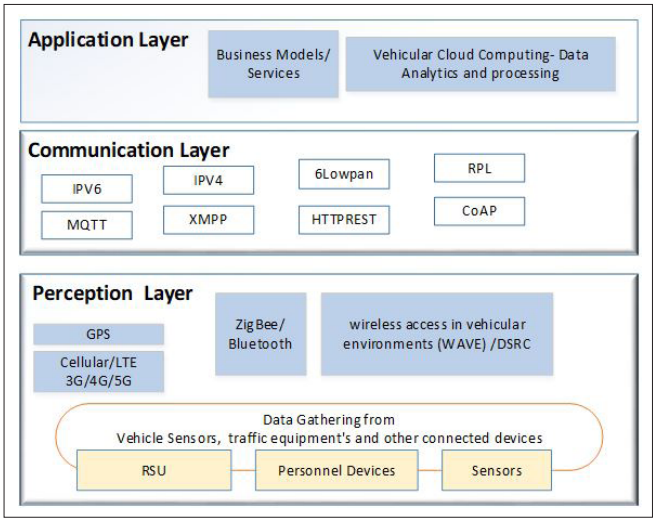

FIGURE 5. Macro architecture — Internet of Vehicles.

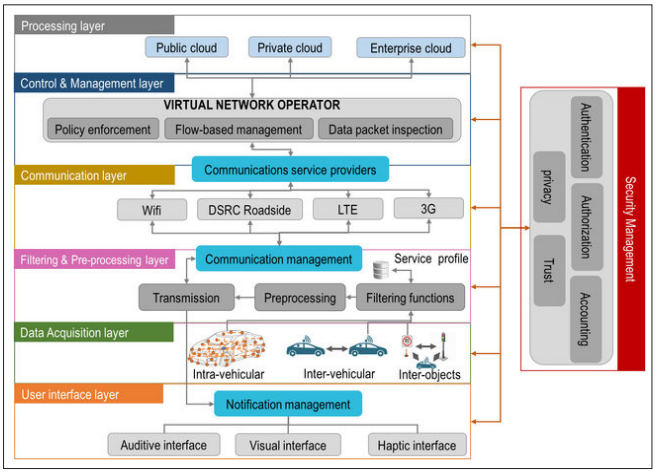

FIGURE 6. Granular architecture — Internet of Vehicles.

Rising Concerns in IoV

The Internet of Vehicles aims to fundamentally improve transportation by connecting vehicles, drivers, passengers, and service providers together. Several new services such as parking space identification, platooning and intersection control, to name just a few, are expected to improve traffic congestion, reduce pollution, and improve the efficiency, safety and logistics of transportation.Proposed end-user services, however, make extensive use of private information with little consideration for the impact on users and third parties (those individuals whose information is indirectly involved) creating serious privacy and trust issues in the Internet of Vehicles at the service level. Various concerns over privacy can be formalised into four basic categories: privacy of personal information, trust, consent to provide information, and multi-party privacy.

To help analyse services, the main relevant end-user services can be taxonomised according to voluntary and involuntary information they require and produce. Other open problems relate to measuring the trade-off between privacy and service functionality, automated consent negotiation, trust towards the IoV and its individual services, and identifying and resolving multi-party privacy conflicts.

Security & Privacy in Internet of Vehicles

In IoV, we need to integrate many different technologies, services, and standards. However, heterogeneity and the large number of vehicles will increase the need for data security. IoVs, as with other technologies, have many security vulnerabilities. Vehicles operate in vulnerable and unprotected environments with serious problems of security in vehicle-to-infrastructure and cloud communications. IoVs can become very vulnerable to cyberattacks. Malicious people can exploit vulnerable connection points and manipulate vehicular data streams with devastating effects such as: MP3 files infecting a whole network of cars very quickly. Once the cybercriminal gets control of the car's data system, he/she could manipulate different components of the car such as brakes, unlock doors, or even turn the car off. At a recent Black Hat cybersecurity conference, a demonstration showed how some software allows attackers to control a Jeep Cherokee while on the move. This example demonstrates the potential dangers on the road ahead for the IoV. One way to analyze the security problem from an effort-and-impact perspective is to identify mitigation techniques that are used in comparable critical infrastructure systems of national importance. Disrupting a vehicle's communication or sensors, for example, would require a more complex and sophisticated

attack than one designed to simply gather information, and disrupting the vehicle's control commands would be even harder. Regardless, the threat is real and a security breach could have severe consequences on drivers, passengers, other vehicles, and infrastructures. For these reasons, it is necessary to make security a high priority for the IoV. Some efforts have been made to address security issues in the IoV. The National Institute of Standards and Technology proposed a framework to improve critical infrastructure cybersecurity that may be incorporated into IoV technologies.

Traditional approaches to security in the IoT don't support this secure, seamless experience. There is little multilayered security embedded in today's IoT solution designs. This leads to vulnerabilities that in turn require regular over-the-air updates and patches, which can't be reliably implemented. Relative to enterprise IT, solution design in the IoT space lags behind in security assurance, testing, and verification. However, the main concerns during the early stages of IoT implementation are around interoperability, cybersecurity, and installation complexities.

Although security, privacy, and trust at a vehicle network level have been explored to some extent, privacy and trust at the service level remain nebulous.The wide spectrum of IoV services utilise personal information (e.g. location, behavioural patterns, videos), which may additionally include involuntary information about third parties (e.g. images of pedestrians or private properties). Such improvident information sharing can lead to breaches in users' and non-users' privacy. Furthermore, access to information through the IoV raises additional concerns, such as whether the IoV can be used as a means to monitor people's activities. Privacy, however, can be a convoluted issue, because minimising information exchange can have negative impact on services and trust in some cases, making it difficult to demonstrate that service providers—and the IoV—are trustworthy.

Digital Trust (or trust in digital solutions) is a complex topic. When do users deem a digital product truly trustworthy? What if a physical product component is added, as in smart, connected products? While security is certainly a key enabler of Digital Trust, there are many other aspects that are important, including ethical considerations, data privacy, quality, and robustness (including reliability and resilience), and certification, compliance, testing as the proofed accordance with standards and rules. The trustworthiness and the risk management is essential. Further exploration of ethical considerations and potential issues could shed new light on the standardization and the cooperation with other organizations.

Trustworthiness

Trustworthiness is an overarching paradigm with a multitude of nuances and distinct aspects such that it has different connotations for different sets of stakeholders, use cases and applications. What aspect or nuance of Trustworthiness may be highly critical in one use case to its stakeholders may be absolutely trivial for some other use case and its stakeholders depending on its context and/or domain. Like Security and Privacy, Trustworthiness is a transversal characteristic that can be applied to any type of ICT Systems such as Smart Car, Domotics, IoT, IA, cloud management and smart city (e.g. system of systems). For example, smart cars develop for Germany may not be considered trustworthy in USA as they may not comply with USA's laws and regulations. Moreover, a smart car and smart pacemaker may not require demonstrating the same trustworthiness characteristics measurement outcomes to be considered trustworthy.

The Trustworthiness paradigm has evolved thru many avatars beginning with Software Quality & Dependability, during its journey subsuming various concerns like reliability, availability, safety, security and many more to a single overarching conceptual framework, which is also considered, quite rightly as Dependability 4.0.

As we already know that completely Trustworthy ICT Systems may never exist, but it is crucial to understand how to define and demonstrate that a specific ICT System can be considered Trustworthy for a specific usage in a specific context. There are multiple schools of thoughts about the Trustworthiness and its applications to various aspects of Technology, Business and Organizations in a comprehensively verifiable manner. Some consider Trustworthiness to be an abstract paradigm, some others treat it as a Non-Functional Requirement specifying emergent properties of a system — i.e. a set of inherent characteristics with their attributes — within the context of quality of use.

Trustworthiness can be viewed as a Systems Engineering concept that covers all the attributes that are involved in having stakeholders 'trust' in a given system. It is primarily a 'black box' attribute which is 'technology' agnostic but is 'domain'/application dependent. Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

Trustworthiness corresponds to the ability to meet stakeholders' expectations in a verifiable way. Depending on the context or sector, and also on the specific product or service, data, and technology used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

A working definition of trustworthiness is the degree to which a user or other stakeholder has confidence that a product or system will behave as intended. This definition can be applied across the broad range of systems, technologies, and application domains. Characteristics of trustworthiness include — Reliability, Availability, Resilience, Security, Privacy, Safety, Accountability, Transparency, Integrity, Authenticity, Quality, Usability and Accuracy...

Like with security, trustworthiness has been understood and treated as a non-functional requirement specifying emergent properties of a system — i.e. a set of inherent characteristics with their attributes — within the context of quality of use. Additionally, like with security, trustworthiness can be established through an organizational process with specific measurable outcomes and key performance indicators (KPIs).

In summary, trustworthiness has been understood and treated as both an ongoing organizational process as well as a (non-functional) requirement. Trustworthiness is ensured and maintained through a sound governance framework and systems engineering practices. Trustworthiness can contribute to the building of confidence. The terms "trust" or "trusted" are sometimes used to characterize specific interactions between technical systems. Systems engaging in such interactions could be considered as trustworthy by operators and users of those systems or by other stakeholders. The ITU-T report on Trust Provisioning introduces three layers of trust: physical trust, cyber trust, and social trust, taking into account the physical infrastructure for data collection (e.g., sensors and actuators), IT infrastructure for data storage and processing (e.g., cloud), and end-applications (e.g., ML algorithms, expert systems, and applications for end-users).

Building Trustworthy IoV Systems

Building trustworthy IoV systems, therefore, can be highly complex due to the large scale of the IoV and the sensitive information many services will require.

Trust is multifaceted and may include trust among users (e.g.), trust between users and service providers, trust between network nodes when propagating information automatically, trust during fog orchestration, finding trustworthy edge devices

to offload computations to, as well as the credibility of the IoV concept itself.

Users may avoid utilising the full spectrum of services, focusing on services from trustworthy providers or services which other trusted parties use (e.g. family). Moreover, people may distrust the IoV altogether if they anticipate the risk that their personal information can be exploited. This can remove any incentives users may have to provide the required information for the effective performance of the IoV. Meanwhile, evaluating trustworthiness in the IoV is highly challenging because it is decentralised. Trust must be handled in real time but networks may be congested in peak hours and reaction time in the IoV is limited. Thus, minimising obscurity in service models, making the intent of information usage clear and legally binding for providers, and employing privacy-by-design concepts could help protect the privacy of the user, facilitating the process of building trust in the IoV.

In addition to data that is collected willingly for specific purposes, data in the IoV can often be collected when not required and can potentially be stored and reused without the user's consent. Therefore, a significant related issue is consent to share information. Among several obligations the GDPR imposes on software operators and service providers, a key obligation is user consent. The complex granularity in the IoV together with the fleeting character of services, however, obfuscate the matter of making informed consensual decisions. This may even result in exploitation of personal information (e.g. payment info, images, location history, driving habits) and activity monitoring even with the user's consent, and may make it easier to inflict physical or psychological harm.

Today, social networks and mobile applications constantly refine privacy control features. However, privacy settings still lack the ability to fine-tune permissions in some cases. Consumers often lack enough information to make privacy-sensitive decisions, and, even with sufficient information, they are likely to trade off long-term privacy for short-term benefits. It is observed further that users consent to personal data sharing by accepting opaque and inflexible policies which are rarely read, indicating that constant consent requests may be inefficient and obtrusive. These are disconcerting findings as we expect consent-based information sharing to be the core of the IoV design and deployment.

Cyber Immunity & Cyber Resilience

The pandemic-induced digital transformation has increased exposure to cyber threats as we cross the digital fault line due to remote working and escalated online presence. To counter this, an intuitive and adaptive cyber posture defined by zero latency networks and quantum leaps will be needed across industries. These developments, while great for humanity, will challenge privilege, privacy, and defend every citizen.

The speed of processing of AI systems is currently seen as providing protection for infrastructures and networks that human operators may not be able to match, especially as cyber-attackers are employing increasingly sophisticated methodologies. AI can potentially respond to a cyberattack scenario far more quickly than a human decision maker.

Cyber Immunity at every layer will create networks that are inherently secure and self-learning. **AI-induced digital intuition** is one of the pillars of cyber-security strategy that will allow intelligent adaption. The ability of AI systems to out-innovate malicious attacks by mimicking various aspects of human immunity will be the line of defence to attain cyber resilience based on both supervised and unsupervised machine learning.

These systems will be designed to make the right decisions with the context-based data, pre-empt attacks on the basis of initial indicators of compromise or attack, and take intuitive remediated measures, allowing any digital infrastructure and organization to be more Resilient.

The Key Factors Inhibiting Wide-Scale IoT/IoV Adoption Today

The convergence of the IoT and cybersecurity can unlock a massive amount of new value. Across industry verticals, applications of the IoT continue to expand, and a shift has occurred from clusters of siloed IoT devices to interconnected IoT environments. This is especially apparent in settings such as factory floors and automotive vehicles. However, the IoT hasn't yet scaled as quickly as expected, and the IoT industry hasn't achieved a genuinely seamless experience in which devices pass into and out of physical environments and are identified, trusted, and managed without a need for separate (and at times manual) authentication steps.

The proliferation of connected devices, along with the advancement of the complexity in IoT use cases (such as autonomous systems and transportation), creates opportunities for multiple players of the value chain. But it also creates the risk of vulnerabilities that could have catastrophic consequences. The risk profiles of many IoT systems are elevated compared with that of enterprise IT, given the IoT's control over physical operations. A seamless IoT experience, therefore, requires a foundation in digital trust, functional convergence of the IoT and cybersecurity, and an early-stage integration of cybersecurity in the architecture design and pilot phase.

A Seamless IoT Experience

A seamless Internet of Things (IoT) experience in any domain, application and/or use case will consist of six components that span enterprise and consumer use cases:

Hyperconnected: Connectivity through multiple standards will be pervasive, connecting a vast number of devices and sensors that seamlessly share data.

Integrated: Integration within and across tech stacks of devices will be effortless (including minimized sign-in effort, self-managed devices, and over-the-air patch updates), with simultaneous use of multiple connectivity standards, platforms, and back-end systems.

Secure and trusted: Dynamic cybersecurity will enable a high degree of trust in handling the multilayered complexity of legacy systems and new solutions, with security enabled through AI-based threat protection at all layers.

Intelligent: Devices and systems will have the intelligence (enabled by AI and machine learning) to draw insights from data and make real-time decisions, allowing the leap from monitored to automated implementation.

Mobile: Devices and networks will require minimal maintenance, be battery efficient, and have a persona (corporate or personal identity) to allow for futuristic experiences.

Hyperpersonalized: There will be personalized experiences across different platforms and scenarios (from home to office and everywhere in between), enabled by the other factors.

Perception Gap

There is a wide mindset gap between IoT solutions buyers and providers in any domain which is more prominent in the IoV domain regarding expected IoT/IoV adoption, digital privacy, and trust concerns, and the delay caused by siloed decision-making leads. Knowing some of these facts should help future technology leaders on both the buyer and provider sides understand the others' mindsets and move toward unlocking the value.

IoV solution providers heavily underestimate the importance of digital trust in comparison with buyers. But IoV buyers

need more cohesive decision-making structures to address their cybersecurity concerns. Most providers blame siloed decision making between the IoT/IoV and cybersecurity groups on the buyer end for delays in IoT/IoV adoption. Conversely, very few buyers believe the decisions are siloed.

From these insights, we conclude that it will take a significant shift in the philosophy of IoT/ IoV solution design, along with a holistic convergence of IoT/IoV and cybersecurity functionalities, to build user confidence in the IoT/IoV, speed up its adoption, and drive new value across its verticals—thus creating a fully interconnected IoV environment. These market forces are further supported by increased policy making at both the public and private levels. Technology leaders who grasp the required mindset will be able to influence disruptive change for both consumer and enterprise applications.

When the industry can converge the IoT/IoV and cybersecurity, the reward could be enormous. What stands in the way? It's highly challenging to manage IoT cybersecurity more so in the IoV domain, because the converged solutions need to be either vertical or use case specific and to include a cross-tech stack layer. Success will hinge on various stakeholders acknowledging the challenges, committing to innovation, and agreeing on industrial standards. Testing and validating the solutions also takes time. Additionally, there is an urgent need for industry talent with expertise in both the IoT/IoV and cybersecurity, and there is already a global cybersecurity talent shortage. Moreover, embedding IoT skill sets within cybersecurity is an emerging discipline.

However, in context of Privacy and Trustworthiness, these are nuaunced and complex issues including subjects like ethics, sociology & governance, and need a comprehensive approach incarporating critical balance amongst Standards, Regulations and Policies to meet the ever evolving needs of the Safe Digital Life of the global citizens in the society. And, Internet of Vehicles is going to be one of the crucial element of the Digital Infrastructure in the decades ahead.

Standards for Internet of Vehicles

IoV involves many participants and the connectivity must be assured between all participants. One of the main challenging issues for the interconnection of vehicles is interoperability. To ensure this, we need to develop standards for the IoV framework. As with other internets connecting real user/consumer experiences with networks to which those user/consumers have no access or control, concerns abound as to risks inherent in the growth of IoV, especially in the areas of privacy and security, and consequently industry and governmental moves to address these concerns have begun including the development of international standards & methods of real-time analysis. These are receiving attention from organisations including the Linux Foundation's ELISA (Enabling Linux In Safety Applications), the connected vehicles initiative at the Institute of Electrical and Electronics Engineers (IEEE), and the Connected Car Working Group at the Cellular Telecommunications Industry Association (CTIA). International organizations and consortia such as the Internet Engineering Task Force, EPCglobal, Institute of Electrical and Electronics Engineers, the European Committee for Standardization (CEN), and the European Telecommunications Standards Institute (ETSI), led by the World Wide Web Consortium (W3C) are investing a lot of efforts to define standards and protocols for IoV. The W3C is focusing on standards for application developers which will provide more accurate access to vehicle data (such as vehicle identification, acceleration and speed, tire pressure, battery status, and personalization information). ETSI and CEN published the basic set of standards requested by the European Commission to ensure interoperable communication between vehicles made by different manufacturers. have been developed for IoT, however, they can be implemented in IoV.

Systems Approach

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure demand a top-down approach to standardization starting at the system or system-architecture rather than at the product level. Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported. It promotes an increased co-operation with many other standards-developing organizations and relevant non-standards bodies needed on an international level. Further, standardization needs to be inclusive, top down and bottom up; a new hybrid model with a comprehensive approach is needed.

Need to develop a comprehensive approach to decarbonization, sustainability, security & resilience, leveraging disruptive technologies, ethically aligned designs, and adopt systems approach to standardization in complex paradigms...

Standards help pre-solve complex problems. Standardization brings innovation and spreads knowledge. Standardization helps define the contours of structured innovation, first because it provides structured methods and reliable data that save time in the innovation process and, second, because it makes it easier to disseminate ground-breaking ideas and knowledge about leading edge techniques. Liberalization and Markets have a lot of great virtues, but they cannot create their own conditions of existences: they must be designed!

Biography

N. Kishor Narang (kishor@narnix.com) is a technology consultant, mentor, and design architect in electrical, electronics, and ICT with over 40 years of professional experience in education, research, design, and consulting. He has over 30 years of hardcore research, design, and development experience in fields as diverse as industrial engineering, power and energy engineering, IT, telecommunications, medical devices, and environmental engineering. Professionally, he is an electronics design engineer practicing design and development across a wide spectrum of products, systems, and solutions through his own independent design house, NARNIX, since 1981. For the last 10 years, he has been deeply involved in standardization in the electrical, electronics, communications, and information technology domains with a focus on identifying gaps in standards to bring harmonization through standardized interfaces to ensure end-to-end Interoperability. He has been leading national standardization initiatives at BIS, the Indian national standards development organization, in smart cities, smart manufacturing, smart energy, and active assisted living as the Chairman of the Smart Infrastructure Sectional Committee LITD 28, along with contributing to multiple other SDOs and initiatives. Globally, he is Vice Chair-Strategy and Project Leader of two international standards in IEC SyC Smart Cities, a Co-Editor of the ISO/IEC JTC1/WG 11 Four Standards, and a member of the Steering Committee of OCEANIS, beyond proactive contributions in many committees in global SDOs.